TIMA-PUF: A reliable arbiter PUF architecture

Azzadine THAJTE
TIMA - Universite Grenoble Alpes, France

Abstract

Physical Unclonable Functions (PUFs) have gained prominence as a robust mechanism for cryptographic applications, including secure key generation and device authentication, by generating unique and irreproducible challenge-response pairs (CRPs). However, conventional PUF architectures frequently exhibit reliability limitations, especially under environmental fluctuations and aging-induced degradations. In this talk, we introduce a novel strong PUF architecture named TIMA-PUF, which leverages the measurement of propagation delays across two identical paths utilizing a high-resolution time-to-digital converter (TDC). The information on the magnitude of the delay variations enhance the response characterization and allows achieving optimal PUF metrics, simply by filtering unreliable CRPs. The proposed PUF benefits from the strengths of a classical arbiter PUF, such as the ability to extract a large number of CRPs at high throughput while improving its main weakness, namely its low entropy. The proposed PUF design has been implemented and tested on FPGA platform, with results showing a significant improvement in PUF metrics after using the filtering technique.