Computer Science 395T - Fall 2014
Computing Cryptographic Data

Instructor: Brent Waters
Office: GDC 6.810
E-mail: bwaters@cs.utexas.edu
Office Hour: Monday after class

TA: Venkata Koppula
Email: k.venkata.vk@gmail.com
Office Hours: Tuesday 3:00-4:00, Friday 3:00-4:00
Location: GDC 1.302, Desk 1

Class: Monday, Wednesday 11:00-12:30 in GDC 2.210

Course Topics Cryptographic program obfuscation allows a party to take in a program description P and create an "obfuscated" version of it. This new program behaves equivalently to the original program, but provably leaks as little as possible about its internals. For many years achieving expressive and secure program obfuscation remained an elusive goal. However, less than two years ago the first mathematically sound candidates appeared. Since then obfuscation has taken the cryptographic research world by storm. In this course we will learn about what obfuscation is, how we can build it and what we can do with it. The course will focus on recent research work in the area.

Course Components The course will consist of the following components:

- Paper synopsis and analysis: Roughly once a week, we will discuss a paper from recent literature. Students must submit a 1.5-2 page analysis of the paper, describing the strengths, weakness and open directions. This report must be submitted before the paper is discussed in class. A satisfactory/non-satisfactory grade will be assigned for each submission.
- Problem Sets: There will be 3 problem sets assigned.
- Conference Presentation: Towards the end of the course, each student will choose a paper and give a twenty minute presentation.

Grading Policy Course grades will be based on the components above and course participation.

Supplemental Material There is no required textbook for this course. However, "Introduction to Modern Cryptography" by Katz and Lindell can be used for reference. Additionally, some of the background material will be covered during the office hours if required.

Course Overview The following is a tentative schedule for the course.

- Advanced Encryption Schemes

    1. Public Key Encryption from LPN assumption
    How Practical is Public-Key Encryption Based on LPN and Ring-LPN?
    (Ivan Damgård and Sunoo Park)

2. Identity Based Encryption
   Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles
   (Dan Boneh and Xavier Boyen, Eurocrypt 2004)
3. Attribute Based Encryption
   Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data
   (Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, CCS 2006)

- Candidate Schemes

4. Witness Encryption
   Witness Encryption and its Applications
   (Sanjam Garg, Craig Gentry, Amit Sahai and Brent Waters, STOC 2013)
5. Indistinguishability Obfuscation
   Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits
   (Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai and Brent Waters, FOCS 2013)

- Using Obfuscation

6. Deniable Encryption and other applications from indistinguishability obfuscator
   How to Use Indistinguishability Obfuscation: Deniable Encryption, and More
   (Amit Sahai and Brent Waters, STOC 2014)
7. One Way Functions from indistinguishability obfuscation
   There is no Indistinguishability Obfuscation in Pessiland
   (Tal Moran and Alon Rosen)
8. Two-round secure MPC
   Two-round secure MPC from Indistinguishability Obfuscation
   (Sanjam Garg, Craig Gentry, Shai Halevi and Mariana Raykova, TCC 2014)
9. Adaptively Secure Functional Encryption
   A Punctured Programming Approach to Adaptively Secure Functional Encryption
   (Brent Waters)
10. Secret Sharing for NP
    Secret Sharing for NP from Indistinguishability Obfuscation
    (Ilan Komargodski, Moni Naor and Eylon Yogev)
11. Multi-party key exchange, traitor tracing and other applications
    Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation
    (Dan Boneh and Mark Zhandry, Crypto 2014)

- Constructing witness encryption from simpler assumptions

12. Witness Encryption from Instance Independent Assumptions
    (Craig Gentry, Allison Bishop Lewko and Brent Waters, Crypto 2014)