Quantum Cryptography (fall 2013) Prof. Dr. Dominique Unruh

Exercise Sheet 13

Out: December 11, 2013 Due: December 17, 2013

Problem 1: Schrödinger equation

[In this problem, there is a strong dependency between subsequent subparts. Thus, if you do not manage to solve one of the subparts, this may mean that you probably cannot even start the next. To avoid that, I offer two options: (i) You can ask for the solution of a subproblem that you cannot solve (in this case, you will not get points for that subproblem). (ii) You can submit part of your homework earlier, in this case you will get the solution for that subproblem while still getting points.]

In this problem, we will investigate the behavior of a free particle (a free particle is a particle that is not influenced by any potential and can travel freely through space).

More formally, we are looking for a wave function that satisfies the time-dependent Schrödinger equation with $V(x) = 0$ for all $x \in \mathbb{R}$.

We will consider the case where at time $t_0 = 0$, the particle is more or less localized, namely its position is Gaussian distributed around $x = 0$.

That is, we have

$$\psi(x, 0) := \frac{1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{x^2}{\sigma^2}}$$

We want to know where the particle will be at time $t > 0$.

(a) Find all solutions to the time-**in**dependent Schrödinger equation with $V = 0$.

Note: You need to find only two linear independent solutions for each energy level $E \in \mathbb{R}$. (You may omit the special case $E = 0$.) All other solutions are linear combinations of those two. If you are not familiar with differential equations: Try how $e^{\alpha x}$ behaves under double differentiation for $\alpha \in \mathbb{C}$.

(b) Express the initial state $\psi_0(x, 0)$ as a linear combination of solutions to the time-independent Schrödinger equation.

Hint: Taking the Fourier transform of $e^{-\alpha x^2}$ for $\alpha \neq 0$ yields the equality $e^{-\alpha x^2} = \frac{1}{2\sqrt{\pi\alpha}} \int_{-\infty}^{\infty} e^{-\frac{k^2}{4\alpha}} e^{ikx}\, dk$ (even if $\alpha \in \mathbb{C}$).

(c) Give a formula for the wave function $\psi(x, t)$ for all x and $t > 0$.

Note: You do not need to simplify the integrals occurring in this formula. Just state the formula for ψ unsimplified.

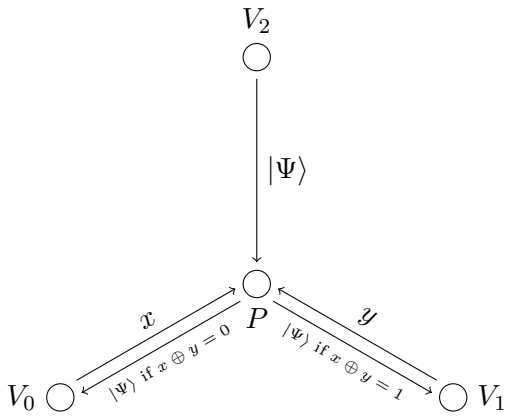

Figure 1: Position-verification protocol.

(d) Simplify the wave function ψ. (For each t, $\psi(x,t)$ should be a Gaussian.) What is the (absolute value of the) variation at time $t > 0$? What does this imply about the location of the particle after some time?

Hint: First, simplify ψ so that it matches the right hand side of the Fourier transform of $e^{-\alpha x^2}$ (see hint above). The variation of a Gaussian $Ae^{-\frac{x^2}{\sigma^2}}$ is defined to be the value σ^2.

Problem 2: Position-based cryptography

(a) Consider the following position-verification protocol (see also Figure 1):

- The honest prover wishes to prove that he is at position P (in 2-dimensional space).
- The verifiers V_0, V_1, V_2 are located around P, each at distance d from P.
- At the same time, V_2 sends a random BB84 qubit $|\Psi\rangle$ to P, and V_0 and V_1 send random bits $x, y \in \{0,1\}$, respectively.
- Upon receipt of $|\Psi\rangle, x, y$, the prover P sends $|\Psi\rangle$ to $V_{x\oplus y}$.
- When $V_{x\oplus y}$ receives $|\Psi\rangle$ back within time $2d/c$, the verifiers accept.

Assume a malicious prover that has three devices P_0^*, P_1^*, P_2^* which are located at the same positions as V_0, V_1, V_2, but not at position P. Describe an attack how the malicious prover can make the verifiers accept.

Hint: Use the idea of teleporting $|\Psi\rangle$ and moving the teleportation endpoint around. However, in this case, you have to be a bit more clever, because neither P_0^* nor P_1^* knows in time where the qubit $|\Psi\rangle$ should end up. You may need several (nested) teleportations.

(b) What is wrong with the following way of using position-based crypto? (Assuming we have a secure position-verification protocol.)

- A server has a file F that he wants to provide to anyone who is in a room R. Only people in R should be allowed to download F.
- To download F, a client P picks a public key pk for a public-key encryption scheme (which we assume to be secure with respect to any reasonable definition) and sends pk to the server. The public key pk is sent over an insecure channel.
- Then the server runs the position-verification protocol to establish that P is indeed in the room R.
- If the position-verification succeeds, the server encrypts F under pk and sends the ciphertext to P (over an insecure network).

Explain why this is insecure (in the sense that it is not guaranteed that only people in the room R can access F). Explain why it is not easy to fix that problem (i.e., why position-verification seems insufficient for the given purpose).

Note: The fact that a malicious device *inside* the room can receive F and forward it to someone outside the room is not considered an attack! Only if someone outside can get F without help from someone inside.