Cryptographic Engineering
ECE 5580 / CS 5580
ECE is the Home Department

I. Catalog Description

Implementation of cryptographic operations and protocols in contemporary computing platforms. Mapping of cryptographic operations, evaluation and optimization of performance and implementation cost, analysis of security against brute-force cryptanalysis and implementation-level attacks. Design of countermeasures against implementation-level attacks, security-testing procedures, and architectures to support a trusted computing base. Pre: 5560 or CS 5560 (3H, 3C).

Course Number: 5580 / CS 5580

ADP Title: Cryptographic Engineering

II. Learning Objectives

Having successfully completed this course, students will be able to:

- Implement common cryptographic operations in contemporary computing platforms.
- Compare performance-evaluation techniques and optimization techniques for the implementation of cryptographic operations.
- Analyze countermeasures to thwart implementation-level attacks on cryptographic operations in hardware and software.
- Evaluate security-testing procedures for the implementation of cryptographic operations.
- Identify the architectural elements that constitute a trusted computing base.

III. Justification

Cryptography is fundamental to ensure trustworthiness of computing in everyday operations, touching every operational aspect of the information society. Computer scientists and engineers therefore have a need to handle and optimize cryptographic implementations with an eye on efficiency and effectiveness. This course discusses techniques for cryptographic engineering in contemporary computing platforms. One aspect of this study is the efficient implementation to meet the performance and cost requirements of computing platforms from handheld computing devices to server-level computers. It includes study of specialized architecture elements that form the trusted computing base. A second aspect is the analysis of implementation attacks, which are a particular concern when attackers have knowledge of, or access to the low-level implementation of cryptographic operations in computing devices. A related aspect is the study of

security testing procedures to certify platforms. The material is therefore relevant to research as well as to design practice.

The course requires the background material in cryptographic algorithms covered in 5560 / CS 5560. The course is taught at the graduate level for students pursuing research in cryptographic applications. The course reviews state-of-the-art research in secure computing platforms and cryptographic engineering and requires independent literature study.

IV. Prerequisites and Corequisites

Pre: 5560 / CS 5560.

V. Texts and Special Teaching Aids

Required Texts: None.
Cryptographic Engineering is a newly developed and rapidly evolving discipline for which a comprehensive text has not yet been written. In lieu of a required text, the course content will be based on recently published papers, standards, and reference documents such as those listed as required course materials.

Required Course Materials: The instructor will provide a collection of relevant conference and journal papers, as well as standards and reference documents in this field. Example papers are listed below:

- S. Erdem, T. Yanik, and C. Koc, "Fast Finite Field Multiplication," pp. 75-104, Chapter 5 in "Cryptographic Engineering," ed. C. Koc, Springer, 2009. doi: 10.1007/978-0-387-71817-0_5.
- W. Schindler, "Evaluation Criteria for Physical Random Number Generators," pp. 25-54, Chapter 3 in "Cryptographic Engineering," ed. C. Koc, Springer, 2009. doi: 10.1007/978-0-387-71817-0_5.
- D. J. Bernstein, "Curve25519: New Diffie-Hellman Speed Records," PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, (PKC 2006), pp. 207-228, Eds. M. Yung, Y. Dodis, A. Kiayas, and T. Malkin, Springer LNCS 3958, 2006, doi: 10.1007/11745853_14.
- P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to Differential Power Analysis," Springer Journal of Cryptographic Engineering, Vol 1(1): pp. 5-27, 2011, doi: 10.1007/s13389-011-0006-y.
- C. Clavier, "Attacking Block Ciphers," 19-35, Chapter 1 in "Fault Analysis in Cryptography," eds. M. Joye and M. Tunstall, Springer, 2012, doi: 10.1007/978-3-642-29656-7_2.

VI. Syllabus

Course Topics	Percent of Course
Implementation of Finite Field Arithmetic	15%
Implementation of Symmetric-Key and Hash Building Blocks	10%
Implementation of True and Pseudo Random Number Generators	5%
Implementation of Public-Key Operations	10%
Optimization for High-Performance and Lightweight Cryptography	5%
Cryptanalytic Machines	5%
Side-channel Analysis and Side-channel Resistant Design	15%
Fault Analysis and Fault Detection	15%
Security Testing Procedures	10%
Building Blocks of a Trusting Computing Base	10%
Total	100%