22

Proofs and algorithms

> *"Let's not try to define knowledge, but try to define zero-knowledge."*, Shafi Goldwasser.

Proofs have captured human imagination for thousands of years, ever since the publication of Euclid's *Elements*, a book second only to the bible in the number of editions printed.

Plan:

- Proofs and algorithms
- Interactive proofs
- Zero knowledge proofs
- Propositions as types, Coq and other proof assistants.

22.1 *Lecture summary*

22.2 *Exercises*

22.3 *Bibliographical notes*

22.4 *Further explorations*

Some topics related to this lecture that might be accessible to advanced students include: (to be completed)

22.5 Acknowledgements