

Exam Review / Comments on Topics Covered and Relationships

Cryptographic Hardware for Embedded Systems

ECE 3170

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Outline

- Reading List
- After Midterm I
- Prior to Midterm I

Outline

- Reading List
- After Midterm I
- Prior to Midterm I

Reading Assignments

- Chapters 1, 2, 3, 7, 9, 11, 12, 14 part 10 only, 17, 18 and 19 of the course textbook by Schneier
- Chapter 3 of the optional textbook by Katz and Lindell
- 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>
- Appendix A and Chapters 1, 4, 5, 6, 7, 8, 9 and 10 of the book on power analysis by Mangard et al.
- Five papers: WDDL, DES DPA, MDPL, Messerges and Plusquellic
- NOTE that you are responsible for everything that is explained in lecture!!!

Outline

- Reading List
- After Midterm I
- Prior to Midterm I

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 & hamming weight dependent microcontroller power (Lecture 21)
 - Energy consumption in silicon and processors (Lecture 22)
 - Covariance and correlation (Lecture 23)
 - Simple Power Analysis (Lecture 24)

Basics (cont'd)

- Questions to consider (additional)
 - How specifically are different power traces gathered and what is their design in order to reveal the information claimed to have been learned? (Lecture 27)
- Differential Power Analysis
 - Difference of Means (Lecture 28)
 - Power trace collections and 5 steps common to all DPA (Lectures 29 and 34)

Countermeasures to DPA

- Introduction to Hiding (Lecture 25)
- WDDL (Lecture 26)
- Masking: DES and DPA (Lecture 32)
- MDPL (Lecture 33)
- 2nd Order DPA (Lecture 34)
- Messerges paper on 2nd Order DPA (Lecture 35)

Hardware Trojans

- Hardware Trojans
 - Lectures 36 and 37

Outline

- Reading List
- After Midterm I
- Prior to Midterm I

Reading

- The following reading has been assigned in the prior lecture notes
 - Chapters 1, 2, 3, 7, 9, 11, 12, 14 part 10 only, 17 parts 4 and 6 only, 18 and 19 of the course textbook by Schneier
 - Chapter 3 of the optional textbook by Katz and Lindell
- The following reading has been recommended for your general knowledge but is not assigned
 - NIST Special Publication 800-22 Revision 1a, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic s,” Rukhin et al., April 2010, <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf>
- NOTE that you are responsible for everything that is explained in lecture!!!

Notation from Schneier

- C_i is ciphertext message i
- P_i is plaintext message i
- E_k is encryption with key k
 - Note that E could be symmetric or asymmetric
 - $E_k(P_i) = C_i$
- D_k is decryption with key k
 - Note that D could be symmetric or asymmetric
 - However, for asymmetric cryptographic, need distinct keys
 - E_{k1} and D_{k2} where $k1$ is the public “key” and $k2$ is the private “key”
 - $E_{k1}(P_i) = C_i$
 - $D_{k2}(C_i) = P_i$
- $\{X\}$ is a set of elements of type X
- $|$ is “such that”; e.g., integer $i \mid 3 < i < 5$ implies that $i = 4$

Notation from Katz and Lindell

- $\{X\}$ is a set of elements of type X
- m is a message in plaintext
 - m is composed of smaller blocks m_i suitable for individual encryption steps
 - $m = \{m_i\}$
- c_i is ciphertext corresponding to message block m_i
- c is ciphertext corresponding to message m
- Enc_k is encryption with key k
 - $c \leftarrow Enc_k(m)$
- Dec_k is decryption with key k
 - $m \leftarrow Dec_k(c)$
- MAC_k is generation of a message authentication code t with key k
 - $t \leftarrow Mac_k(m)$ or, alternatively, $t \leftarrow Mac_k(c)$
- $\langle a, b \rangle$ is a concatenation of a followed by b

Basics

- Terminology, attacks (e.g., CCA), standards
 - Cryptography I (Lecture 2)
- Birthday attack
 - Cryptography II (Lecture 3)
- Data Encryption Standard (Lecture 4)
- Asymmetric cryptography using RSA (Lecture 5)
- Number theory, complexity, Galois field (Lecture 6)
- Authentication I (Lecture 7)
 - Entity authentication
 - Message integrity
 - Nonrepudiation
 - Protocols, Man-in-the-Middle, Replay and Spoofing attacks

First Step (Just One Step up from the Basics)

- Hash functions (Lecture 8)
 - One-way
 - Example: MD5
 - Three different types of “resistance”
 - Relationship between the three
- Encryption modes: ECB and CBC (Lecture 9)
 - Issues: initialization vector, ciphertext stealing
- Theory of cryptography using block ciphers (Lecture 10)
 - Confusion and diffusion
 - S-box and permutation
 - Feistel networks
- Message Authentication Codes and three Encryption + MAC options
 - Different ways to encrypt a message and authenticate its integrity (Lecture 11)

Second Step up from the Basics

- Number theory, complexity, Galois field (Lecture 6)
- Digital signatures (Lecture 12)
- Advanced Authentication (Lecture 13)
- CCA attacks on some ciphers (Lecture 14)
 - Note the use of a theoretical construct called an “oracle” as well as unlimited errors
- Key length (Lecture 15)

Third and Final Step up from the Basics

- Using a Block Cipher as a MAC (Lecture 16)
- Shift registers, feedback and hash properties (Lecture 17)
 - Maximum length sequence, primitive polynomial
 - Context: digital systems test (Lecture 18)
- NIST tests for randomness (Lecture 19)