CSc 85030: Advanced Cryptography: Digital Currencies

Instructor: Rosario Gennaro
Office Hours: Mondays after class, or by appointment
Course Webpage: `http://www-cs.ccny.cuny.edu/ rosario/csc85030/`

Overview: This class will cover the cryptographic algorithms and protocols that support digital currencies. We will also discuss cryptographic mechanisms for anonymous communication over the Internet. The class will focus mostly on mathematical tools and proofs and therefore is a theoretical class in nature. However we will also cover real-life currencies like Bitcoin, and briefly touch upon networking and systems issues related to deployment of digital currencies. We might even have guest lecturers on policy and legal consequences of the adoption of digital currencies.

Prerequisites: Students are expected to be familiar with the basic concepts of cryptography such as encryption and digital signatures, though we will spend some time reviewing some of this material. More importantly students are expected to have knowledge of basic notions of number theory, probability theory and discrete mathematics. For some of the prerequisites students can consult books such as *Introduction to Algorithms* by T. Cormen, C. Leiserson, R. Rivest and C. Stein (chapter 31 and Appendix C), *A Computational Introduction to Number Theory and Algebra* by V. Shoup (available as free PDF at `www.shoup.net`) and *Cryptography Made Simple* by N. Smart.

Textbook: There is no textbook for the course. At each lecture the instructor will assign readings that students will be expected to have completed by the next lecture. For the Bitcoin part of the course we will loosely follow a textbook draft: *Bitcoin and Cryptocurrency Technologies* by A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder available online at
`https://piazza.com/princeton/spring2015/btctech/resources`

Assignments: Students will be required to

- Take notes for at least one lecture during the semester. The notes will have to be typed up in LaTeX and submitted to the instructor for revisions.
- Read a paper on digital currencies that will not be covered in class and give a presentation at the end of the semester. The student can request the instructor to assign the paper to her/him or suggest her/himself the paper to the instructor for approval.
- Solve the occasional homework that will be assigned during class.

Collaboration on the above assignments is allowed and actually encouraged. In the case of homework: (1) students must write up solution on their own and return individual solutions; (2) students must acknowledge their collaborators; (3) students are allowed to consult the Internet or any other sources, but again they must acknowledge them. In the case of lectures and presentations collaboration must be discussed with the instructor.

Topics: Cryptography Review (2 Lectures). Digital Cash via Blind Signatures (3 Lectures). Anonymous Channels (3 Lectures). Bitcoin (4 Lectures). Applications and Extensions of the Bitcoin Model (2 Lectures).