This course meets on Mondays from 4-5pm and Tuesdays from 3-5pm.

Planned Lectures Until Spring Break

1/22  Introduction to Cryptography
1/23  Complexity Theory Review and Interactive Proofs

1/29  Zero-Knowledge Proofs
1/30  Zero-Knowledge Proofs with auxiliary inputs, composition, and for all of NP

2/05  Proofs of Knowledge and Identification Schemes
2/06  Oblivious Transfer

2/12  Secure Multiparty Computation I
2/13  Secure Multiparty Computation II

2/19  NO CLASS: President’s Day
2/20  NO CLASS

2/26  Signature Schemes
2/27  Balancing Authentication and Privacy: Anonymous Credentials and E-Cash

3/05  Efficient Proof of Knowledge Techniques
3/06  Signatures of Knowledge (and problems with the random oracle model)

3/12  NO CLASS: Spring Break
3/13  NO CLASS: Spring Break

We will resume lectures on Monday, March 19 as usual. The last lecture of the semester is Tuesday, April 24.