Design and Analysis of Light Weight Physically Unclonable Function (PUF) Targeting Cost Effective Hardware Security

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

in

Computer Science & Engineering

By

Mahabub Hasan Mahalat
(NITD/Phd/CS/2018/01021)

Under the Supervision of

Dr. Bibhash Sen
Associate Professor
Department of Computer Science & Engineering, NIT Durgapur



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY DURGAPUR
WEST BENGAL – 713209
INDIA

May, 2022

Abstract

The unprecedented growth of technology, rising number of advanced threats, limitations of conventional security measures propel the innovation of hardware-oriented security mechanisms. Also, the emergence of the Internet of Things (IoT) triggers the development of lightweight security. Towards this direction, Physically Unclonable Function (PUF) has emerged as a promising hardware security primitive to provide cost effective security. PUF maps an input (challenge) to an output (response) where the intrinsic manufacturing variation of the underlying entity defines the unique mapping relation. The contributions of this thesis focus on the design, analysis, and applications of PUF for low-cost security. In particular, the silicon PUFs (PUFs implemented on Silicon device/IC) are investigated here due to their apparent applications.

Stability against the environmental noise (reliability), hardware overhead, the ability to uniquely identify a device (uniqueness), and security are the primary criteria in designing a PUF. Also, the implementation challenges of a PUF on Field Programmable Gate Array (FPGA) plays a vital role in design. In this thesis, a number of PUF designs have been proposed to tackle these challenges. The work presents the design of a latch based ring oscillator(RO) PUF due to its suitability on FPGA to improve the stability against environmental noise without imposing additional area overhead. Experimental analysis is performed by characterizing the latch based RO PUF on FPGA in different environmental conditions. Again, arbiter PUF for its lightweight structure is advocated as the most promising for IoT. But the requirement of symmetric implementation makes it difficult to implement a high-quality arbiter PUF on FPGA. This work performs an experimental analysis on the existing tuning concept used to implement an arbiter PUF on FPGA, which depicts its limitations. Thus, the thesis develops a switching structure named path changing switch (PCS) and utilizes it to implement an arbiter PUF on FPGA efficiently. The performance and security of the PCS-based arbiter PUF are verified. Subsequently, the XOR composition is suggested and validated to enhance the performance and security of the basic PCS based arbiter PUF. The thesis also presents a circular configurable arbiter PUF (CAPUF) design that amalgams non-linearity and strict avalanche criterion (SAC) to ensure desired security while maintaining high reliability with cost-effective hardware.

Finally, the thesis deals with the application of PUF for the low-cost security of lightweight devices. A secure and lightweight scheme is developed for communication among different Wireless Sensor Network (WSN) devices by combining PUF with secret sharing schemes. The performance analysis, the formal and informal security analysis illustrate the suitability of the proposed scheme.