INTRODUCTION TO MODERN CRYPTOGRAPHY
KU BLOCK 1A, 2016-17

FINAL HOMEWORK
DUE: MONDAY 14/11/2016 8:30AM

GORJAN ALAGIC

Instructions.

This homework assignment is different from the rest. Your goal in this assignment is to learn some aspect of cryptography on your own, and then explain it in a clear, technical piece of writing. Please read the instructions below carefully, and write me if you have any questions.

- *Topic selection.* You have two options for selecting topics:
  (1) Choose a section of Katz and Lindell which you find interesting, but which we have not covered in class. There's a lot to choose from: hash functions, practical constructions, digital signatures, trapdoor permutations, etc.
  (2) Look at the list of "accepted papers" in CRYPTO 2016 and CRYPTO 2015, and find one that you find interesting.

  In either case, you are **not** responsible for explaining the entire section, or the entire paper. For example, it is better to focus on one particular construction of a hash function, rather than trying to explain all of Chapter 5. Or, if the paper you choose gives a new scheme for fully-homomorphic encryption (FHE), you can choose to just talk about basics of FHE: what it is, why it is useful, how to define it, etc. **Once you have selected a topic, e-mail me with a brief summary of what you want to do (with a link to the paper, if you chose one.)**
- *Target audience.* The target audience is a person who just finished our course. So please don't assume familiarity with elliptic curves, computational indistinguishability obfuscation, multilinear maps, etc. Of course, only I will read your paper. But, you should try to write it in such a way that, if you gave it to one of your fellow students, they could read it, understand it, and be excited about it!
- *Requirements.* You must try to make your writing look as neat, clear, and understandable as the Katz and Lindell text. Follow all of their conventions in notation. State **Definitions** and **Theorems** just as they would. Explain things. In particular, you must:
  (1) Typeset your paper properly, with title, author, abstract, and citations;
  (2) Explain the topic *informally* and why it is interesting or useful;
  (3) Explain the topic *formally*, with proper definitions and all relevant details;
  (4) Number your definitions, theorems, and equations, so you can properly refer to them later;
  (5) State and formally prove at least one non-trivial result about the topic. It's ok if this is from the book, so long as you *understand it*, rewrite it and explain it in your own words;
  (6) Conclude with some ideas for where one could go next to read more about your topic.
- *Format.* As stated above, the homework must be typeset. Use 11pt or 12pt font, and reasonable margins. Try to aim for 4-6 pages, plus title page and references. Most of the

4-6 pages should be writing. Avoid overly long and boring calculations; if you must have them, put them in an appendix and refer to the appendix from the main body of the paper.

Department of Mathematical Sciences, University of Copenhagen
E-mail address: galagic@gmail.com