CS 290g Cryptographic Engineering

Spring Term 2015
http://cs.ucsb.edu/~koc/cren
Monday & Wednesdays 3:00-4:50pm

Description

Cryptography provides techniques, mechanisms, and tools for private and authenticated communication, and for performing secure and authenticated transactions over the Internet as well as other open networks. It is highly probable that every single bit of information flowing through our networks will have to be either encrypted and decrypted or signed and authenticated in a few years from now.

This infrastructure is needed to carry over the legal and contractual certainty from our paper-based offices to our virtual offices existing in the cyberspace. In such an environment, server and client computers as well as handheld, portable, and wireless devices will have to be capable of encrypting or decrypting and signing or verifying messages. That is to say, without exception, all networked computers and devices must have cryptographic layers implemented, and must be able to access to cryptographic functions in order to provide security features. In this context, efficient (in terms of time, area, and power consumption) hardware and software structures will have to be designed, implemented, and deployed. Furthermore, general-purpose (platform-independent) as well as special-purpose software implementing cryptographic functions on embedded devices are needed. An additional challenge is that these implementations should be done in such a way to resist cryptanalytic attacks launched against them by adversaries having access to primary (communication) and secondary (power, electromagnetic, acoustic) channels.

This course is designed for computer science, computer engineering, electrical engineering, and mathematics students interested in understanding, modeling, designing, developing, testing, and validating cryptographic software and hardware. We study algorithms, methods, and techniques in order to create state-of-art cryptographic embedded software and hardware using common platforms and technologies.

Topics

**Block Cipher and Hash Algorithms:** Introduction to block ciphers and AES and hash algorithms. Efficient AES software implementations. Specialized hardware for secret key algorithms. Design methods for secret-key cipher and hash algorithms. Block cipher modes of operation and their implementation on reconfigurable hardware devices. Secure and efficient implementations of symmetric cryptographic primitives in reconfigurable hardware devices.

**Multi-precision Integer Arithmetic:** Arithmetic with large numbers. Exponentiation algorithms and addition and subtraction chains. Non-adjacent forms. Montgomery multiplication. Hardware and software implementation of arithmetic methods for cryptographic applications.


**Public-Key Cryptography:** Software and hardware realizations of modular arithmetic and finite fields. Fundamentals and algorithms for public-key cryptography RSA, Diffie-Hellman, and elliptic curve cryptography and discrete logarithms. Cryptanalysis of public-key cryptographic algorithms key length issues for public-key cryptographic algorithms. Cryptographic co-processors.

**Deterministic and True Random Number Generators:** Random number generators (RNGs) for cryptographic applications. Deterministic and true RNGs. Design of deterministic RNGs. Design and evaluation criteria for physical random number generators.

Course Plan and Project

This course is open for all graduate students; undergraduate students who have taken cs178 or have the basic knowledge of cryptography. There will be 5 homework assignments. Participants are required to engage in a project (in a group) which will be the majority of their work. Participants are expected to study, investigate, or implement and then write a paper or presentation using \LaTeX. There are essentially 3 types of projects:

Tutorials: Pick a topic, and find several papers covering it, study and understand them well, and then write a short tutorial or survey paper or presentation.

Hardware or software implementation: Pick an algorithm and a platform and implement the algorithm with a particular set of objectives in mind (speed, security, or power). Create the software and write a short presentation in addition to the usual design disclosure.

Original work: It is not at all unlikely that you have discovered (or, you will discover) a new method, algorithm, implementation technique, or improve an existing one. If you do, write a paper describing your method or technique.

Course Material

- Technical reports, journal papers, and conference proceedings will also be provided.

Instructor

Professor Koç (pronounced as “Coach”) is the co-founder of the CHES (Cryptographic Hardware and Embedded Systems) Workshop which is the premiere conference covering hardware and software realization aspects of cryptography and security. He is also the founding editor-in-Chief of the Journal of Cryptographic Engineering, the most comprehensive source of high-quality scientific articles on methods, techniques, tools, implementations, and applications of research in cryptographic engineering. Koç is the co-author of the books Cryptographic Algorithms on Reconfigurable Hardware and Cryptographic Engineering, published by Springer. In addition to contributing to 6 conference proceedings as co-editor, he has also authored or co-authored more than 150 journal and conference papers, and 13 US patents. He is an IEEE Fellow, for contributions to cryptographic engineering.

Çetin Kaya Koç
koc@cs.ucsb.edu
http://cs.ucsb.edu/~koc