University of Tartu | Prof. Dr. Dominique Unruh

Quantum Cryptography

Exam study guide, fall 2018

Last Update: February 21, 2019

About the exam. The exam will be a written exam. You may not use external tools or notes. You are, however, allowed to bring one page of **handwritten** notes (one **page**, not one sheet!). In the list below, sometimes it says "[Given: xxx]". In this case, you will be given "xxx" as part of the exam question. After the exam has been corrected, you will have to opportunity to look at the correction and, if present, point out mistakes in the correction. A re-exam will be scheduled only if needed.

Things to learn. You should be able to...

- ...reproduce and work with the following definitions from linear algebra: trace, Hermitian, positive, unitary, orthogonal projection, tensor product. Section 1
- ...evaluate simple quantum circuits. I.e., given an initial state and a quantum circuit, compute the final state of the quantum circuit and/or the probabilities of certain measurement outcomes. [Given: Definitions of the individual gates] In particular, you should be able to analyze simple quantum experiments such as the Deutsch-Jozsa algorithm or the bomb tester. Section 4
- ...give a mathematical description of a quantum state given a textual description. (E.g., given "photon 1 is vertically polarized and photon 2 is diagonally polarized", write down the vector representing the state.)
- ...give a mathematical description of a measurement given a textual description. (E.g., given "we measure whether the third photon is horizontally polarized", describe the projectors constituting that measurement.)
- ...convert a measurement described by projectors into one described by subspaces and vice versa.
- ...convert a state in ket-notation (e.g., $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$) into a state in vector notation (e.g., $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$).
- ...give the definitions of the following gates: CNOT, SWAP, controlled-U. Section 5

- ... compute the state of a composite system given the states of individual subsystems. Section 6
- ... apply unitary transformations on a subsystem of a composite system.
- ... apply measurements on a subsystem of a composite system.
- ... write down a quantum state probability distribution given a textual description. (E.g., convert "with probability $\frac{1}{2}$, the qubit is $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, and with probability $\frac{1}{2}$, the qubit is $|0\rangle$" into a quantum state probability distribution.) Section 9
- ... derive the quantum state probability distribution that results from a particular experiment. (I.e., give a list of steps, tell what the state probability distribution is afterwards.)
- ... apply elementary operations to state probability distributions (such as unitary transformations, measurements, and extending the state space).
- ... explain "physical indistinguishability".
- ... transform an state probability distribution into a density operator.
- ... apply elementary operations to density operators (such as unitary transformations, measurements, and extending the state space).
- ... decide whether two given state probability distributions are physically indistinguishable.
- ... convert a density operator in ket-notation (e.g., $\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$) into a state in vector notation (e.g., $\begin{pmatrix} \frac{3}{4} & 0 \\ 0 & \frac{1}{4} \end{pmatrix}$).
- ... compute a partial trace of a given density operator. Section 10
- ... explain the meaning of partial trace.
- ... compute a purification of a density operator. [Given: a decomposition of the density operator into Eigenvectors, e.g., $\rho = \frac{1}{4}|\Phi\rangle\langle\Phi| + \frac{3}{4}|\Psi\rangle\langle\Psi|$.]
- ... apply Lemmas 6, 7, and 8 to compute/bound trace distances. [Given: Lemma 8] Section 12
- ... compute the trace distance of two density operators.
- ... compute a statistical distance given the explicit distributions.
- ... explain the meaning of the trace distance.
- ... create simple security definitions involving the trace distance.
- ... explain the individual steps of the QKD security proof on a high level. Section 13

- ... explain the individual parts of the security definition of QKD. [Given: the definition]
- ... given a protocol that does not satisfy the definition, explain why not (by giving an attack). [Given: the security definition]
- ... given a variant of the security definition in which some part is missing/changed, explain why it is a bad definition (e.g., if it is unfulfillable, say why; if it does not give enough security, give an example protocol that satisfies the definition and an attack that illustrates that the definition is not what we want). [Given: the original security definition]
- ... explain the meaning of min-entropy (classical/quantum). [Given: the definition of min-entropy]
- ... explain the concept of a strong randomness extractor (classical/quantum). [Given: the definition of strong randomness extractors]
- ... apply Definition 47, Lemma 18, Lemma 22, Theorem 8, Lemma 28, or Lemma 29 in computations of bounds on min-entropies or guessing probabilities. (The difference between min-entropy and smooth min-entropy as well as the ε's in H_∞^ε can be ignored.) [Given: the definitions/lemmas/theorems]
- **[REMOVED]** ... explain the definitions of the hiding and binding property for commitments. Section 14
- **[REMOVED]** ... given a commitment scheme that is not hiding, find and explicitly describe an attack against the hiding property. (Assuming there is a simple attack.)
- **[REMOVED]** ... same for binding.
- **[REMOVED]** ... given the Schmidt decomposition of the state of sender and recipient of a commitment after committing to 0 and after committing to 1, describe an attack against the binding property. [Given: definition of Schmidt decomposition]
- **[REMOVED]** ... explain the individual steps of the impossibolity proof of unconditionally secure quantum commitments on a high level. (For the case of zero quantum memory.)
- **[REMOVED]** ... explain the bounded quantum storage model. Section 14.1
- **[REMOVED]** ... discuss the advantages and disadvantages of the bounded quantum storage model.
- **[REMOVED]** ... describe a secure commitment protocol in the bounded quantum storage model.
- **[REMOVED]** ... explain the individual steps of the security proof in the bounded quantum storage model on a high level.
- **[REMOVED]** ... apply Definition 47, Lemma 18, Lemma 22, Theorem 8, Lemma 28, or Lemma 29 in computations of bounds on min-entropies or guessing probabilities. (The difference between min-entropy and smooth min-entropy as well as the ε's in H_∞^ε can be ignored.) [Given: the definitions/lemmas/theorems]

- ... define the factoring problem. Section 17
- ... define the order finding problem.
- ... explain how to solve factoring given a solution for order finding (efficiently).
- ... explain how to do order finding using a quantum computer (efficiently; ignoring issues with approximate results due to the order not dividing N).
- ... explain what it means that the DFT does a frequency analysis (i.e., express this fact as a formula).
- ... given a small LWE instance where the error e is 0, compute s. Section 21
- ... distinguish the different variants of the LWE problem. More specifically, given a description of an algorithm, say which of the LWE problems it breaks (and, if it is clear from the description, with which parameters) [given: Definition 75 (but not Definitions 74, 73].
- ... given a small ciphertext in Regev's cryptosystem where $e = 0$ (no error term), compute the plaintext [given: the definition of Regev's cryptosystem].
- ... explain why Regev's cryptosystem is superior to RSA or ElGamal or similar cryptosystems in a setting where post-quantum security is required.
-