1

Chapter

Introduction

Starting 2018, an incredible amount of progress has been made in this burgeoning area called quantum cryptography. In these notes, my goal is to give you some flavour of these exciting developments. The following is an ambitious and therefore tentative course outline. The basic goal will be to cover Unit 1 and one key result from Units 2, 3 and 4. The remaining units will be covered, depending on the pace of the course.

§ 1.1 Outline

Unit 1: Review:

Primer on quantum formalism. [VW '16]

Lay of the land:

Impagliazzo's worlds: in particular MiniCrypt and Cryptomania

Introduce the main directions:

- (T1) post-quantum cryptography (make classical constructions secure against quantum adversaries),
- (T2) quantum analogues of classical functionalities,
- (T3) functionalities impossible without quantum (excluding those in T2),
- (T4) basing cryptography on quantum complexity

Focus on information theoretic results (T3): key distribution (BB84, Ekert), proof of security, secret sharing, impossibility of bit commitment, impossibility of strong coin flipping, achieving optimal strong coin flipping using weak coin flipping, self-testing CHSH, all bipartite states can be self-tested [VW '24].

Unit 2: (T2) Verification:

Regev's quantum reduction [Regev'09]

Weak quantum verifier: based on MBQC [GKK17]

Classical verifier: assuming LWE is hard, Mahadev [Mahadev 18, Vidick 22]

Classical verifier: two non-communicating provers [RUV 12]

Unit 3: (T2) QFHE: construction and its applications:

Mahadev's QFHE construction [Mahadev 17]

Compiling non-local games [KLVY 23]

Verification assuming QFHE [NZ 23]

Unit 4: (T4) Minimal assumptions: Minicrypt and below

OT is in Miniqcrypt [GLSV 20, BCKM 20]

Crypto despite having NP=P or similar [Kre 21, KQST 23]

Microcrypt Primitive Zoo [Or Sattah]

Unit 5: (T1/T2) Multi Party Computation

(T1) Post-quantum Commitments (collapse-binding commitments) [Unruh'16]

(T1) Post-quantum MPC [HSS 11]

(T2) Quantum 2-PC [DNS '10 and '12]

(T2) Quantum MPC w/ quantum communication [Dulek, Grilo, Jeffery, Majenz, Schaffner]

(T2) Quantum MPC w/ classical communication [Bartusek '21]

Unit 6: (T3) Quantum-only functionalities I

Unclonable encryption: construction in the Random Oracle Model [AKLLZ '22]

Certified deletion [BK '22]

Quantum Pseudorandom unitaries [MH '24]

Unit 7: (T3) Quantum-only functionalities II

Quantum Money and Lightning [Zhandry '17]

iO for pseudo-deterministic functions [BKNY '23]

Unit 8: Bonus/extra reading (references will be provided later)

Other key topics in cryptography:

Interactive proofs

Zero knowledge

Quantum rewinding

Quantum Random Oracle Model

Everlasting security

Connections to physics:

Self-testing using a single quantum device

Non-locality => Proof of quantumness + rigidity

Black hole radiation decoding and commitments

Cryptographic tests of python's lunch conjecture

Computationally bounded theory of entanglement

References

GKK 17: Verification of quantum computation: An overview of existing approaches

VW 24: Introduction to Quantum Cryptography (book)

VW 16: Quantum Proofs (survey)

RUV 12: Classical command of quantum systems

Vidick 22: Course FSMP, Fall'20: Interactions with Quantum Devices

Mahadev 18: Classical verification of quantum computations

Mahadev 17: Classical Homomorphic Encryption for Quantum Circuits

KLVY 23: Quantum Advantage from Any Non-Local Game

NZ 23: Bounding the Quantum Value of Compiled Nonlocal Games: From CHSH to BQP verification

BCKM: One-Way Functions imply Secure Computation in a Quantum World

MH24: How to Construct Random Unitaries

Or Sattah: MicroCrypt Zoo

Kre21: Quantum pseudorandomness and classical complexity

KQST21: Quantum cryptography in algorithmica

DNS '10: Secure two-party quantum evaluation of unitaries against specious adversaries

DNS '12: Actively Secure Two-Party Evaluation of any Quantum Operation

DGJMS '19: Secure Multi-party Quantum Computation with a dishonest majority

Bartusek '21: Secure Quantum Computation with Classical Communication

BK 22: Cryptography with Certified Deletion

HSS11: Classical Cryptographic Protocols in a Quantum World

Unruh'16: Collapse-binding quantum commitments w/o random oracles

AKLLZ '22: On the Feasibility of Unclonable Encryption and more

Zhandry '17: Quantum Lightning Never Strikes the same state twice

MH '24: How to Construct Random Unitaries

BKNY '23: Obfuscation of pseudo-deterministic quantum circuits

Regev '09: On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Video Tutorials:

- Dakshita Khurana: Cryptography with certified deletion
- Mark Zhandry: Security Reductions (multi-part series)

Preferred/reference Textbooks:

There are no textbooks for this course as the material is at the frontier of current research in quantum cryptography. Relevant lecture notes/tutorials/survey articles have already been referenced above.

Resources to review basics of quantum info/computation

- Lecture notes on Quantum Computation by John Preskill (Caltech)
- Introduction to Quantum Information and Computation, MA Nielsen and IL Chuang

Resources to review classical cryptography

- Introduction to Modern Cryptography. Jonathan Katz and Yehuda Lindell.
- Foundations of Cryptography (Volumes 1 and 2). Oded Goldreich.

Other resources

- Zhandry's lecture notes on quantum cryptography