BU Security Group Doctoral Subject Exam in Cryptography and Information Security, 2012

Professors Canetti, Goldberg, Reyzin, and Triandopoulos

1 Announcement

The Doctoral Subject Exam in Cryptography will take place in November or December of 2012 to be determined by the faculty administering it. The goal of the exam is to test the students' preparedness for conducting research within the security group. Students intending to take the exam should contact Professors Canetti, Goldberg, and Reyzin by the end of September. Post-master's students are expected to pass this exam in their second year; post-bachelor's students can (but are not encouraged to) wait until their third year. Students are strongly encouraged to join forces and organize a reading group to study for this exam.

Structure of the exam: The exam will consist of two parts. The in-class portion will last for 2-3 hours and require basic understanding of all the topics below. Students will also have the option to omit a small fraction of the in-class questions. The second portion of the exam will be a 2-day take home exam (open book) that will consist of more in-depth questions. For the take-home exam, students should prepare to answer questions from Topic 1, as well as any **two** topics from Topics 2–7; these two topics will be chosen in advance, by discussion between the student and advisor.

2 Topics Covered

Below is the list of topics covered. Note that topics may be included in more than one item.

1. The union of the contents of BU CAS CS 538 as taught by Leo in Fall 2010 and by Ran in Fall 2011. The material appears in the online class notes at:
   - `http://www.cs.bu.edu/~reyzin/teaching/cryptonotes/`
   - `http://www.cs.tau.ac.il/~canetti/f08.html`
   - `http://www.cs.tau.ac.il/~canetti/f09-materials/f09-scribe3.pdf`
   - `http://www.cs.tau.ac.il/~canetti/f09-materials/f09-scribe4.pdf`
2. Correctness of outsourced computation: the definition of PCPs and main result (without constructions/proofs) ([Din07, Section 1] has a concise introduction); the Kilian/Micali protocol for succinct arguments for NP [Mic00].
3. Key exchange: the basic Diffie-Hellman protocol (which assumes authenticated communication channels between the parties) and challenges in designing protocols when such channels do not exist, as explained in chapters 1–5 `http://webee.technion.ac.il/~hugo/sigma-pdf.pdf`. The setting of password-based key exchange, as explained in Section 1 of `http://eprint.iacr.org/2010/368.pdf`.
4. Distributed Computing in the presence of faults: Models of synchrony and corruption. Basic protocols and impossibility results for Byzantine Agreement, broadcast, and leader election in synchronous and asynchronous networks, with and without randomization, with and without initial authentication. A good source is [AW04, Chapters 2, 5, 14.1 and 14.3] (the book is available on the shelves of the 135 suite).
5. Real/ideal paradigm for multiparty computation and the problems of composition, as explained in chapters 1–5 of `http://eprint.iacr.org/2006/465`.

6. The definition of k-anonymity. The definition of differential privacy, composition properties, aggregation with Laplace noise, stable transformations [McS09]. The take-home part of this exam will also require knowledge of the local sensitivity and smooth sensitivity [NRS07].

7. Threat models and secure protocols for the following: DNS (DNSec (Section 2 of [AM01]), IP (IPsec (Chapter 19 of [Sta11])), BGP (Secure BGP [KLS00]), HTTP (TLS (Chapter 16 of [Sta11])). No details of protocols are expected, but an understanding of what security risks they are addressing, and how the protocols fit together.

8. The basic principles of the following attacks: buffer overflow (stack-smashing/return-oriented programming), cross-site scripting, side channels (power consumption/timing/caching).

References

[AM01] G. Ateniese and S. Mangard. A new approach to dns security (dnssec). In *Proceedings of the 8th ACM conference on Computer and Communications Security*, pages 86–95. ACM, 2001.

[AW04] Hagit Attiya and Jennifer Welch. *Distributed Computing: Fundamentals, Simulations, and Advanced Topics*. John Wiley and Sons, Inc, 2nd edition, 2004. ISBN 0-471-45324-2.

[Din07] Irit Dinur. The PCP theorem by gap amplification. *J. ACM*, 54(3):12, 2007.

[KLS00] S. Kent, C. Lynn, and K. Seo. Secure border gateway protocol (s-bgp). *Selected Areas in Communications, IEEE Journal on*, 18(4):582–592, 2000.

[McS09] F.D. McSherry. Privacy integrated queries: an extensible platform for privacy-preserving data analysis. In *Proceedings of the 35th SIGMOD international conference on Management of data*, pages 19–30. ACM, 2009.

[Mic00] Silvio Micali. CS proofs. *SIAM Journal on Computing*, 30(4):1253–1298, 2000.

[NRS07] K. Nissim, S. Raskhodnikova, and A. Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 75–84. ACM, 2007.

[Sta11] W. Stallings. *Cryptography and network security, Fifth Edition*, volume 5. Prentice hall, 2011.