Abstract

The last 25 years have witnessed an exponential growth of the number of devices connected to the Internet of Things (IoT) from a million in 1992 to 20 billion in 2017. Despite IoT has become widespread, this concept is still not well-established due to several reasons such as lack of standards, security and data protection issues, maintenance cost, etc. Since much of the sensitive personal data is transmitted via IoT devices, security can be highlighted as one of the most important challenges for this area. Classical hardware cryptography methods have two major disadvantages, significant hardware overhead required for its implementation and non-volatile memory for secret key storage. One effective way to provide secure chip authentication with low overhead is the Physical Unclonable Functions (PUF). They are widely used as a cryptographic primitive to avoid the need for storing the key or secret that can be used to retrieve the device key in the non-volatile memory. PUFs uses the intrinsic manufacturing process variations of the chip to generate unique and random response to a given challenge to identify a chip. It is a unique property of the integrated circuit (IC). For reliable key generation, it is required that the responses of the PUF are highly stable against operating environment variations such as temperature and supply voltage variations. One of the most well-explored PUF design is Arbiter PUF (A-PUF), which has been utilized by Verayo to implement RFID ICs as well as by Xilinx to include PUF IP as a hardware root of trust for its new Zynq UltraScale+ devices. However, existing Arbiter PUF designs suffer from poor reliability especially when implemented on FPGA platform due to routing constraints. On the other hand, improving temporal stability of A-PUF responses makes the circuit vulnerable to modeling attack using machine learning methods.

This thesis presents a comprehensive overview of state-of-the-art PUF designs and their ASIC and FPGA implementations. As a means for reliability enhancement, a new hybrid PUF based on A-PUF is proposed. Using the RS-latch instead of D Flip-Flop as an arbiter makes it possible to expand the original response states to a ternary set {stable 0, stable 1 and High Frequency Oscillation (HFO)}. The enhanced reliability and uniqueness were attested by experimental results implemented on FPGA platform. To further improve its reliability to the ideal 1.0 over a wide range (from -45 °C to +90 °C) of temperature, a challenge classification algorithm is introduced. The proposed method has been tested on identical FPGA chips of two different families and has shown no degradation on uniqueness. To prevent modeling attack, two approaches based on non-linear challenge processing are presented in this thesis. It has been shown that the proposed techniques are resilient against different machine learning algorithms including the most advanced Covariance Matrix Adaptation Evolutionary Strategy (CMA-ES). The abovementioned contributions are utilized to build a low-cost authentication protocol based on 100% accurate model of A-PUF.