ECE 4451: Introduction to Hardware Security and Trust

Credits and contact hours: 3 Credits (Two 75-minute class periods per week)

Instructor: Marten van Dijk

Textbook: none

Other supplemental materials: Selected academic papers on secure processor architectures and related topics.

***Specific course information*:**

a. *Catalog Description*: Fundamentals of hardware security and trust for integrated circuits. Cryptographic hardware, invasive and non-invasive attacks, side-channel attacks, physically unclonable functions, watermarking of Intellectual Property (IP) blocks, FPGA security, counterfeit detection, hardware Trojan detection and prevention in IP cores and integrated circuits.

b. *Prerequisite*: ECE 3401; consent of instructor; open only to students in the School of Engineering.

c. *Required, elective, or selected elective:* Selected elective (CMPE)

***Specific goals for the course*:**

a. *Specific outcomes of instruction*: To understand main hardware security concepts:
   a. To be able to converse intelligently about secure processor architectures.
   b. Being able to simulate performance of added hardware modules.
   c. Understand a wide range of hardware security concepts. In particular, be able to reason about security in terms of adversarial models, hardware vulnerabilities, and attacks.
   d. Describe conceptually how the field of hardware security is evolving.

b. *EAC Criterion 3 Student Outcomes addressed by the course*:

(1) **an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics**
Students apply principles of engineering to do several hands-on assignments during which they design and attack security solutions.

(2) **an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors**
n/a

(3) **an ability to communicate effectively with a range of audiences**
n/a

(4) **an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts**
n/a

(5) **an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives**
n/a

(6) **an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions**
n/a

(7) **an ability to acquire and apply new knowledge as needed, using appropriate learning strategies.**
Students use the web, library databases, and other resources to find material for completing their assignments.

Topics covered:
This course treats several topics in hardware security:

- The main focus is secure processor architectures: Intel SGX as well as academic processors such as Aegis, Ascend, and Sanctum together with the minimally required computer architecture background.
- Cryptographic concepts (no proofs or formal definitions) used in secure processor architectures such as AES, RSA, Hash, MAC, digital signatures, public key encryption, and ORAM.
- Brief explanation of side channel attacks, physical unclonable functions, TRNG, supply chain management, and hardware Trojans and an overview of several other topics (in particular, security in cyber physical systems and embedded systems, e.g., the power grid and smart cities).
- Several coding assignments (involving attacks and computer architectural simulation of designed modules).