ECE/CS 5580 Cryptographic Engineering
Spring 2016

Instructor:	Patrick Schaumont
Office:	Durham 337
E-mail:	schaum@vt.edu
Office Hours:	R 1:00P-3:00P
TA:	Nahid Farhady Ghalaty
TA Office:	SWEL
E-mail:	farhady@vt.edu
Office Hours:	M 12:30P-2:30P
Class Time:	TR 9:30A-10:45A
Class Location:	Durham 261
Class Website:	http://scholar.vt.edu

1 Objectives

Cryptography plays a fundamental role in the practical implementation of information security, needed in a vast range of applications from safe banking using electronic credit cards, over user privacy in medical record storage, up to protecting a nation state from electronic theft and cyber-attacks. With the Internet of Things, cryptographic implementations will be found over an ever wider range of computing architectures and performance budgets.

The central question addressed in this course is *how we can build efficient and secure cryptography?* One aspect of this study is the efficient implementation to meet the performance and cost requirements of computing platforms from handheld computing devices to serverlevel computers. This includes the 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 lowlevel implementation of cryptographic operations in computing devices.

Topics covered in the course include the implementation of Finite Field Arithmetic, Symmetric-Key and Public-Key operations; design and testing of True and Pseudo Random Number Generators; Optimization techniques for High-Performance and Low-Footprint Cryptography; Design of Cryptanalytic Machines; Sidechannel and Fault Analysis Techniques; Countermeasures; and Security Testing Procedures.

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.

2 Prerequisites

- ECE/CS 5560 (Fundamentals of Information Security). Students who have not taken this course have to contact the instructor before proceedings.

3 Text and References

- The class material will come from several text books and seminal publications. There will be a source reference with each lecture. The key references (text books and seminal publications) will be available online.
- The proceedings of the yearly workshop on Cryptographic Hardware and Embedded Systems (CHES) carry state-of-the-art results relevant to handheld computer security. CHES was held each year from 1999. URL: http://dblp.uni-trier.de/db/conf/ches/index.html
- Journal publications and conference publications can be retrieved through several portals, depending on the publisher.

  - IEEExplore for papers published by IEEE.
    URL: http://ieeexplore.ieee.org/
  - ACM Portal for papers published by ACM.
    URL: http://portal.acm.org
  - IACR ePrint archive for papers published by IACR.
    URL: http://eprint.iacr.org
  - A comprehensive catalog of IACR proceedings is kept by J. Muir at Carleton.
    URL: http://www.ccsl.carleton.ca/ jamuir/crypto_springer.php
  - LNCS for papers published by Springer.
    URL: http://www.springerlink.com/content/105633/

4 Course Work

As a student in *Cryptographic Engineering*, you will be involved in research and design aspects of cryptographic components. The format of the course is as follows.

- There will be a **regular lecture series** taught by the instructor to introduce major topics in cryptographic engineering. We will cover implementations for finite-field arithmetic, symmetric-key (AES) and public-key (ECC) cryptography, and random number generation. We will also discuss implementation attacks (passive and active) and countermeasures for them. Finally, we discuss platform implementation issues: optimizations for high-performance and 'lightweight' cryptography, security testing, and trusted computing platforms.
- There will be a **student class presentation** series to present selected research papers on the topics discussed in the regular lecture series. The research papers will be assigned by the instructor. All students (in groups of 3 students) will need to take part in a presentation of about 30 minutes. Both the presenters as well as the audience will be graded, in the following manner. At the start of each presentation, the instructor will randomly assign one or more students as presentation-evaluator(s). The student evaluator needs to prepare a written summary of the presentation, including an assessment of presentation style,

clarity and overall quality. The evaluator will submit the report to the instructor and will be graded on the submitted report.

- There will be a **single research project**, implemented as a group effort. Each group will count at least 3 students. The assignment consists of a cryptographic design problem (see further under Problem Definition). The project will be implemented in three phases: capturing of the functional specification; mapping to target platform; and optimization. The objective of this research project is to approach and, if feasible, outperform state-of-the-art as document in contemporary literature.

  Each group will need to document the results for each phase in a report. This report will be graded for the entire group. The final report will be reviewed as a conference submission (ie. the instructors will look for external reviewers, who are experts in this field).

  Each group will also maintain a blog and document weekly progress. There needs to be at least one blog entry every week. Each blog entry is written by a single, identifiable group member. The blog server will remain private within the class, but will be open for every student enrolled in the class. Participation and discussion will be encouraged and graded.

5 Grading

Grades are assigned throughout the semester, based on the Course Work delivered during the course project, the presentations, and the class engagement. Your graded is determined by a mix of group work and individual effort.

Item	Graded	Graded	Grade %
Item	per group	per student	Grade %
In-class Presentation	X		20 %
Presentation Evaluation Report		X	10 %
Project Report 1	X		10 %
Project Report 2	X		10 %
Project Report 3	X		20 %
Blog Entries		X	15 %
Blog Comments		X	15 %

6 Honor Code Policy

Adherence to the Virginia Tech Honor Code is expected in all phases of this course. Any work that you submit for a grade must be your own, or that of the group in case of the Project. In particular, proper citation of external source code material is essential.

See http://ghs.grads.vt.edu for information about the Graduate Honor System.

Abuses of the Honor Code Policy include for example cheating on Quizzes and plagiarism in presentations and project work. Such violations will be reported to the Office of the Honor System.

7 Special Needs

- Reasonable accommodations are available for students who have documentation of a disability from a qualified professional. Students should work through Services for Students with Disabilities (SSD) in 152 Henderson Hall. Any student with accommodations through the SSD Office should contact the instructor during the first two weeks of the semester.

- If participation in some part of this class conflicts with your observation of specific religious holidays during the semester, please contact the instructor during the first two weeks of class to make alternative arrangements.

- If you miss class due to illness, especially in the case of an exam or some deadline, see a professional in Schiffert Health Center. If deemed appropriate, documentation of your illness will be sent to the Deans Office for distribution to the instruction.

- If you experience a personal or family emergency that necessitates missing class, contact the Dean of Students at 231-3787 or see them in 152 Henderson Hall.

8 Tentative Schedule

Week	Date	Lecture	Topic	Blog	Presentation	Report
1	19 Jan	R1	Introduction			
	21 Jan	R2	Prime Field Arithmetic			
2	26 Jan	R3	Modular Multiplication			
	28 Jan	R4				
3	2 Feb		*no lecture*	B1		
	4 Feb	R5	Multiprecision Arithmetic			
4	9 Feb		*no lecture*	B2		
	11 Feb	R6	AES			R1
5	16 Feb		(partial class/discussion)	B3		
	18 Feb	R7	AES-GCM			
6	23 Feb	R8	Random Number Generation	B4		
	25 Feb	R9	AES on MSP-430			
7	1 Mar	R10	Bitslice Arithmetic	B5		
	3 Mar	P	Project Status Report			
8	8 Mar		Spring Break			
	10 Mar		Spring Break			
9	15 Mar	R11	Side-channel Analysis	B6		
	17 Mar	P	Guest Lecture: Doubling Attack			R2
10	22 Mar	R12	Countermeasures	B7		
	24 Mar	P			P3*, P4	
11	29 Apr	R13	ECC	B8		
	31 Mar	P			P1*, P2*	
12	5 Apr	R14	Hash-based Signatures	B9		
	7 Apr	P			P7, P8*	
13	12 Apr	R15	Lightweight Crypto	B10		
	14 Apr	P			P9*, PA*	
14	19 Apr	R16	Trusted Computing Base	B11		
	21 Apr				PB*, PC*	
15	26 Apr	R17	Guest Lecture: TBD	B12		R3
	28 Apr		Project Discussion			
16	3 May	R19	Project Discussion			

R*i* lectures are *regular* lectures.

P lectures are *research presentation* lectures.

9 Organization of the Project

- Please refer to a separate document, posted on scholar, for the project timeline, and grading criteria we will use.

10 Organization of the Research Presentations

- Please refer to a separate document, posted on scholar, for a list of research papers, and the grading criteria to use for the presentation evaluations.