EEL 5934 Cryptographic Engineering

Credits: 3 credits

Textbook, Title, Author, and Year: NA

Reference Materials: Will be provided in the classroom.

Specific Course Information
Catalog Description: This course provides application perspective of cryptography and focuses on the computations, engineering, and secure implementations. This is a course for students interested in hardware and software design in industry and real-world security and cryptographic applications. The course is devoted to the state-of-the-art in cryptographic hardware/software and embedded systems. The students will learn about computational algorithms and architectures as well as about cryptanalysis of the cryptographic devices. The students will re/learn programming of cryptographic primitives on ASM, C, and hardware (using VHDL). Real world applications include implementations on cellphones, FPGA, and IoT devices with 8-bit/16-bit microcontrollers.

Prerequisites: Discrete Mathematics (MAD 2104) or permission of the instructor.

Specific Goals for the Course: This is a cryptography engineering course. The students learn about embedding cryptographic algorithms and architectures into security products such as embedded devices where they can use programming to prototype to verify and demonstrate concepts. They will learn about implementations on hardware and software platforms including FPGAs and CPUs.

Brief List of Topics to be Covered:

- Mathematical background: Number theory, abstract algebra, Finite fields.
- Finite Field and Modular Arithmetic, Prime fields and binary extension fields.
- Representation of finite field elements: Polynomial basis, Normal basis.
- Exponentiation over finite fields.
- Trace and half trace function over finite fields.
- Multiplication over finite fields, super-serial, bit-level, digit-level, bit-parallel, Karatsuba, Subquadratic multipliers, Systolic array multipliers, hybrid-double multipliers.
- Multiplicative Inversion, Fermatt's little theorem, Extended Euclidean Algorithm.
- Public key cryptography, RSA, Elliptic curve cryptography.
- Group law, group operations, Point multiplication, coordinates systems.
- Security-level and key size.
- Standardized finite field arithmetic and elliptic curve cryptography.
- Post-quantum cryptography Hardware and software aspects.