Experiment 7 summary

This experiment focused on implementing and analyzing hardware-based security primitives, specifically Physical Unclonable Functions (PUFs) and True Random Number Generators (TRNGs), using SRAM and Ring Oscillators (ROs) on a Field-Programmable Gate Array (FPGA). This experiment was not completed in its entirety, but the outcome of each part was predicted based on online material / ChatGPT interpretation.

Part 1: SRAM PUF Implementation
- Steps: Assembly language code was written for the microcontroller to send SRAM cell data to the FPGA. Matlab was used to calculate the mean value and hamming distance of the data signatures.
- Observations: A signature of 64 bytes from SRAM power-up states was generated. The frequency of the square wave generated was 1.08Hz. Significant bit variations are expected at different voltages.

Part 2: RO-PUF Implementation
- Steps: RO-PUF was implemented to generate a 128-bit key. Data collected at different voltages and analyzed.
- Observations: The keys varied with changes in operating voltage, indicating sensitivity to voltage variations.

Part 3: SRAM-based TRNG
- Steps: Multiple signatures were taken from the SRAM PUF to identify random bits. These bits were used as a source for the TRNG.
- Observations: An 8-bit value from specific SRAM cells was identified as a suitable source for TRNG.

Part 4: RO-based TRNG Implementation
- Steps: Implemented using ten 5-stage ROs. The number of stages and ROs were varied, and the results were collected at different voltages.
- Observations: The design showed variations in output, demonstrating the effectiveness of the RO-based TRNG.

Part 5: Randomness Evaluation
- Steps: The NIST statistical tool was used to evaluate the randomness of the RO-based TRNG.
- Observations: Comprehensive testing was conducted, though specific results of the randomness tests were not detailed in the summary.

Summary

The experiment successfully demonstrated the implementation and evaluation of SRAM and RO-based PUFs and TRNGs. Challenges were encountered in microcontroller coding and placement of ROs, but were overcome. The experiment highlighted the sensitivity of these

hardware-based security primitives to environmental factors like voltage, and their potential applications in generating secure, unclonable identities and random numbers for cryptographic purposes. The effectiveness and robustness of these systems were evaluated, demonstrating their potential in hardware security.