Physical Unclonable Function: Extracting Hardware Fingerprints to Generate Cryptographic Key

Tauhidur Rahman, Florida International University

Full points: 100 (see rubric)

Objective: The objective is to introduce students to the concept of side-channel attacks, focusing on power consumption analysis to extract sensitive information from embedded systems. Students will learn to analyze power consumption traces and explore countermeasures to mitigate side-channel vulnerabilities.

Task for Students:

Pre-lab Reading:

- Overview of side-channel attacks and their relevance in embedded systems security (see class lecture)
- Explanation of different side-channel attack vectors, with a focus on power consumption analysis (see class lecture).

Write a Code: Use the cryptographic code that you implemented in Module 2.

Setting up the Experiment:

- Upload the sample cryptographic code to the microcontroller board.
- Connecting the oscilloscope or power analysis tool to the microcontroller for data collection.

Power Consumption Analysis

- Execute cryptographic operations (e.g., AES encryption) on the microcontroller while collecting power consumption traces.
- Save the power traces to a computer for analysis.

Data Processing and Attack:

- Process the power traces using side-channel analysis software (e.g., ChipWhisperer).
- Use the side-channel attack algorithm provided to you to recover a secret key.
- Discuss the observed patterns and leakage points.

Countermeasures and Mitigations

- Discuss possible countermeasures against side-channel attacks (e.g., blinding, masking, hardware-based protections).
- Discussion of best practices in securing embedded systems against side-channel vulnerabilities.