Cryptography
Abstracts

Saturday 10:15 – 12:15
Shafi Goldwasser, MIT
Anna Lysyanskaya, Brown University
Alice Silverberg, University of California, Irvine
Nadia Heninger, UCSD

Sunday 8:30 – 10:30
Tal Rabin, IBM Research
Tal Malkin, Columbia University
Allison Bishop Lewko, University of Texas, Austin
Yael Tauman-Kalai, Microsoft Research – New England

Saturday 10:15 – 12:15

On Probabilistic Proofs
Shafi Goldwasser, MIT

ABSTRACT

Flavors and applications of verifiable random functions
Anna Lysyanskaya, Brown University

A random Boolean function is a function where for every input x, the value f(x) is truly random. A pseudorandom function is one where, even though f(x) can be deterministically computed from a small random "seed" s, no efficient algorithm can distinguish f from a random function upon querying it on inputs x1,...,xn of its choice. A verifiable random function (VRF) is a pseudorandom function that can be verified. That is to say, a VRF consists of four algorithms: Generate, Evaluate, Prove, Verify. Alice chooses uses Generate to pick her function f, Evaluate to evaluate it and compute y=f(x), Prove in order to compute a proof p(x) that y is indeed f(x). Bob can then use Verify in order to ascertain that it is indeed the case that y=f(x). At the same time, whenever Bob is not given a proof p(x) for a particular x, no efficient algorithm allows him to determine whether y=f(x) or is random. In this talk I will give a survey of verifiable random functions and their constructions and applications.

Elliptic Curve Primality Tests for Numbers in Special Forms
Alice Silverberg, University of California, Irvine

In joint work with Alex Abatzoglou and Angela Wong, we use elliptic curves with complex multiplication to give primality proofs for integers of certain forms, generalizing earlier work of B. Gross and of R. Denomme and G. Savin who dealt with elliptic curves with complex multiplication by $Q(i)$ and $Q(\sqrt{-3})$.

Lattices in Cryptanalysis and List Decoding of Error-correcting Codes

Nadia Heninger, UCSD

Coppersmith's algorithm is a celebrated technique for finding small solutions to polynomial equations modulo integers, and it has many important applications in cryptography. In this talk, I will show how to use lattices to recover an RSA private key from partial information and to find a large approximate common divisor of several integers. Then we will see how the ideas of this technique can be extended to a more general framework encompassing list decoding of Reed-Solomon, Parvaresh-Vardy, and algebraic-geometric codes. These seemingly different problems are all perfectly analogous when viewed from the perspective of algebraic number theory.

Sunday 8:30 – 10:30

On a Magic of Math in a Key Exchange Protocol

Tal Rabin, IBM Research

ABSTRACT

Public Key Encryption: From Basic Security to Stronger Notions

Tal Malkin, Columbia University

Public key encryption (PKE) allows parties that had never met in advance to communicate over an unsafe channel. The notion was conceived in the 1970s, followed by the discovery that one could provide formal definitions of security for this and other cryptographic problems, and that such definitions were achievable by assuming the hardness of some computational problem (e.g., factoring large numbers). For PKE, the most basic security definition -- semantic security -- guarantees passive privacy, namely that it is infeasible to learn anything about the plaintext from its encryption. However, as cryptographic applications grew more sophisticated, this level of security is often not sufficient, since it does not protect against active attacks arising in networked environments. Much recent work has focused on achieving stronger security notions for PKE, such as protections against adaptive corruptions, man-in-the-middle attacks (malleability), chosen ciphertext attacks, leakage and tampering attacks. I will review some of the main themes in this line of work, focusing on the example of using any basic PKE as a "black box" to construct a non-malleable PKE.

Functional Encryption: Current Systems and Proof Techniques

Allison Bishop Lewko, University of Texas, Austin

In this talk, we will describe some examples of functional encryption and the challenges that arise in proving their security. We will then discuss the methodology of dual system encryption (recently introduced by Waters) and a few of its applications.

Cryptography Robust against Side Channel Attacks
Yael Tauman-Kalai, Microsoft Research – New England

Traditionally, cryptographers assume that the secret keys are totally hidden from the adversary. However, in reality there are various real-world physical attacks, including, timing and power attacks, which allow an adversary to (continually) leak information about the secret keys. In addition, there are various attacks, including heat and EM radiation attacks, which allow an adversary to (continually) tamper with the secret keys.
Recently, there has been a large and growing body of work, which tries to secure cryptographic systems against such, so called, side-channel attacks.

In this talk, I will survey some of these results, and focus on two recent results, which show how to construct cryptographic schemes that are secure even against an adversary that continually leaks (bounded) information about the secret key, and continually tampers with the secret key.

These results are based on joint work with Zvika Brakerski, Jonathan Katz and Vinod Vaikuntanathan, and on joint work with Bhavana Kanukurthi and Amit Sahai.