COS 433 - Cryptography - Final Take Home Exam

Boaz Barak

December 13, 2005

- Read these instructions carefully *before* starting to work on the exam. If any of them are not clear, please email me before you start to work on the exam.

- **Schedule:** You can work on this exam in a period of 96 hours of your choice between December 15^{th}, 2005 and January 17^{th}, 2005 at 12:00 pm. The exam needs to be submitted to my mail box by January 17^{th}, 2005 noon. *This is a strict deadline.* You may submit the exam earlier. If you typed up your exam, I would appreciate it if you also email me a copy of it at the same time. If you submit it through the mail box earlier than the deadline, please email me to let me know you did so, and email again if I don't acknowledge receipt.

- **Restrictions , honor code:** You should work on the exam alone. You can use your notes from the class, the homework exercises and their solutions, and the handouts I gave in class or put on the webpage. You can also use any personal summaries and notes of the material that you prepare before starting to work on the exam. *You should not use any other material while solving this exam.* You should write and sign the honor pledge on your submitted exam (the pledge is "I pledge my honor that I did not violate the honor code during this exam and followed all instructions").

- **Writing:** You should answer all questions *fully*, *clearly* and *precisely*. When describing an algorithm or protocol, state clearly what are the inputs, operation, outputs, and running time. When writing a proof, provide clear statements of the theorem you are proving and any intermediate lemmas or claims. I recommend that you first write a draft solution of all questions before writing (or preferably, typing) up your final submitted exam.

- **Partial solutions:** If there is a question you can not solve fully, but you can solve a partial/relaxed version or a special case, then please state clearly what is the special case that you can solve, and the solution for this case. You will be given partial credit for such solutions, as long as I feel that this special case captures a significant part of the question's spirit.

- **Polynomial security:** Whenever in this exam we say that a primitive is *secure* under some attack, we mean that it is $(T(n), \epsilon(n))$ secure for $T(n) = n^{\omega(1)}$ and $\epsilon(n) = n^{-\omega(1)}$, where n is the key size/security parameter of the scheme . That is, any adversary that is implementable by polynomial-sized circuit, and attacks the primitive has probability less than $1/poly(n)$ of success (for every polynomial $poly(\cdot)$ and large enough n). The conditions of the attack and meaning of success are of course determined by particular security definition.

- **Assumptions:** You may assume as true any of the axioms/assumptions that were given in class: existence of one-way permutations, commitment schemes, pseudorandom generators, pseudorandom permutations, hardness of factoring random Blum integers, hardness of inverting the RSA permutation, decisional Diffie Hellman, existence of chosen-message (CMA) secure signature schemes, existence of collision-resistant hash functions, existence of chosen ciphertext (CCA) secure encryption schemes, and existence of secure oblivious transfer (OT) and private information retrieval (PIR) protocols. Whenever you use such an assumption, state it clearly and precisely. It is recommended that you review these assumptions and definitions before you start working on this test.

Note on the random oracle model: You can use the random oracle model, but it is preferred that you avoid doing so if possible (you will get at least the majority of points for a valid solution in the random oracle model). If you use as a black-box a CCA secure encryption scheme this does not count as using the random oracle model (even though the only construction we saw for this in class used the random oracle model).

- **Quoting results:** You can quote without proof theorems that were proven in class. However, you should quote them precisely, and state the date and lecture number where the theorem was proven. You can also use the hardcore theorem of Goldreich and Levin, even though it was not fully proved in class. When solving a question, you can use the results of a previous question as given, even if you did not manage to solve it.

- **Clarifications:** I have made an effort to make the questions as clear and unambiguous as possible. In case any clarifications are needed, I will try to be always available by email. You can also email me with your number and good times to call, and I will call you back. If you need me more urgently, you can call me at my cell phone 917-674-6110 between 11am and 10pm EST. You can also reach Dave at his email. Feel free to email me before starting to work on the exam to check my availability in that 96 hour period. If there are any unresolved doubts, please write your confusion as part of the answer and maybe you will get partial credit.