

## Handout 3: Fun Problems

*Instructor: Silvio Micali**Teaching Assistant: Rafael Pass*

Below is a (growing) list of “fun” problems mentioned in class.

**Zero-Knowledge**

1. Can you find a *constant-round* zero-knowledge proof for NP that has a *constant* (say  $\frac{1}{2}$ ) soundness error ?
2. Can you say *something* about the security of the “parallelized” version of the Graph 3 Coloring protocol (although it might not be zero-knowledge) ?

**Oblivious Transfer**

1. Try providing a definition of an Oblivious Transfer protocol where the sender wishes to send an *arbitrary* string (and not just the factorization of two numbers, as seen in class)?