Summary of course material

Zero-knowledge proofs

263-4665-00L

Lecturer: Jonathan Bootle

Notes

- Grey = non-examinable

- Black = examinable
- Blue = can always be stated without proof (if not already given)
- Orange = examinable with prompts (e.g. protocol details given, question asks for analysis)

Week 1

Lecture 1

- Definitions of P, NP
- Definition of interacting algorithms and IP class
- IP for GNI and analysis (completeness, soundness)
- Definition of ZK

Week 2

Lecture 2

- ZKP for GI and analysis (completeness, soundness, ZK)
- Black-box ZK, HVZK
- Indistinguishability, computational, statistical ZK
- Security with auxiliary inputs
- Computational soundness, knowledge soundness
- GI protocol is knowledge sound

Exercise Sheet 2

- Quadratic residues protocol
- Hamiltonian cycle protocol with cards/commitments
- Sudoku protocol

Week 3

Lecture 3

- Public coin proofs
- Trees of transcripts
- Special soundness
- Special soundness => knowledge soundness
- Sigma protocols
- Commitment schemes
- Elgamal and Pedersen
- G3C protocol and analysis
- Parallel repetition of sigma protocols

Exercise Sheet 3

- IP definitions
- Commitment schemes
- GI implementation

Week 4

Lecture 4

- Sigma protocol AND composition
- Sigma protocol OR composition
- MPC protocol definitions and properties
- MPC-in-the-head sigma protocol
- FS heuristic
- Coin-flip protocol
- SHVZK->ZK compiler

Exercise Sheet 4

- Necessity of Prover’s Randomness in ZK Protocols
- ZK for GNI
- ZK for GI

Week 5

Lecture 5

- SHVZK->ZK compiler
- Schnorr protocol and analysis
- Same DLOG, Pedersen, commitment to zero protocols
- VDM matrices invertible
- Multiplication proof

Graded Exercise Sheet

Week 6

Lecture 6

- Multiplication proof
- Non-zero proof
- CSAT proof
- Low degree circuit proof
- (non) membership proof

Exercise Sheet 6

- HVZK<->SHVZK sigma protocols
- Fiat-Shamir Pitfalls
- One-of-many proofs, part a) only

Week 7

Lecture 7

- Sumcheck protocol
- coNP
- Arithmetisation, UNSAT proof
- Layered circuit definition
- MLE existence and uniqueness
- Schwartz-Zippel lemma
- GKR protocol and analysis

Exercise Sheet 7

- Arithmetic circuit decomposition
- ZK with extractable commitments
- Sumcheck for triangle-counting

Week 8

Lecture 8

- Facts about MLEs
- GKR analysis
- Informal defs, PCP, IOP + variants
- R1CS definitions

Exercise Sheet 8

- UNSAT IP efficiency
- IP in PSPACE
- Sumcheck with codes

Week 9

Lecture 9

- R1CS definition
- R1CS IOP and analysis (rowcheck, lincheck, input consistency)
- Poly commitment definitions
- Pedersen scheme and analysis

Graded Exercise Sheet

Week 10

Lecture 10

- Pedersen eval protocol and analysis
- Bilinear pairing maps
- AFGHO commitments

Exercise Sheet 10

- Streaming prover sumcheck
- GKR analysis for binary trees
- R1CS question

Week 11

Lecture 11

- Committed evaluation protocol
- IOP to argument compiler idea
- IOP to argument compiler security sketch
- BPP definition
- NIZK impossibility without CRS
- NIZK syntax and security
- BGN cryptosystem and analysis

Exercise Sheet 11

- AFGHO commitments
- Sumchecks and DLOG polycommits

Week 12

Lecture 12

- NIZK bit proofs and analysis
- CSAT NIZK and analysis
- Lagrange and vanishing polynomials, divisibility
- QAP and strong QAP from R1CS
- Linear PCP for QAP and analysis
- Constant-size NIZK + analysis

Exercise Sheet 12

- Feasibility of NIZKs beyond BPP
- NIZK for QR

Week 13

Lecture 13

- Linear PCP for QAP and analysis
- Constant-size NIZK + analysis

Tips

- GI, QR, HC, G3C protocols are also sigma protocols
- The techniques used to analyse the sigma protocol for low-degree circuits can be used to analyse most of the other DLOG-based interactive protocols
- G3C, HC, MPCitH sigma protocols have similar analysis
- GKR and R1CS IOP have similar analysis