Project Topics

1 Overview

- You can pick a topic from the ones listed here, or choose a topic of your own.
- The last five weeks (starting March 27) will be your presentations. Each of you needs to give two lectures based on your project topic.
- You need to submit a final project report at the end of semester.
- Notify me of your choice of topic by Feb 15. If you are choosing a new topic, send me a brief description and a list of papers you plan to start with.
- For the topics listed as follows, the list of papers is for reference. You are free to choose other papers to start.
- To understand many of these papers, you probably need to read earlier papers cited in the paper to understand them.

2 Searchable Encryption

There are tons of papers in this area. The following are just some of the newer ones.

- D Boneh, B Waters. Conjunctive, Subset, and Range Queries on Encrypted Data. eprint

3 Attribute-Based Encryption

Read modern attribute-based encryption schemes.


4 Security of MAC


The preliminary version of this paper was entitled Authenticated Encryption in SSH: Provably Fixing the SSH Binary Packet Protocol, and appeared in the Proceedings of the 9th ACM conference on Computer and Communications Security (CCS), ACM, 2002.

• Jongsung Kim and Alex Biryukov and Bart Preneel and Seokhie Hong. On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1. Cryptology ePrint Archive: Report 2006/187

5 Software Protection

Read both the practical and theoretical side of software protection.

6 Cryptographic Notions of Privacy

The goal is to read on cryptographic notions of privacy in statistical databases and privacy-preserving data mining, and explore whether they are applicable to the setting of privacy-preserving data publishing.


7 Fuzzy Extractors and Usage of Biometric Data

Fuzzy extractors try to extract the same secret when the input contains noise. There are likely both formal cryptographic treatment, as well as practical algorithms. The following lists a few papers on cryptographic treatment.

8 Misc papers

These could be interesting, and each may lead to reading a few other papers, and could serve as a project as well.