SETS’26

Title: Improving RO-PUFs on FPGAs: A Filtering Approach for Improved Reliability and Entropy

Authors: Vasilii Kulagin, Giorgio Di Natale, Elena-Ioana Vatajelu

Abstract :

Physical Unclonable Functions (PUFs) are increasingly used as a practical alternative to non-volatile memory for cryptographic primitives. Instead of storing secrets on-chip, a PUF derives a device-unique response on demand. In practice, however, PUF outputs can drift over time: small variations in temperature or supply voltage, whether from normal operation or adversarial stress (e.g., thermal attacks), may lead to unreliable and biased responses. This presentation introduces a new filtering technique for ring oscillator PUFs (RO-PUFs) implemented on an FPGA, aimed at improving response stability while reducing bias.