Midterm II Review / Comments on Topics Covered and Relationships

*Cryptographic Hardware for Embedded Systems*

*ECE 3894*

Fall 2019

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology
Basics

• Questions to consider
  • If one measures the energy consumption or power of a microchip, what do the power traces reveal?
  • What is the statistical methodology used to reveal the information claimed to have been learned?

• Power Analysis
  • Introduction (Lecture 25)
  • Energy consumption in silicon and processors (Lecture 26)
  • Hamming weight dependent microcontroller power (Lecture 28)
  • Detailed examples of HW dependent power (Lecture 29)
  • Data and operation dependent power (Lecture 30)
  • Covariance and correlation (Lecture 30)
Differential Power Analysis (DPA)

• Introduction (Lecture 27, slides from the University of New Mexico)
• Five steps common to all DPA (Lecture 31)
Countermeasures to DPA

• Introduction (Lecture 35, slides from the University of New Mexico)