Design and Implementation of a Secure Physical Unclonable Function In FPGA

Submitted by aekwall on Mon, 06/28/2021 - 12:40pm

Title
Design and Implementation of a Secure Physical Unclonable Function In FPGA

Publication Type
Conference Paper

Year of Publication
2020

Authors
Latha Ch., Mary, Bazil Raj, A.A., Abhikshit, L.

Conference Name
2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)

Date Published
jul

Keywords
Challenge Response Pair, composability, delays, field programmable gate arrays, Hamming distance, Hardware Trojans, Intellectual Property Protection, intellectual property security, Inverters, physical unclonable function, policy-based governance, pubcrawl, Resiliency, Ring Oscillator PUF, Ring oscillators, Semiconductor device measurement, Temperature measurement

Abstract
A Field Programmable Gate Array (FPGA) is a digital Integrated Circuit made up of interconnected functional blocks, which can be programmed by the end-user to perform required logic functions. As FPGAs are re-programmable, partially re-configurable and have lowertime to market, FPGA has become a vital component in the field of electronics. FPGAs are undergoing many security issues as the adversaries are trying to make profits by replicating the original design, without any investment. The major security issues are cloning, counterfeiting, reverse engineering, Physical tampering, and insertion of malicious components, etc. So, there is a need for security of FPGAs. A Secret key must be embedded in an IC, to provide identification and authentication to it. Physical Unclonable Functions (PUFs) can provide these secret keys, by using the physical properties of the chip. These physical properties are not reproducible even by the manufacturer. Hence the responses produced by the PUF are unique for every individual chip. The method of generating unique binary signatures helps in cryptographic key generation, digital rights management, Intellectual Property (IP) protection, IC counterfeit prevention, and device authentication. The PUFs are very promising in signature generation in the field of hardware security. In this paper, the secret binary responses is generated with the help of a delay based Ring Oscillator PUF, which does not use a clock circuit in its architecture.

DOI
10.1109/ICIRCA48905.2020.9183101

Citation Key
latha_ch_design_2020
field programmable gate arrays Resiliency pubcrawl composability policy-based governance delays Semiconductor device measurement Temperature measurement Hamming distance Inverters Challenge Response Pair Hardware Trojans Intellectual Property Protection Physical Unclonable Function Ring Oscillator PUF Ring oscillators intellectual property security