A NOVEL BRAM BASED PUF FOR FPGA BASED EMBEDDED SYSTEMS

Ahmad Al Khas [1] , M.Sc., Instructor;[1]
Ihsan Cicek[2], Ph.D., Assistant Professor;[2]
[1]Vocational School, [2] Dept. of Electrical-Electronics Eng.,
Istinye University, Istanbul, Turkey

Introduction

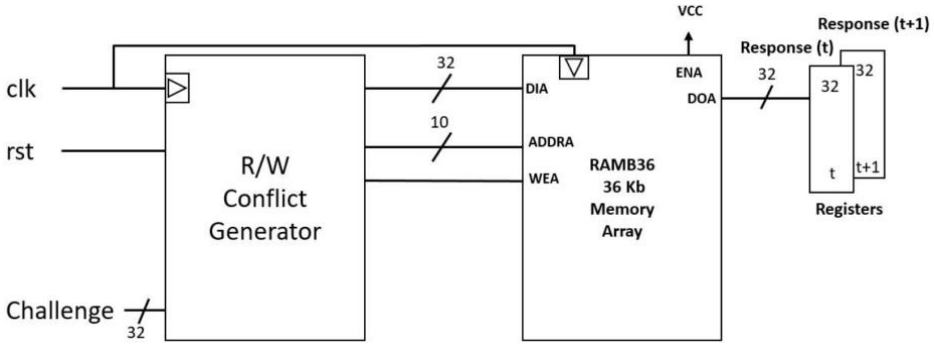
Because of the ubiquitous use of semiconductors in a myriad of products, counterfeit and clone electronic components pose a global threat to the health, safety and security of lives that depend on electronics. Cryptographic methods have been developed for protection against counterfeiting, however the associated cost and resource overhead quickly became a burden for cost sensitive applications such as IoT. Physically unclonable functions PUFs are hardware security primitives which yield unclonable and inherently instance-specific measures of integrated circuits. Security provided by PUFs does not require any extra steps in the fabrication process and is very cost effective [1]. They offer secure authentication with little or no cryptographic assets on the system, thus becoming an efficient solution for resource scarce IoT applications [2]. There are various types of PUFs available in the literature that rely on different design primitives such as arbiters, ring-oscillators or SRAMs [3]. SRAM PUFs depend of the bit-cell uncertainty at the power-up. In FPGA technology, embedded SRAMs also known as Block RAMs (BRAMs) are zeroized on boot and it is not possible to power cycle them easily to generate randomness as in the case of ASICs since designers have limited control. In this work, we present a novel PUF for use in FPGA devices, which is based on creating temporal collisions between the write and read operations that yield random responses from the BRAM. We verified the PUF operation by measurements using an integrated logic analyzer (ILA) provided by FPGA vendor.

FPGA Hardware Implementation and Verification of The BRAM PUF

We used a Xilinx Artix-7 family FPGA device to implement the BRAM PUF which is based on the concept of read-write collisions that can be triggered by the custom module that implements the algorithm shown in Fig.1. The module can trigger the unstable behavior by sending a write and a read request at the same clock cycle to an arbitrarily chosen 10-bit BRAM address. The BRAM is configured to operate in 32-bit synchronous TDP mode.

RWC-PUF generates two 32-bit responses R1, R2 for an arbitrary 32-bit challenge on each operation cycle. R1 is the 32-bit response data resulted from the collision while the challenge was being written and R2 is the one generated during the clearance of the 32-bit challenge data created previously in the same address location. FPGA hardware implementation of the BRAM PUF requires

only 68 LUTs, 135 FFs 17 CLB slices and 1 BRAM to run at 300 MHz on a Xilinx Artix-7 XC7A35T device.



Algorithm 1 Algorithmic Flow of The RWC Generator

```
1: for falling edge(clock cycle T) do
2:     if (State[(T mod 4)] != State[(T mod 4) - 1] then
3:         [T] Address(port A) ← Random_Data[9:0]
4:         [T] Data(port A,in) ← Challenge[T mod 4]
5:         [T+1] Response 1 ← Data(port A, out)[31:0]
6:         [T+2] Data(port A,in) ← Zeros[31:0]
7:         [T+3] Response 2 ← Data(port A, out)[31:0]
8:     else
9:         State[T+1] ← State[T]
10:    end if
11: end for
```

Figure 1. Hardware architecture and algorithm of the proposed BRAM PUF

We used an integrated ILA shown in Fig.2 to observe and acquire the internal signals and verify the expected unstable behavior of the BRAM during hardware execution. The initial hardware test response sets (R1, R2) have been recorded with the help of ILA from two different FPGA boards for comparison. In both experiments, we used the same test conditions and applied the same challenges on the two separate Artix-7 FPGA devices and obtained totally different, device specific responses from each board which confirmed the random behavior. If the RWC generator had failed to generate metastability, the challenges and responses should have been equal for each device.

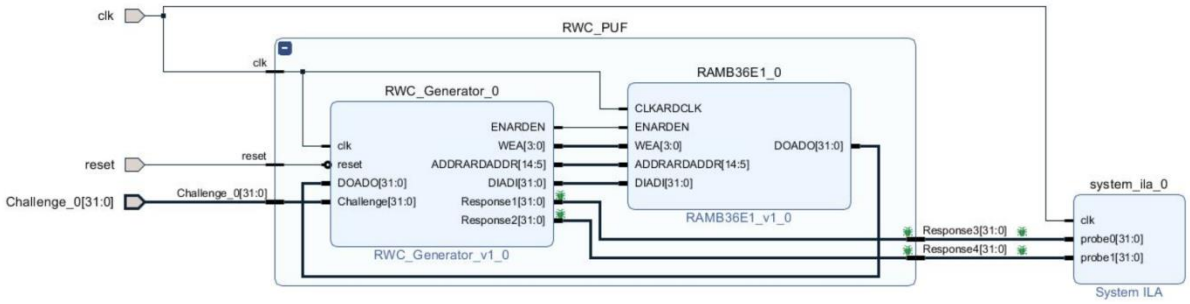


Figure 2. FPGA Implementation of the proposed BRAM PUF.

Performance evaluation of The BRAM PUF

It is essential to have PUFs with reliable, unique, and unbiased responses for cryptographic applications. We collected challenge response pairs (CRPs) for R1 and R2. PUF reliability is tested by measuring the average of Hamming distance between responses for the same applied challenge to the device under test. Intra-chip Hamming distance is the figure-of-merit for the reliability [4]. Since semiconductor devices have temperature dependent behavior, reliability has been measured for temperature variations using a PID controlled hot-plate for heating the FPGA board to the constant temperature of interest while the PUF is operating as shown in Fig. 3. We have acquired response data R1 and R2 at the temperatures 0°C, 26°C (ref.) and 55°C and calculated the associated reliability levels as shown in Table 1 and Fig.4.

Table 1. Reliability Analysis Results of the BRAM PUF for R1 and R2.

Response Type	Min. Reliability (%)	Max. Reliability (%)	Avg. Reliability (%)
R1 at 0°C	96.875	99.8801	98.9208
R1 at 0°C	82.8125	99.8991	93.3122
R2 at 55°C	96.875	99.9190	98.8987
R2 at 55°C	82.8125	99.6094	93.2019

Figure 3. Hotplate testing.

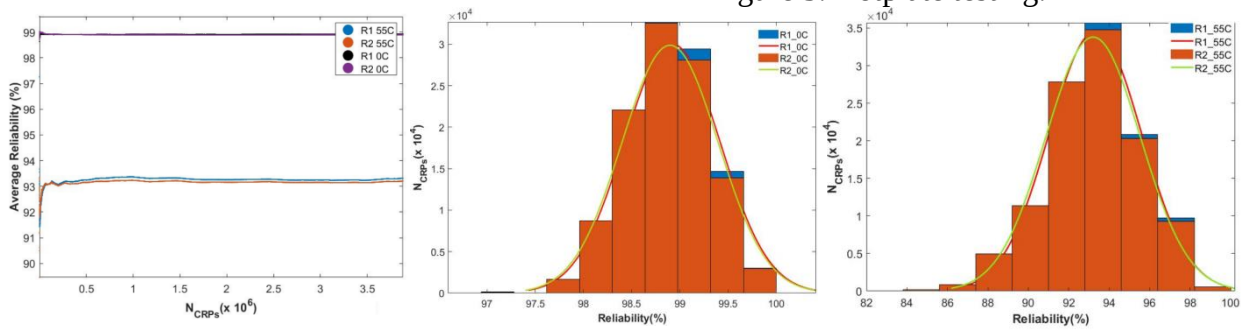


Figure 4. a- Average reliability, b- Reliability at 0°C, c- Reliability at 55°C for R1and R2.

Conclusion

We presented a new BRAM PUF circuit for FPGAs which uses the read-write collisions to generate random responses for any challenge applied to an arbitrarily chosen BRAM address. Our PUF design provides two types of responses R1, R2 and both of them can be used as CRPs. Acquired CRPs for both response type R1 and R2 are evaluated using the reliability metric found in the literature. According to the results both response types exhibit high reliability levels around 99% at 0 °C, however, at 55 °C we observed approximately 7% drop in reliability for both response types with R1 being marginally better. We will evaluate the uniqueness, uniformity and bit-aliasing properties of the PUF circuit as a future work.

References

1. Selimis G., et. al., Evaluation of 90nm 6t-SRAM as physical unclonable function for secure key generation in wireless sensor nodes. 2011 IEEE International Symposium of Circuits and Systems (ISCAS) (2011), pp. 567–570.

2. Mukhopadhyay D. PUFs as promising tools for security in internet of things. IEEE Design Test 33, 3 (June 2016), pp. 103–115.

3. McGrath T., Bagci I. E., Wang Z. M., Roedig U., Young R. J. A PUF taxonomy. Applied Physics Reviews 6, 1 (2019), 011303.

4. Maiti A., Gunreddy V., Schaumont P. A systematic method to evaluate and compare the performance of physical unclonable functions. Embedded Systems Design with FPGAs (2013), 245–267.

Abstract

Physically Unclonable Functions (PUFs) are device specific unique digital fingerprints which are used in cryptographic applications for key generation, unique ID generation and challenge-response based authentication. SRAM based PUFs have become very popular in the ASIC industry as a result of increased security demand against cloning. However, their use in the FPGA applications is limited, since it is not possible to power-cycle the SRAMs once the FPGA device is configured. In this work, we introduce a new approach for designing SRAM based PUFs for FPGAs that use timing violation instead of power cycling. Our PUF design is based on the idea of triggering a collision between read and write operations in a block-RAM to generate random responses. We have functionally verified the PUF prototype implemented on an Artix-7 FPGA device using an integrated logic analyzer. The challenge response pairs acquired from the PUF prototype have been tested for reliability. On the average, proposed PUF achieved 93% reliability at 55 °C ambient temperature.

Keywords: Physically Unclonable Function, BRAM PUF, SRAM PUF, FPGA Fingerprint.