A Framework for the Evaluation of Physical Unclonable Functions

Abhranil Maiti, Vikash Gunreddy, Patrick Schaumont

{abhranil, gvikash7, schaum}@vt.edu

Electrical & Computer Engineering Department, Virginia Tech, Blacksburg, Virginia, USA

In this work, we define a framework that will evaluate the performance of a Physical Unclonable Function (PUF) which is an emerging technology in hardware security area. The framework will work on the challenges and the responses of a PUF irrespective of the underlying PUF circuit.

A PUF is a chip-unique challenge-response mechanism exploiting manufacturing process variation inside integrated circuits (ICs). It has many useful applications such as device authentication and secure, memory-less key storage. A mobile device can be authenticated using a PUF challenge-response pair. Moreover, a cryptographic key can be securely embedded in a mobile device using a PUF without an expensive storage circuit such as flash memory therefore reducing resource cost and solving key storage issues.

A PUF should generate responses that are not only unpredictable but also consistently reproducible. It is critical to quantify these quality factors in a concrete manner such that the performance of a PUF can be evaluated fairly accurately. This is becoming even more essential as many different PUF techniques have been proposed so far. Our proposed framework will be able to compare the efficiency of different PUF techniques with respect to a common reference.

In this context, we not only define several performance indicators but also explore many other performance indicators proposed by different researchers. For example, it is important to evaluate how the device identifiers composed of PUF responses can distinguish several different chips without error. We analyze different performance indicators based on an n-bit PUF identifier to estimate the ability of a PUF to correctly distinguish a sizable group of chips. Similarly, we also study how the reliability of a PUF response bit could be determined based on measurement data from a PUF. We validate the framework using data measured from multiple PUF techniques implemented on off-the-shelf FPGA chips.