Abstract

Design and Analysis of Secure Physically Unclonable Function Compositions

Silicon Physically Unclonable Function (PUF) circuits exploit device-level CMOS manufacturing process induced variations to define a random and IC-specific physical challenge-response mapping. Since most of the primitive delay PUF designs such as Arbiter PUF (APUF) are proven to be insecure against modeling attacks, compositions of primitive PUFs are used to achieve robustness against modeling attacks. However, the reliability of the resultant PUF is usually significantly less compared to primitive PUF designs. The primary goal of this thesis is the design and security analyses of secure PUF compositions with higher reliability assurance.

Our proposed Composite PUF design framework can be used to design a PUF using a set of primitive PUFs with enhanced performance and security metrics. One of the major problems with most of the existing PUF compositions is that reliability of the resulting PUF reduces with increasing number of primitive PUFs used in compositions. As a solution to this problem, we propose a multiplexer based composition of APUFs, called MPUF. Our proposed MPUF variant, called rMPUF, can achieve higher reliability and security against reliability based modeling attack compared to any practical instance of XOR APUF. To the best of our knowledge, rMPUF is the only APUF composition that is robust against most powerful reliability based modeling attack.

Since APUF designs are often used in composition due to its lightweight property, we propose an architectural analysis technique to select good APUF variants for composition. Our analysis reveals that the classic APUF architecture is superior to its two FPGA variants, namely Programmable delay line based APUF (PAPUF) and Double APUF (DAPUF). Thus, in ASIC, APUF should be used in composition instead of architecturally weak PAPUF and DAPUF.

For security analysis, we develop an unpredictability test based on the propagation property of PUF. We show that APUF, XOR APUF and Lightweight Secure PUF (LSPUF) cannot pass this test. As a result of the failure in this test, it is revealed that adversary can generate related challenge-response pairs (CRPs). These related CRPs should not be used in security applications. In addition, we develop various cryptanalysis techniques that can be used by an adversary to reduce the security level of PUF design. We also demonstrate how these cryptanalysis techniques are used along with traditional machine learning techniques to achieve an enhanced modeling attack. Our proposed cryptanalysis assisted modeling attack on LSPUF shows that multibit output LSPUF instances are not secure.

Finally, we provide fault-tolerant implementations of various delay PUFs implemented on FPGA against laser fault attacks. Our fault tolerant solutions can detect runtime faults, and prevent information leakage through faulty output. To recover the faulty PUFs on FPGA, we implement PUFs using configurable LUT and random-sliding features.

Keywords: Physically unclonable functions (PUF), Arbiter PUF, Composite PUF, Cryptanalysis, Modeling Attacks, Chosen-challenge Attacks, Adaptively Chosen-challenge Attacks, Architectural Bias, Propagation Property, Field Programmable Gate Array (FPGA), Fault Tolerant PUF Implementation.