MTAT.07.006 Research Seminar in Crypthography
Comments on the survey "Zero-Knowledge"

Kadri Hendla

November 19, 2005

1 Introduction

The purpose of this document is to give comments on Oleg Koshik's survey "Zero-Knowledge". The survey gives a brief overview of zero-knowledge proofs. Zero-knowledge proofs are interactive methods for proving something to another party without revealing anything else other than the validity of the given statement.

2 General Remarks

The overall impression of the survey is good. It gives the reader a general understanding of zero-knowledge proofs and their applicability. The text is structured logically, first giving the basic background on zero-knowledge proofs, then elaborating them and finally finishing with some examples of their application in cryptography. The survey isn't too technical, but it might be a bit difficult to understand for people with little background in graph theory. The text is generally well-written, although some minor spelling mistakes can be found, some of which are mentioned in the section below.

3 Detailed Comments

The opponent has following remarks on the survey.

1. In the introduction "behaviour" is misspelled as "behaivour".

2. In the chapter "Preliminary Background", the opponent would suggest explaining what the abbreviations P, BPP and NP stand for, for people not familiar with complexity theory.

3. Also in the same chapter, the meaning of the sentence *"We say that algorithm runs in probabilistic polynomial time, if it can flip coins runs in time polynomial in the length of the input."* is unclear.

4. The opponent would also like to know the sources this survey is based on.