ENEE 759O
Cryptography Against Physical Attacks

Time/Place: Tues 11:00am-1:50pm, AVW 2446
Credits: 3

Instructor: Dana Dachman-Soled
Email: danadach@ece.umd.edu

Course Goals: Traditional cryptographic models capture basic security guarantees and allow us to give mathematical proofs of security for constructed schemes. Often, however, cryptographic models do not capture real-life attacks such as timing attacks, power analysis attacks and fault injection attacks. In the past few years, there has been a huge effort in the field to introduce new models that allow us to give rigorous security proofs even against attackers who may launch so called "physical attacks" in addition to traditional, black-box attacks on cryptographic schemes. In this course, we will survey some of this recent literature. Topics will include constructing basic cryptographic primitives such as public key encryption and signatures schemes resilient against bounded and continuous leakage attacks, constructing basic cryptographic primitives secure against limited tampering attacks, and a more general approach of constructing compilers that allow the conversion of any circuit into one that is resilient against leakage and/or tampering.

Course Prerequisites:
Co-requisite: EENE641 or CMSC651, or permission of the instructor (see below for the topic prerequisites).

Topic Prerequisites:
Familiarity with basic notions from discrete math, algorithms and theory of computation.

Textbooks:
None

References:
Books:

1. "Introduction to Modern Cryptography: Principles and Protocols" by Jonathan Katz and Yehuda Lindell.
2. "Foundations of Cryptography" by Oded Goldreich, Vols I and II. Drafts of most chapters can be found online at: http://www.wisdom.weizmann.ac.il/~oded/foc-drafts.html.

Conference Proceedings:

1. Springer: Advances in Cryptology (CRYPTO, EUROCRYPT and ASIACRYPT)
2. Springer: Theory of Cryptography (TCC)
3. IEEE Computer Society: Symposium on Foundations of Computer Science (FOCS)
4. ACM: Symposium on Theory of Computing (STOC)

Core Topics:

1. Introduction to Cryptography:
    a. Basic cryptographic primitives and security models
    b. Basic constructions and security proofs
2. Symmetric Cryptographic Primitives secure against leakage
    a. Constructions of: Stream Ciphers, Block Ciphers
3. Cryptographic primitives secure against bounded leakage
    a. Introduction to the model
    b. Constructions of: Public Key Encryption and Digital Signatures in this model.
4. Cryptographic primitives secure against continual leakage
    a. Introduction to the model
    b. Constructions of: Public Key Encryption and Digital Signatures in this model.
5. Cryptographic primitives secure against continual tampering (and leakage)
    a. Introduction to the model
    b. Constructions of: Public Key Encryption and Digital Signatures in this model.
6. Compilers for leakage and tampering
    a. Constructions of tampering and/or leakage compilers for memory
    b. Constructions of leakage compilers for circuits
    c. Constructions of tampering compilers for circuits

Optional Topics:

1. Leakage Resilient Zero Knowledge
2. Leakage Resilient Secure Multiparty Computation
3. Cryptography with Auxiliary input
4. Impossibility Results and Lower Bounds for Leakage and Tampering

Course Structure:

This course is split into three parts: In the first part, regular lectures are given. During this period, students start reading technical articles and select their project topics. In the second part, students present papers in class and report on the progress of their projects. Finally, at the end of the semester students present their projects. Extensive reading of research papers is required; students are expected to be actively involved in class during all three parts of the course.

Grading Method:

The grading will be based on the student's paper presentation, research project and class participation.