Hardware-Oriented Security and Trust
ECE 4156 A / ECE 6156 A
Spring 2026

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 10, 50 pts. (ECE 4156) 60 pts. (ECE 6156)
Due Friday April 17 prior to 11:55pm

1) (10 pts.) What is the purpose of a fuzzy extractor?

Solution

The major purpose of fuzzy extraction is to encode or "sketch" the challenges in a way that with helper data calculated the original response can be recovered or extracted even in the presence of one or a few bit errors. In other words, even with "fuzziness" or errors in the responses, the encoding techniques including helper data calculations enable the reliable extraction of the correct response with a high probability (depending on how many bit errors there are – above a certain threshold the fuzzy extraction no longer works).

2) (20 pts.) Consider the reverse fuzzy extractor.

a. (10 pts.) What is the purpose of a reverse fuzzy extractor? Be sure to distinguish your answer from the answer you gave for the purpose of a fuzzy extractor (see question 4 above); in other words, if you give the same answer here you will receive zero points.

Solution

A fuzzy extractor has two procedures as follows. First, there is the Generate or Gen process which produces helper data. Second, there is a Reproduce or Rep process which error-corrects a response with potential bit errors given the potentially erroneous response and the helper data.

The original published approaches to fuzzy extraction carried out the Gen process on the server during enrollment (i.e., where the server is the main computational entity interacting with the resource constrained chip with the PUF) while the Rep process is carried out on the same chip as the PUF. However, the observation that the Gen process is much simpler and more constrained than the Rep process led to the proposal of reverse fuzzy extraction.

A reverse fuzzy extractor implements the expensive Rep process on the server with the Gen process implemented on the same chip as the PUF. The purpose of this is to reduce the energy and computational overheads incurred on the resource constrained PUF chip.

b. (10 pts.) What must the server do to the stored response bitstring it has in its secure database in a reverse fuzzy extractor scheme?

Solution

In the reverse fuzzy extractor scheme, the server must "error-correct" the stored response bitstring r_i using the helper data hd_i to produce r''_i which hopefully is equal to r'_i (where r'_i is the uncorrected PUF response to the challenge)

3) (10 pts.) Briefly describe the difference between detecting Hardware Trojans in a hardware description, e.g., a VHDL module, versus detecting Hardware Trojans in a GDS II layout. What types of detection techniques can be used for each?

Solution

Detecting Hardware Trojans at the HDL/gate-level (e.g., VHDL) is a pre-silicon problem focused on analyzing design intent and logic behavior, whereas detection at the GDSII/layout level is a post-design/post-fabrication problem focused on physical structure and side effects. At the HDL level, detection techniques rely on functional and structural analysis, such as information-flow tracking, formal verification (limited to smaller circuits), testability metrics (e.g., controllability/observability), and identifying rarely activated logic or anomalous trigger conditions.

In contrast, layout-level detection cannot rely on high-level semantics and instead uses physical inspection and side-channel analysis, including imaging (SEM/optical comparison), power/delay signatures, and comparison against a "golden" chip reference. Additionally, path-delay testing and multi-parameter side-channel measurements are commonly used at the GDSII stage to detect subtle parametric changes introduced by Trojans. HDL detection is more scalable and preventive but can miss well-hidden Trojans, while layout-level detection is more direct but costly and often requires physical access and reference designs.

4) (10 pts.) Hardware Trojans can be classified into two basic classes, functionally disruptive and information leakage types. Indicate the basic detection strategies that are applicable for detecting Trojans in each class: detection strategies include logic testing, parametric testing and IC deprocessing.

a. (5 pts.) Indicate the basic detection strategies for functionally disruptive Hardware Trojans.

Solution

Functionally disruptive Trojans modify the intended behavior of the circuit (e.g., cause failure or incorrect outputs), so logic testing is the primary detection strategy. This involves ATPG-based test pattern generation to activate rare trigger conditions and observe incorrect outputs, especially targeting low-controllability/low-observability nodes . Parametric testing can also help, since added Trojan logic may slightly alter delay or power. IC deprocessing is effective as a means to directly inspect structural modifications, though it is costly and destructive.

b. (5 pts.) Indicate the basic detection strategies for information leakage Hardware Trojans.

Solution

Information leakage Trojans typically do not alter functional outputs and are often subtle, making logic testing largely ineffective . Instead, parametric testing is the main strategy, detecting subtle side-channel anomalies such as changes in power, EM emissions, or timing caused by the Trojan's covert activity. These Trojans can be very small and stealthy, sometimes leaking data via power or communication channels without obvious functional impact . IC deprocessing can also be used to physically identify hidden circuitry, though it may still miss very small or selectively inserted Trojans.

5) [ECE 6156 only!] (10 pts.) Why is it a concern in a reverse fuzzy extractor that the helper data changes from one run of the protocol to the next?

Solution

Helper data leaks some information about the response r_i in fuzzy extractors. But, with variations in helper data string additional information may be revealed that the adversary can use in attack models.

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES, INCLUDING OTHER/PREVIOUS SECTIONS OF ECE COURSES TAUGHT BY PROFESSOR MOONEY SUCH AS THOSE WITH NAMES INCLUDING HARDWARE ORIENTED SECURITY AND TRUST AS WELL AS CRYPTOGRAPHIC HARDWARE FOR EMBEDDED SYSTEMS. ALL HOMEWORK SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SUBMISSIONS MUST BE DONE ONLINE. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE WITH THICK INK AND MAY NOT BE ABLE TO USE LOW RESOLUTION PHOTOS OF HANDWRITTEN DIAGRAMS). FAILURE TO PROVIDE CLEAR AND LEGIBLE ANSWERS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).