

Final Exam

Date: 2021-05-30

University of Tartu

- The exam is open book. You are allowed to use any materials / textbooks etc. You are not allowed to communicate with others or to google for specific answers to problems written in this exam.
- You can reach a total of 100 points.
- You have 150 minutes for the exam. (Thus, about 1.5 minutes per point.)
- Write your solutions on blank sheets. Make sure that to put your name on **each** sheet. Make sure that you indicate on **each sheet which problem** you are solving.
- Some problems are marked as **bonus points**. These allow you to get points beyond 100 points. However: Bonus points do not count for getting an A (you need to achieve 90% using only non-bonus points). And for getting a B, bonus points count half (you need to achieve 80% of the non-bonus points using non-bonus points and half of the bonus points). For getting C (70%), D (60%), E (50%), and passing (50%), bonus points count fully.
- **Be neat and write legibly.** You will be graded not only on the correctness of your answer, but also on the clarity with which you express it.
- At the end, please photograph your solutions (make sure the focus is good!) and upload them at the link that will be provided in the Zoom call.
- You can use the following table to mark which problems you have solved so that you do not accidentally overlook one (“[]” denotes bonus problems):

Problem:	1					2						3		4	
	(a)	(b)	(c)	(d)	(e)	(a)	(b)	(c)	(d)	(e)	(f)	(a)	(b)	(a)	(b)
Points:	8	8	8	9	[9]	8	8	8	[8]	8	8	9	9	9	[8]
Done?															

- Good luck!

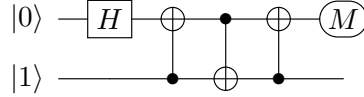
Problem 1: Basics (8+8+8+9+[9]=33+[9] points)

- (a) Consider the unitary transformation defined by $U : |x\rangle|y\rangle = |y\rangle|x \oplus y\rangle$ for all $x, y \in \{0, 1\}$.

Write U as a matrix.

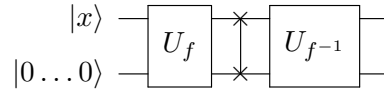
- (b) Compute $U(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle)$.

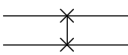
- (c) What is the outcome of the measurement M in the following quantum circuit? (I.e., for each possible measurement outcome, give the probability and the post measurement state.)



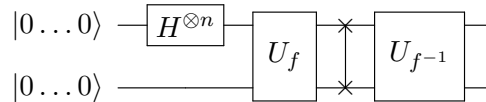
M denotes a measurement of a single qubit in the computational basis. H denotes the Hadamard transform.

- (d) Let $x \in \{0, 1\}^n$. Let f be a permutation on $\{0, 1\}^n$. What is the quantum state that results from applying the following quantum circuit?



Each horizontal line stands for n qubits. U_f is the unitary transformation defined by $U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$. $U_{f^{-1}}$ is the unitary transformation defined by $U_{f^{-1}}(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f^{-1}(x)\rangle$. The symbol  stands for swapping (exchanging) the upper n qubits with the lower n qubits.

- (e) With the notation from (d), what is the final state of the following circuit?



Use (d). Simplify as much as possible!

Problem 2: Ensembles and density operators (8+8+8+[8]+8+8=40+[8] points)

Consider the following three experiments:

- A. Alice chooses a random bit $r \in \{0, 1\}$ and sends $|r\rangle$.
- B. Alice chooses a random bit $r \in \{0, 1\}$ and sends $U|r\rangle$ with $U := \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$.
- C. Alice uniformly chooses $r \in \{0, +, -\}$ (i.e., each possibility has probability $\frac{1}{3}$) and sends $|r\rangle$.

- (a) What are the ensembles E_A, E_B, E_C describing the state sent by Alice in the experiments A, B, and C, respectively?
- (b) What are the density operators ρ_A, ρ_B, ρ_C corresponding to E_A, E_B, E_C .
- (c) Show that the states sent in experiments A and B are physically indistinguishable.

- (d) With what probability can an adversary distinguish between the state sent in experiment A and the state sent in experiment C?

(More precisely, compute the maximum difference of the probabilities that an adversary outputs 1 given the state from experiment A and given the state from experiment C.)

Hint: Use the trace distance.

Note: If you find yourself wishing for a computer algebra system to help with computing eigenvectors, you probably made a computation mistake.

- (e) Give an ensemble E_D such that $E_D \neq E_C$, but E_C and E_D are physically indistinguishable.

Note: No proof is needed that they are indistinguishable. But if you give the wrong solution, an argument why it is correct may help to get partial points if the mistake is, e.g., just due to a calculation error.

- (f) Let f be a permutation on $\{0,1\}^n$. Let U_f be the unitary transformation on \mathbb{C}^{2^n} defined by $U_f|x\rangle = |f(x)\rangle$.

Let $|\Psi\rangle := |0 \dots 0\rangle \otimes |1 \dots 1\rangle$ be a state in $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ (i.e., a state consisting of two n -bit systems, one initialized with $|0 \dots 0\rangle$, the other with $|1 \dots 1\rangle$). Let ρ be the corresponding density operator.

We apply $H^{\otimes n}$ to *each* part of the system. Then we apply U_f to the *second* part of the system. Then we trace out the second part of the system (i.e., apply tr_B).

What is the resulting density operator?

Hint: Think before computing. This should need hardly any computation. Drawing a quantum circuit may help you to see things more clearly.

Problem 3: Security definitions (9+9=18 points)

- (a) Consider the following protocol:

- Alice has a uniformly random secret $m \in \{0,1\}^n$.
- Then Alice produces some quantum state that depends on m and sends it over an insecure quantum channel so that the adversary Eve gets it. (Let ρ_m denote the density operator describing the state in the case m .)
- Bob does nothing.

Give a security definition that describes the fact that m stays secret. (Eve should learn no part of m . It is not sufficient to say that Eve learns nothing.) Your security definition should allow for an ε -error.

Hint: Use trace distance.

- (b) Consider the following variant of the security definition for quantum key distribution:

Definition 1 (Security of QKD – bad variant) Let a QKD protocol π be given. Let $n \in \mathbb{N}$. Let $\varepsilon > 0$.

Let an adversary Eve be given (that has full control over the quantum channel between Alice and Bob, but can only listen to but not modify the classical channel between Alice and Bob). Then let $\rho_{ABE}^{\text{Real}} \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ be the density operator describing the joint state of Alice's, Bob's and Eve's system in the case that Alice and Bob do not abort. Here $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^{2^n}$ because Alice's and Bob's final state consist of an n -bit key, and \mathcal{H}_E is some arbitrary Hilbert space defined by Eve.

Let $S_{\text{Ideal}} \subseteq S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ be the set of all states of the form

$$\left(\sum_{k \in \{0,1\}^n} 2^{-n} (|k\rangle\langle k| \otimes |k\rangle\langle k|) \right) \otimes \rho_E, \quad \rho_E \in S(\mathcal{H}_E).$$

By P_{success} denote the probability that Alice and Bob do not abort the protocol and thus output a key (given a particular adversary Eve).

We say that π is ε -secure if the following holds: For every adversary Eve, we have that

$$\exists \rho_{ABE}^{\text{Ideal}} \in S_{\text{Ideal}} : \quad \text{TD}(\text{tr}_E \rho_{ABE}^{\text{Real}}, \text{tr}_E \rho_{ABE}^{\text{Ideal}}) \cdot P_{\text{success}} \leq \varepsilon.$$

Note: The only difference to the original definition is that we compute $\text{TD}(\text{tr}_E \rho_{ABE}^{\text{Real}}, \text{tr}_E \rho_{ABE}^{\text{Ideal}})$ instead of $\text{TD}(\rho_{ABE}^{\text{Real}}, \rho_{ABE}^{\text{Ideal}})$. I.e., we throw away Eve's part of the system before computing the trace distance.

Why is this a bad definition? Explain why it is possible to have a protocol that satisfies this definition, but is a very bad protocol (in terms of security) anyway.

(It is not a correct answer to give drawbacks that the original definition of QKD shares. For example, saying that this definition does not exclude denial-of-service.)

Problem 4: LWE and Regev (9+[8] points)

- (a) You are given an LWE instance $A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$, $b := \begin{pmatrix} 5 \\ 1 \\ 5 \end{pmatrix}$. Parameters are $q = 11$ (i.e., computations are in \mathbb{Z}_{11}), $m = 3$, $n = 2$. You happen to know that due to a problem with the randomness generator, the noise is $e = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

What is the secret s ?

- (b) (A, b) as in the preceding subproblem are used at the public key of Regev's cryptosystem. (The parameters are the same, and the noise e still has the same known value.) You see the ciphertext (c_1, c_2) with $c_1 = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$, $c_2 = 4$.

What is the plaintext $\mu \in \{0, 1\}$?