Graduate Seminar on Topics in Modern Cryptography

Prof. Dr. Nitin Saxena

Wintersemester 2010-11: From Friday, 15th Oct 2010.
Tuesday 1415-1545, LWK Lipschitzsaal, Endenicher Allee 60.
Friday 1215-1345, LWK Lipschitzsaal.
(Sometimes we move to: LWK Hausdorffraum)

Background:
Students who are aware of the basics of computation and basic algebra will find the seminar especially interesting.

Outline:
This seminar will study some basic and advanced topics in Cryptography. Firstly we study the general cryptographic primitives, like - encryption, authentication, digital signature and key distribution. Then we will study some concrete cryptosystems based on - elliptic/hyperelliptic curves, NTRU and Ajtai-Dwork lattices.

The students will be expected to present at least two lectures during the semester. Some topics to choose from are given below (see Reference). To send your choices or to ask for more details contact `ns@hcm.uni-bonn.de`

- Modern Encryption (One-way functions)
- Private-key Cryptography (DES, AES)
- Public-key Cryptography (DH, RSA)
- Hash Functions (SHA, MD)
- Message Authentication (Pseudo-random MAC, Cipher-block MAC)
- Digital Signature (RSA, El Gamal)
- Key distribution (DH, 3-party)
- Protocols (IP, ZKP, Multi-party, E-election)
- Hyper/elliptic Curve Cryptography
- NTRU cryptosystem

- Ajtai-Dwork cryptosystem
- Fully homomorphic encryption using *ideal* lattices.

Reference -

1) *Lecture Notes on Cryptography*, Goldwasser & Bellare. Lecture notes at
`http://cseweb.ucsd.edu/~mihir/papers/gb.pdf`

2) *The state of elliptic curve cryptography*, Koblitz, Menezes & Vanstone. Paper at
`http://www.springerlink.com/content/p54420v066743254/`

3) *An elementary introduction to hyperelliptic curves*, Menezes, Wu & Zuccherato. Paper at
`http://www.math.uiuc.edu/~handuong/crypto/menezes_wu_zuccherato.pdf`

4) *An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU Cryptosystem*, Scholten & Vercauteren. Paper at
`http://www.cosic.esat.kuleuven.be/publications/article-520.pdf`

5) *Lattice-based Cryptography*, Micciancio & Regev. Paper at
`http://www.cs.tau.ac.il/~odedr/papers/pqc.pdf`

6) *Fully homomorphic encryption using ideal lattices*, Gentry. Paper at
`http://crypto.stanford.edu/craig/`