Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

1. Exercise sheet
Hand in solutions until Monday, 01 November 2010, 23:59h.

Reminders.

- For the course we remind you of the following dates:
  - Lectures: Tuesday and Wednesday 13:00h-14:30h **sharp**, b-it 1.25.
  - Tutorial: Tuesday 14:45h-16:15h **sharp**, Room 1.25.
- A word on the exercises. They are important. Of course, you know that. In order to be admitted to the exam it is necessary that you earned at least 20% of the credits. Just as an additional motivation, you will get a bonus for the final exam if you attended both lecture and tutorial *regularily* and earned more than 60% or even more than 80% of the credits.

Exercise 1.1 (Unitary transformations). (12 points)

A Hilbert-space V is a complete complex vector space, equipped with a scalar product. We will always denote elements x of V by $|x\rangle$. In quantum information theory we only consider the Hilbert spaces $\mathbb{C}^n$ for some $n \in \mathbb{N}$ with the scalar product $\boxed{3}$

$$\langle x \mid y \rangle := \sum_{i=1}^{n} \bar{x}_i y_i.$$

Define the length of $|x\rangle$ as $\sqrt{\langle x \mid x \rangle}$.

(i) Verify that the scalar product defined above has the following properties:

(a) Prove that the operation is linear in the second argument, i.e. $\boxed{2}$

$$\langle x \mid y_1 + y_2 \rangle = \langle x \mid y_1 \rangle + \langle x \mid y_2 \rangle \quad \text{and} \quad \langle x \mid cy \rangle = c \langle x \mid y \rangle .$$

What can you say about the linearity in the first argument?

(b) $\langle x \mid y \rangle = \overline{\langle y \mid x \rangle}$, $\boxed{1}$

(c) $\langle x \mid x \rangle \in \mathbb{R}_{\geq 0}$ with equality if and only if $|x\rangle = 0$. $\boxed{1}$

For a matrix $U \in \mathbb{C}^{n \times n}$ define its *adjoint* as $(U^*)_{i,j} = \overline{U_{j,i}}$, i.e. as the the conjugated and transposed matrix of U. We call a matrix *unitary* if $U^{-1} = U^*$.

(ii) Show that for any matrix we have $\langle U^* x \mid y \rangle = \langle x \mid Uy \rangle$. Hint: Express any vector in terms of the standars basis $e_1 = (1, 0, \ldots, 0)^T, \ldots, e_n = (0, \ldots, 0, 1)^T$ and write out both inner products. $\boxed{4}$

(iii) Conclude that unitary matrices U preserve the inner product, i.e. we have $\langle Ux \mid Uy \rangle = \langle x \mid y \rangle$. $\boxed{1}$

Exercise 1.2 (The toss of a fair coin). (8+5 points)

Consider a quantum system with two basic states "head" $|h\rangle$ and "tail" $|t\rangle$. We call this system a *quantum coin*. Consider a time evolution $\boxed{3}$

$$\begin{aligned} |h\rangle &\mapsto \frac{1}{\sqrt{2}}|h\rangle + \frac{1}{\sqrt{2}}|t\rangle\,, \\ |t\rangle &\mapsto \frac{1}{\sqrt{2}}|h\rangle - \frac{1}{\sqrt{2}}|t\rangle\,, \end{aligned}$$

which is called a *fair coin toss*.

$\boxed{2}$ (i) Write down the matrix representation of the fair coin toss and prove that it is unitary.

$\boxed{1}$ (ii) Verify that when we start with one of the states $|h\rangle$ or $|t\rangle$, after the toss, we will end up in a state where $|h\rangle$ and $|t\rangle$ are observed both with probability $\frac{1}{2}$.

$\boxed{2}$ (iii) Show that when we start with the state $|h\rangle$ and perform the coin toss twice, we end up again with state $|h\rangle$.

$\boxed{+5}$ (iv) Interpret the result.