A NOVEL TECHNIQUE OF CONFIGURABLE RING OSCILLATOR FOR PHYSICAL UNCLONABLE FUNCTIONS

Kavita Chandrakant Mugali ¹, Prof. Minakshee M. Patil ²

¹,² Department of Electronics and Telecommunication, Sinhgad Academy of Engineering, Kondhwa, Pune, India.

ABSTRACT: The Silicon Physical Unclonable Function (SPUF) was first introduced by Devadas. The silicon PUF works on the basis of the variations in delays present in the gates as well as wires. The ring oscillator PUF is one of the implementation of SPUF. The ring oscillator requires one pair of ring oscillators for each output bit. So for collecting more number of output bits to acquire safe security level, more number of ring oscillators are required. This problem can be solved by using configurable PUF. Configurable ring oscillator PUF was introduced by Maiti to improve reliability of basic ring oscillator PUF. In this PUF, the ring oscillator is fitted in configurable logic block (CLB) by using look up tables (LUT) and dedicated multiplexers. In this paper the configurable ring oscillator analysis is presented. The hard macro of configurable ring oscillator is implemented for identical placement and outing inside CLB. The configurable logic block gives better results than simple ring oscillator PUF.

Keywords: Physical Unclonable Functions, Configurable ring oscillator, Hard macro, Challenge-response pairs.

[1] INTRODUCTION

In cryptographic applications device authentication has become an important issue. The PUF circuits can be used to authenticate the devices at very low cost. PUFs work based on the property of process variation which is inherent in the circuit. The general PUF is shown in Figure 1. It takes m bits of challenge and gives n bit response [7]. These response bits vary from chip to chip for same challenges. Thus the challenge response pairs can be generated. The particular challenge-response mapping is unique for each chip. So the particular chip can be authenticated. The quality of PUF can be measured by using inter chip and intra chip variations. The inter chip variation is the bits changed when the PUF is regenerated again and again for same chip. Inter chip variation is the comparison of the bits produced by the PUF on one chip to the bits produced by the same PUF on other chip [2].
There are many types of PUFs. Butterfly PUF, optical PUF [8], logic based PUF, magnetic PUF, silicon PUF [4] etc are the types of various PUFs. The silicon PUF [4] is further classified as arbiter PUF and ring oscillator PUF [1].

[1.1] ARBITER PUF

It uses two paths for inputs and also has the D type flip flop as an arbiter [6]. The rising edge input signal is given simultaneously to both input paths. The output bit depends on the faster path signal. The disadvantage of this type of PUF is that it requires the symmetric type of routing and placement of design in the FPGA. If this condition is not satisfied then the response of arbiter PUF depends on routing delays instead of process variations.

[1.2] RING OSCILLATOR PUF

The basic ring oscillator is the chain of odd number of inverters. Figure 2 shows the basic ring oscillator. The ring oscillator PUF requirement is that only the ring oscillator instances should be identical and not the entire design to be symmetrically placed and routed. The identical routing of ring oscillators can be achieved by using hard macro on FPGA. Even the ring oscillators are very similar in nature their frequencies are slightly different due to delay difference in their paths. This property of ring oscillators enables them to identify devices and to authenticate the particular device [3, 9]. The 1-out-of-k masking scheme is used for better reliability. The PUF using ring oscillator is shown in Figure 3.

[2] CONFIGURABLE RING OSCILLATOR

Maiti [1] introduced the configurable ring oscillator for PUF which is fitted within the single CLB in Xilinx FPGA. The advantage of this size is that all the routings of resources inside CLB are limited to switch box associated with the particular CLB. This type of ring oscillator can be duplicated by using hard macro. The differences in the frequencies of this type of ring oscillators depend only on process variation. The CLB inside Xilinx Spartan 3 FPGA consists of four slices. Each slide has two LUTs, two flip flops, one multiplexer and some other resources.
Figure 4 shows configurable ring oscillator. The select lines of multiplexers used to select the LUTs are named as C1, C2, C3. These select lines enable eight different configurations of select signals. The ring oscillator defined by each configuration has different frequency of oscillation as the delay variations within different LUTs are different. Thus while comparing frequencies of two ring oscillators the configuration taken into account must be the same for both ring oscillators. Thus the difference between two selected ring oscillator frequencies depends only on manufacturing variations and not on the routings. Thus eight different output bits can be generated by selected only single pair of ring oscillator. The mapping of ring oscillator in single CLB of Xilinx Spartan 3 FPGA is shown in Figure 5.

![Figure 4. Configurable ring oscillator](image)

![Figure 5. Mapping of configurable ring oscillator in single CLB of Xilinx Spartan3](image)

[3] HARD MACRO

By using lowest FPGA primitives the required design can be implemented. This can be done by creating hard macros. The hard macro is implemented by using Xilinx FPGA editor. They are the manually placed, configured and routed designs. They can be instantiated several times inside the FPGA. The design created by using hard macro has exactly similar layout and arrangement inside the circuit instantiated in FPGA.

The above feature of hard macro is taken into account and can be used for the similar structures of ring oscillators which are instantiated multiple times inside FPGA. Figure 6 shows the ring oscillator hard macro created for Xilinx Spartan 3 FPGA by using FPGA editor. The ring oscillator consists of three inverters and one AND gate to provide enable input signal to it. These inverters and AND gate are placed inside the LUTS. The multiplexers used to choose path inside oscillator are also fitted in dedicated multiplexer inside the slice.

The configuration logic blocks (CLB) are the basic building blocks of Xilinx FPGAs. The entire ring oscillator is fitted in single CLB. The routing inside hard macro is concerned only with the switch boxes and look-up tables (LUT). So they are easier to handle. Only three
in inverters are used in this type of ring oscillator which enables the routing of single ring oscillator only within one CLB. This ensures that all the ring oscillator instances have identical routing within CLB. Thus local routing inside CLB is achieved in this manner.

**Figure 7** shows the hard macro instantiated in Spartan 3 FPGA. An array of 9x9 ring oscillators is created and placed at the desired location. The relative placement constraints can be given in the constraint file (.ucf file) to all the ring oscillator instances to place them at the desired location inside FPGA. Generally the array of ring oscillators is placed in the middle portion of the FPGA layout.

![Figure 7: Hard macro instantiated in Xilinx Spartan 3](image)

The frequency of ring oscillator depends on its location inside FPGA layout [5]. Other PUFs like arbiter PUF and butterfly PUF require symmetrical routing for local as well as non local wires. This is very difficult task to achieve [7]. But the ring oscillator PUF allows to instantiate hard macro for symmetrical routing. So it is very easy instantiate it multiple times.

The ring oscillators which are at the center of FPGA layout are faster than located at the edges of FPGA. Other logic circuits present around the ring oscillator array also have the significant influence on the frequency of ring oscillator. This causes spatial dependence of frequencies. So the logic circuit other than ring oscillator array should be placed at some distance from array to separate them to reduce influence. The logic can be placed separately by floor planning by Xilinx tool.
[4] CONCLUSION

The configurable ring oscillator is implemented on Xilinx Spartan 3 platform. An array of 9x9 ring oscillators is instantiated by creating hard macro of the configurable ring oscillator. The ring oscillator PUF is tested on the Xilinx Spartan 3 (xc3s250PQ208) FPGA. Only negligible amount of bits got changed during testing it on same FPGA. The results are very much better than the simple basic ring oscillator PUF. Thus the configurable ring oscillator is promising approach for the authentication of the chips.
REFERENCES