Quantum Cryptography (spring 2022)	Dominique Unruh
Exercise Sheet 01	
Out: 2022-02-25	Due: 2021-03-04

Read me: You will need 50% of all homeworks to qualify for the exam. (That is, if you get at least 50%, your final grade will be the exam grade. And if you do not get 50%, you do not pass the course.)

You may hand in your solutions in person or by email. If you submit by email, either scan a handwritten solution or typeset your solution readably. I do not consider ASCII formulas readable. For nicely typeset solutions, you can get up to three extra points for the effort.

When submitting, indicate your name and your matriculation number. On your first submission, please also indicate a password, this password will be needed for accessing the solutions and your points online.

You may work in teams to solve the problems. If you do, everyone has to formulate their own solution! (No copy&paste.)

Each problem has a table with some data to be filled by you. The prefilled field "knowlets" refers to the knowlets that this problem is based on (see the lecture notes). If you think the problem depends on a knowlet not indicated there, please add it. In the field "time", please indicate how long it took for you to solve this problem. In the field "difficulty", please indicate the perceived difficulty level as a grade from A–E. (E.g., B means that B-level student would probably be able to solve this fully.) The data you enter here does not affect your grade, it is used for statistics for future semesters. (If the exercise sheet itself is not part of your submission, please just provide the data somewhere in your submission.)

1 Working with quantum states

(a)

Knowlets:	UniTrafo ProblemID: UTInv
Time:	
Difficulty:	

Show that by applying a unitary transformation to a quantum state, no information is ever lost. More exactly, assume that a unitary transformation U is applied to a given quantum state Ψ, resulting in a state Φ. Then show that there is another unitary transformation V (not depending on Ψ or Φ) such that applying V to Φ gives Ψ again.

(b)

Knowlets:	QState, Rota, ComplMeas ProblemID: RotaPolPhoton
Time:	
Difficulty:	

Assume that a photon is in the state $\Psi = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. (Here the α component corresponds to the vertical part and the β component to the horizontal part.) Let R be a rotation of angle $\theta = \frac{\pi}{3}$. Let F denote a polarisation filter that lets only vertically polarised light through. Assume that the photon Ψ is first sent through R and then through F. It turns out that in this setting, the photon is absorbed by F with probability 1.

Given these informations, what do you know about α? (I.e., what are the possible values of α?)

(c)

Knowlets:	ComplMeas ProblemID: RepeatMeas
Time:	
Difficulty:	

What is wrong with the following approach:

Alice has a qubit $|\Psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}$. They want to initialise the qubit to $\begin{pmatrix}1\\ 0\end{pmatrix}$. They know that when measuring Ψ, with probability $\frac{1}{2}$ they get the measurement outcome 0 and the qubit will be in state $\begin{pmatrix}1\\ 0\end{pmatrix}$. Thus they repeatedly measure the qubit in the computational basis until they get the outcome 0. Since the probability is $\frac{1}{2}$ each time, the expected number of measurements until they get their $\begin{pmatrix}1\\ 0\end{pmatrix}$-initialised qubit is 2.

(d)

Knowlets:	UniTrafo ProblemID: UniTrafo
Time:	
Difficulty:	

Which of the following are valid (unitary) transformations:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix}i & -1\\ i & 1\end{pmatrix}.$$

(e)

Knowlets:	QState ProblemID: 5Paths
Time:	
Difficulty:	

Consider a system in which a single photon may be sent through 5 different paths. The photon may be polarised in any direction. Give a Hilbert space for describing the state of this photon and give a natural basis for expressing this state. How do you write that the photon is 45°-polarised and on path 3?

(f)

Knowlets:	QState ProblemID: 5PathsMulti
Time:	
Difficulty:	

Consider a system in which each of 5 paths may contain a photon (or not), and each of these photons may be polarised in any direction. Give a Hilbert space for describing the state of these photons and give a natural basis for expressing this state. How do you write that there is a photon on path 3 that is 45°-polarised and no photons on the other paths?

2 Composed systems

(a)

Knowlets:	QState, ProjMeas ProblemID: MeasCat
Time:	
Difficulty:	

Consider the following state on n qubits: $\frac{1}{\sqrt{2}}|0\dots0\rangle + \frac{1}{\sqrt{2}}|1\dots1\rangle \in \mathbb{C}^{2^n}$.[1] Someone measures the last qubit (i.e., whether it is 0 or 1). What happens to the state?[2]

(b)

Knowlets:	Tensor ProblemID: TensorDistrib
Time:	
Difficulty:	

Show that $(U \otimes V) \cdot (U' \otimes V') = (UU') \otimes (VV')$. Here U, U', V, V' are $n \times n$ matrices.

Hint: To show that two matrices A, B are equal, it is sufficient to show that $A|ij\rangle = B|ij\rangle$ for all basis vectors $|ij\rangle$.

(c)

Knowlets:	Tensor ProblemID: TensorBili
Time:	
Difficulty:	

Show that $\otimes$ is bilinear, i.e., $(a+b)\otimes c = (a\otimes c)+(b\otimes c)$ and $c\otimes(a+b) = (c\otimes a)+(c\otimes b)$. This holds both if a, b, c are matrices and if they are vectors.

(d)

Knowlets:	ProjMeas ProblemID: ProjMeasPr1
Time:	
Difficulty:	

Show that in a projective measurement with outcomes $i \in I$, it holds that $\sum_{i\in I} \Pr[\text{outcome } i \text{ occurs}] = 1$. (I.e., some outcome will always occur.)

Note: Recall that $\|x\|^2$ for any vector x is $x^\dagger x$. And that $P^\dagger P = P$ for orthogonal projectors P. And that $(xy)^\dagger = y^\dagger x^\dagger$. Then take the formula for the measurement probability and just simplify.

[1] We call this a *cat state* because of its similarity to Schrödinger's cat: A cat which is dead can be seen as consisting of n dead particles ($|\text{dead}, \dots, \text{dead}\rangle$), and a living cat can be seen as consisting of n living particles ($|\text{alive}, \dots, \text{alive}\rangle$). (This is of course a simplification!).

[2] This can be seen as an explanation what happens if we try to implement Schrödinger's cat: Even with a very high quality box, information about at least one atom of the cat will leak to the outside (i.e., it is measured whether the atom is "alive"). This has then an effect on the state of the whole cat.

	Knowlets:	ProjMeas ProblemID: 5PathsMeas
(e)	Time:	
	Difficulty:	

In the situation of Problem 1 (e),[3] we measure whether there is a photon on path 3. Formulate this mathematically (i.e., as a projective measurement).

Note: You only need to formulate the measurement. You are not required to apply it (i.e., to compute probabilities and post-measurement states).

	Knowlets:	ProjMeas ProblemID: 5PathsMultiMeas
(f)	Time:	
	Difficulty:	

In the situation of Problem 1 (f),[4] we measure whether there is a photon on path 3. Formulate this mathematically (i.e., as a projective measurement).

Note: You only need to formulate the measurement. You are not required to apply it (i.e., to compute probabilities and post-measurement states).

[3] Reminder: "Consider a system in which a single photon may be sent through 5 different paths. The photon may be polarised in any direction. Give a Hilbert space for describing the state of this photon and give a natural basis for expressing this state. How do you write that the photon is 45°-polarised and on path 3?"

[4] Reminder: "Consider a system in which each of 5 paths may contain a photon (or not), and each of these photons may be polarised in any direction. Give a Hilbert space for describing the state of these photons and give a natural basis for expressing this state. How do you write that there is a photon on path 3 that is 45°-polarised and no photons on the other paths?"