COS 433 - Cryptography - Final Take Home Exam

Boaz Barak

May 2, 2010

- 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 48 hours of your choice between Monday May 3rd 2010 and Friday May 14th 2010 5pm. (i.e., you need to submit the exam either 48 hours after you downloaded it from the website or by Friday May 14 5pm, whichever comes sooner.) *This is a strict deadline.* You may submit the exam earlier.

  Please *type up* the exam, and submit it (as a pdf, postscript, or word doc file) to Boaz, Sushant and Shi by email. If you have a problem with typing up the exam, then please let me know as soon as possible. In this case you should submit *two copies* of the handwritten exam to my mailbox, and also email me, Sushant and Shi at the same time to let us know that you've done so.
- **Restrictions, allowed texts, 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 the Boneh-Shoup, Katz-Lindell, Goldreich and Arora-Barak textbooks as well as Trevisan's lecture notes. You can also use any personal summaries and notes of the material that you prepare on your own or with a group before starting to work on the exam. *You should not use any other material while solving this exam.* When you submit the exam by email, you should also include in the email the honor pledge (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 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.
- **Assumptions:** Unless explicitly said otherwise, you may assume as true any of the axioms/assumptions that were given in class such as: existence of one-way functions and permutations, commitment schemes, pseudorandom generators, functions and 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 a fully homomorphic encryption scheme. 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 unless the question states otherwise, 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 public key 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 or given as a homework exercise. However, you should quote them precisely, and state the date and lecture number or the homework number and question. You *cannot* quote without proof any other results— this includes results that were only stated without proof in class, and results that are proven in the textbooks but not in class. If you do use a proof from another source such as a textbook, you should write the proof in full but also add a reference to the place it appears. 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 609-981-4982 between 11am and 10pm EST. You can also email Sushant and Shi as well. If there are any unresolved doubts, please write your confusion as part of the answer and maybe you will get partial credit.