CS655: Cryptography **Spring 2007**

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 a tons of paper in this area. The following are just some of the newer ones.

- M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier and H. Shi. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. Advances in Cryptology - Crypto 2005 Proceedings, Lecture Notes in Computer Science Vol. 3621, V. Shoup ed, Springer-Verlag, 2005.
- R Curtmola, J Garay, S Kamara, R Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. ACM CCS 2006.
- J. Bethencourt, D. Song, and B. Waters. New constructions and practical applications for private stream searching. Oakland 2006.
- D Boneh, B Waters. Conjunctive, Subset, and Range Queries on Encrypted Data. eprint

3 Attribute-Based Encryption

Read modern attribute-based encryption schemes.

- D. Boneh and M. Franklin. Identity Based Encryption from the Weil Pairing. In Advances in Cryptology CRYPTO, volume 2139 of LNCS, pages 213229. Springer, 2001.

- Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, EUROCRYPT, volume 3494 of Lecture Notes in Computer Science, pages 440456. Springer, 2005.

- A. Sahai and B. Waters. Fuzzy Identity Based Encryption. In Advances in Cryptology Eurocrypt, volume 3494 of LNCS, pages 457473. Springer, 2005.

- V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data. In ACM conference on Computer and Communications Security (ACM CCS), 2006.

- J. Bethencourt, A. Sahai and B. Waters. Ciphertext-Policy Attribute-Based Encryption. To appear in Oakland'07.

- M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In ACM conference on Computer and Communications Security (ACM CCS), 2006.

4 Security of MAC

- M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. Advances in Cryptology - Crypto 96 Proceedings, Lecture Notes in Computer Science Vol. 1109, N. Koblitz ed, Springer-Verlag, 1996.

- M. Bellare. New Proofs for NMAC and HMAC: Security without Collision-Resistance. Advances in Cryptology - Crypto 2006 Proceedings, Lecture Notes in Computer Science Vol. 4117, C. Dwork ed, Springer-Verlag, 2006.

- M. Bellare, K. Pietrzak and P. Rogaway. Improved Security Analyses for CBC MACs. Advances in Cryptology - Crypto 2005 Proceedings, Lecture Notes in Computer Science Vol. 3621, V. Shoup ed, Springer-Verlag, 2005.

- M. Bellare, T. Kohno and C. Namprempre. Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm. ACM Transactions on Information and System Security (TISSEC), Vol. 7, Iss. 2, May 2004, pp. 206–241.

  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.

- P.C. van Oorschot. Revisiting Software Protection. ISC 2003.

- Oded Goldreich, Rafail Ostrovsky. Software Protection and Simulation on Oblivious RAMs. JACM 1996.
- On the (im) possibility of obfuscating programs. Crypto 2001.
- Christian S. Collberg. Watermarking, tamper-proofing, and obfuscation-tools for 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.

- Dakshi Agrawal and Charu C. Aggarwal. On the design and quantification of privacy preserving data mining algorithms. PODS 2001.
- Alexandre Evfimievski , Johannes Gehrke , Ramakrishnan Srikant, Limiting privacy breaches in privacy preserving data mining, PODS 2003.
- Irit Dinur and Kobbi Nissim. Revealing information while preserving privacy. In PODS 2003.
- Cynthia Dwork and Kobbi Nissim. Privacy-preserving Datamining on Vertically Partitioned Databases. Crypto 2004.
- S. Chawla, C. Dwork, F. McSherry, A. Smith, and H. Wee, Towards Privacy in Public Databases. Theory of Cryptography Conference, 2005.
- A. Blum, C. Dwork, F. McSherry, and K. Nissim, Practical Privacy: The SuLQ Framework, Principals of Database Systems, 2005.

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.

- Xavier Boyen, Reusable Cryptographic Fuzzy Extractors, in ACM CCS '04, 2004.
- Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure Remote Authentication Using Biometric Data. Eurocrypt 2005.
- Yevgeniy Dodis, Jonathan Katz, Leonid Reyzin, Adam Smith: Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets. Crypto 2006.

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.

- Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Amit Sahai: Cryptography from Anonymity. FOCS 2006.
- Silvio Micali, Rafael Pass, Alon Rosen: Input-Indistinguishable Computation. FOCS 2006.