Physical Unclonable Function: Extracting Hardware Fingerprints to Generate Cryptographic Key

Tauhidur Rahman, Florida International University

Full points: 100 (see rubric)

Objective of Core Course: Design of a memory controller.

Added Security Concept: Use the start-up value of SRAM as a device fingerprint.

Designing a memory controller for SRAM (Static Random-Access Memory) involves several components and considerations. SRAM is a type of volatile memory that stores data as long as power is supplied. Here's a high-level outline of how you can design a basic SRAM memory controller:

- **Specification and Requirements**: Define the specifications and requirements of your SRAM memory controller. Determine the data bus width, address bus width, memory size, clock frequency, and any specific timing requirements.
- **Address Decoding**: Create an address decoder that takes the address input from the CPU and selects the appropriate SRAM memory location. The address decoder should convert the CPU's address into the SRAM's row and column addresses.
- **Control Logic**: Develop control logic that manages the read operation. This logic should include state machines or control signals to coordinate the various steps of the read process, including address setup, data retrieval, and output.
- **Read Operation**: Implement the read operation, which typically involves the following steps:
    - Assert the Chip Select (CS) signal to enable the SRAM chip.
    - Provide the row and column address to the SRAM.
    - Activate the Read Enable (RE) signal to initiate the read operation.
    - Wait for the SRAM to output the data.
    - Capture and buffer the data output from the SRAM.
- **Data Output Buffer**: Design a data output buffer that temporarily stores the data read from the SRAM. The buffer should match the data bus width of your system.
- **Timing Considerations**: Pay close attention to timing constraints, including setup and hold times, clock-to-output times, and any other SRAM-specific timing parameters specified in the SRAM's datasheet.
- **Clock Synchronization**: Ensure that the memory controller's clock is synchronized with the SRAM's clock domain if necessary. This may involve clock domain crossing techniques to avoid timing issues.

Added Security Concept:

- **Read Start-up Data**: Activate the SRAM and retrieve its initial data.
- **Multiple Measurements**: Power down the device and subsequently restart it five times, recording the start-up values on each occasion.
- **Measure Reliability**: Assess the consistency of each measurement by comparing the obtained signatures and calculating the variations between successive measurements.

- **Uniqueness Test**: Swap out the SRAM and observe if two different SRAM modules yield distinct output values.