

# 21

## *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.

### 21.1 LECTURE SUMMARY

### 21.2 EXERCISES

**R** **Disclaimer** Most of the exercises have been written in the summer of 2018 and haven't yet been fully debugged. While I would prefer people do not post online solutions to the exercises, I would greatly appreciate if you let me know of any bugs. You can do so by posting a [GitHub issue](#) about the exercise, and optionally complement this with an email to me with more details about the attempted solution.

### 21.3 BIBLIOGRAPHICAL NOTES

### 21.4 FURTHER EXPLORATIONS

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

## 21.5 ACKNOWLEDGEMENTS