Midterm II Review / Comments on Topics Covered and Relationships

ECE 4156/6156 Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading Assignments Since Midterm I

- Chapter 8 of Introduction to Modern Cryptography by Katz and Lindel, but only the parts related to the RSA lecture notes
- Chapter 10 of Introduction to Modern Cryptography by Katz and Lindel, but only the parts related to the lecture notes
- Physically Unclonable Functions: *Constructions, Properties and Applications* by Roel Maes, Springer-Verlag, 2013.
- R. Needham and M. Schroeder, "Using encryption for authentication in large networks of computers," *Communications of the ACM*, Vol. 21, 1978, pp. 120-136.
- G. Lowe, "An attack on the Needham-Schroeder public-key authentication protocol," *Information Processing Letters*, Vol. 56, Issue 3, Nov. 1995, pp. 131-133.

Reading Assignments Since Midterm I (cont'd)

- NIST Special Publication 800-22 Revision 1a, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," Rukhin et al., April 2010, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf
- Federal Information Processing Standards (FIPS) Publication 197, "ADVANCED ENCRYPTION STANDARD (AES)," November 2001, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
- Chapter X: PUF-Based Authentication, Jim Plusquellic – Univ. of New Mexico, http://ece-research.unm.edu/jimp/HOST/book_chapters/authentication.pdf

Syllabus Module 1 Topic Covered

- Entropy & randomness

Syllabus Module 2 Topic Covered

- AES

Syllabus Module 3 All Topics Have Been Covered

- PUF construction classes
- PUF entropy sources
- PUF metrics & attacks including machine learning
- Practical considerations including current status