600.641 Special Topics in Theoretical Cryptography January 22, 2007

Handout 3: Student Survey

Instructor: Susan Hohenberger

Please return to the instructor. Items (1) and (2) will be used for the mailing list.

Information

1. Name:
2. Email address:
3. I am going to school (circle one): full-time part-time.
4. I am working on my (circle one): undergraduate M.S.S.I. M.S. Ph.D.
5. I am taking this course (circle one): definitely probably maybe no.
6. My major is:

Background

True or False:

1. T or F: I am comfortable with Big O and Omega notation (e.g., $O(k^2 + k)$ and $\Omega(n \log n)$).
2. T or F: IP=PSPACE.
3. T or F: (Basic) RSA encryption is secure against chosen-plaintext attacks, but is not secure against chosen-ciphertext attacks.
4. T or F: In a "zero-knowledge proof" with respect to a language $L \in NP$, an honest verifier accepts only if $0 \notin L$.
5. T or F: The Pedersen commitment scheme is computationally hiding and perfectly binding.
6. T or F: Suppose $\mathbb{G}$ is an algebraic group. If the Computational Diffie-Hellman problem is easy to solve in $\mathbb{G}$, then so is the Decisional Diffie-Hellman problem.

Interests

In the following list, please circle the number of any topic you find particularly interesting. Feel free to add suggestions to the list as well. FLIP PAGE OVER.

1. Encryption

2. Program Obfuscation (i.e., anti-reverse engineering technologies)
3. Database Security (e.g., zero-knowledge sets)
4. Cryptography and Game Theory
5. Theoretical Treatment of Side-Channel Attacks
6. Universal Composibility (UC) Security (i.e., defining security for any environment)
7. Identity-Based Cryptography
8. Elliptic Curves and Bilinear Maps
9. Cryptographic Voting Protocols
10. Cryptography with Imperfect Randomness (e.g., Can wind patterns help me securely choose my secret key?)