Theoretische Physik für Quantentechnologien

Prof. Dr. Frank Wilhelm-Mauch
Prof. Dr. Giovanna Morigi

SS 2016 **10.05.2016**
Blatt 2.2 **Fälligkeitsdatum: 17.05.2016**

***Achtung**: Ihre Lösungen sind am Anfang der nächsten Übung (Dienstag 17.05.) abzugeben.*

Aufgabe 3: BB84-Protokoll (*10 Punkte*)

In der Vorlesung haben Sie den BB84 Algorithmus zur Verschlüsselung von Daten kennengelernt. Wir wollen diesen in dieser Aufgabe nochmals etwas vertiefen. Hier noch einmal die grundlegenden Fakten:

- Alice präpariert ein Qubit in $|0\rangle$ oder $|1\rangle$
- Danach wendet sie zufällig ein Hadamard-Gatter an oder lässt das Qubit unverändert
- Bob misst das von Alice gesendete Qubit, wobei er vor der Messung auch rein zufällig ein Hadamard-Gatter anwendet oder das Qubit unverändert belässt
- Danach erfolgt eine klassische Kommunikation, in der die beiden austauschen ob ein Hadamard-Gatter angewendet (in welcher Basis gesendet bzw. gemessen wurde) wurde oder nicht
- Die Messungen, bei denen die Basis übereinstimmt können nun als Schlüssel verwendet werden.

a) Denken Sie sich ein eigenes Beispiel aus, bei dem Alice 16 Qubits an Bob schickt. Schreiben Sie die Basen und die Messergebnisse tabellarisch nieder und geben Sie den resultierenden Schlüssel an (Versuchen Sie die Basen zufällig zu wählen). (*3 Punkte*)

b) Zeigen Sie an ihrem Beispiel, dass ein Abhören durch Eve bei der klassischen Kommunikation zwischen Alice und Bob festgestellt wird. (*3 Punkte*)

c) Wie wahrscheinlich ist es, dass das Abhören durch Eve bei diesem Beispiel nicht entdeckt wird und wie skaliert diese Wahrscheinlichkeit mit der Anzahl der gesendeten Qubits? (*1 Punkt*)

d) Es gibt eine etwas unintuitivere Version dieses Verschlüsselungsprotokolls, welches auf den ersten Blick anders erscheint, sich aber als exakt dasselbe herausstellt. Nehmen Sie an es existiert eine zentrale Quelle, die Qubit-Paare im verschränkten Zustand

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

erzeugt und ein Anteil jedes Paares an Alice und den anderen Anteil an Bob schickt. Zeigen Sie, dass auch so am Ende ein gemeinsamer Schlüssel erzeugt wird. (*2 Punkte*)

e) Argumentieren Sie, dass dieses Protokoll aufgrund der Verschränktheit auf den ersten Blick sicherer gegen eine Abhörung durch Eve erscheint – bei genauerem Hinsehen aber beide Versionen gleich sicher sind. (*1 Punkt*)

Aufgabe 4: Übertragung von Bits (*10 Punkte*)

Ein zum BB84 Protokoll ähnliches Verfahren basiert auf der Idee, dass Alice Bob versichern möchte, dass sie eine gewisse binäre Entscheidung getroffen hat, ohne ihm diese Entscheidung sofort mitzuteilen. Hierzu schreibt sie ihre Antwort (*Ja* oder *Nein*) auf ein Blatt, verschließt es in einer Box und sendet die Box ohne den entsprechenden Schlüssel zu Bob. Sobald Bob die Box erhält kann er sicher sein, dass Alice ihre Entscheidung nicht mehr ändern kann – Alice widerum kann sich sicher sein, dass Bob ihre Entscheidung nicht kennt, solange sie ihm nicht den Schlüssel zusendet.
Im untersuchten Protokoll besitzt Alice n unterscheidbare Qubits, die Sie bei einem Ja($Nein$) zufällig im Zustand $|0\rangle$ ($H|0\rangle$) oder $|1\rangle$ ($H|1\rangle$) präpariert und an Bob sendet. Diesem liegen nun n Qubits vor, die sich jeweils mit gleicher Wahrscheinlichkeit in einem der beiden orthogonalen Zustände $|\psi\rangle$ und $|\phi\rangle$ befinden (ihm ist nicht bekannt welche Basis Alice gewählt hat).

(a) Wie groß ist die Wahrscheinlichkeit $p(0)$, dass Bob bei einer Einzelqubit-Messung diesen Qubit im Zustand $|0\rangle$ misst? (*1 Punkt*)

(b) Schließen Sie daraus, ob aus der Messung aller Qubits eine Information über die Zustände $|\psi\rangle, |\phi\rangle$ gewonnen werden kann. Wenn ja, wie? (*1 Punkt*)

Wir nehmen nun den Fall an, dass Alice n Qubits in einem der Basiszustände $|x\rangle$ präpariert und anschließend eine unitäre n-Qubit Transformation U anwendet. Die daraus erhaltenen Qubits werden an Bob übermittelt. Es soll untersucht werden, ob Bob etwas über die Wahl von U lernen kann, wenn er weiß, dass alle 2^n Werte von x gleichwahrscheinlich sind. Bob möchte sich hierzu m Ancilla-Qubits zunutze machen, die er mit denen von Alice kombiniert und eine unitäre $(n+m)$-Qubit Transformation W auf alle Qubits anwendet. Anschließed will er eine Information über U erhalten, indem er alle $n+m$ Qubits misst.

(c) Geben Sie den Zustand $|\Psi_x\rangle$ des Systems aus $n+m$ Qubits vor der Messung an. (*1 Punkt*)

(d) Wie groß ist die Wahrscheinlichkeit, dass Bob den Wert z erhält, wenn er alle Qubits misst? (*5 Punkte*)

(e) Wie kann aus dem Ergebnis aus Teil (d) eine Information über U gewonnen werden? Ist es möglich? Begründen Sie! (*2 Punkte*)

Aufgabe 5: No-cloning-Theorem und Quantenteleportation (*10 Punkte*)

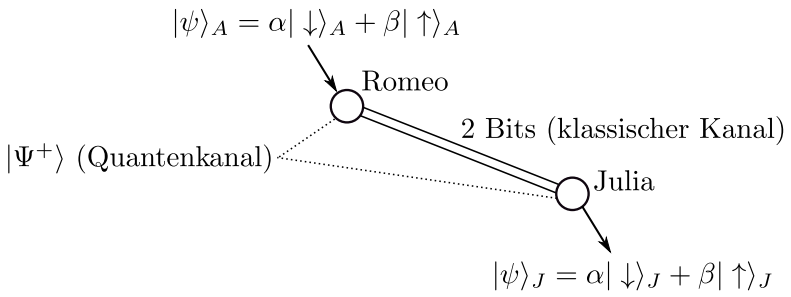
Romeo spielt oft mit dem Spin von Silberatomen (System A). Manchmal findet er sehr schöne Zustände, die er gerne klonen würde. Er wäre gerne in der Lage jeden möglichen Zustand zu klonen, weil er nicht weiß welchen er gut finden wird. Um das zu erreichen nimmt er ein weiteres Silberatom (System B) im Zustand $|e\rangle_B$ und möchte eine unitäre Transformation $U^{-1} = U^\dagger$ finden, sodass er jeden Zustand des Systems A klonen kann, also

$$U|\psi\rangle_A|e\rangle_B = |\psi\rangle_A|\psi\rangle_B, \quad \forall \text{ Spinzustände } |\psi\rangle_A$$

gilt.

(a) Zeigen Sie, dass eine solche Transformation nicht existiert. (*1 Punkt*)

Das macht Romeo traurig, sodass er hofft den Zustand zumindest der weit erntfernten Julia zeigen zu können. Die beiden können über einen klassischen Kanal kommunizieren indem sie zwei Bits übermitteln. Sie haben weiterhin eine Quelle zur Hand, die Silberatompaare im Bellzustand



$|\Psi^+\rangle$ emittiert. Wir erinnern uns daran, dass die vier Bellzustände durch

$$|\Phi^+\rangle_{RJ} = \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow\rangle_{RJ} + |\uparrow\uparrow\rangle_{RJ}\right)$$
$$|\Phi^-\rangle_{RJ} = \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow\rangle_{RJ} - |\uparrow\uparrow\rangle_{RJ}\right)$$
$$|\Psi^+\rangle_{RJ} = \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle_{RJ} + |\uparrow\downarrow\rangle_{RJ}\right)$$
$$|\Psi^-\rangle_{RJ} = \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle_{RJ} - |\uparrow\downarrow\rangle_{RJ}\right)$$

gegeben sind, wobei die Indizes R und J angeben welche Atome zu Romeo bzw. zu Julia fliegen. Nun kann Romeo Bellmessungen an den zwei System A und R machen, d.h. er kann feststellen in welchem Bellzustand sich das Atompaar befindet. Julia hingegen kann jede mögliche unitäre Transformation an ihrem Atom durchführen (sie arbeitet an dem System J).

(b) Nehmen Sie an, der Zustand den Romeo Julia zeigen will sei

$$|\psi\rangle_A = \alpha\,|\downarrow\rangle_A + \beta\,|\uparrow\rangle_A\,.$$

Schreiben Sie den Zustand $|\Gamma\rangle_{ARJ}$ des Gesamtsystems, das aus den Subsystemen A, R und J besteht, auf. (*1 Punkt*)

(c) Schreiben Sie den Zustand $|\Gamma\rangle_{ARJ}$ nun als eine Summe von Tensorprodukten von Bellzuständen des AR Subsystems und Zuständen des Subsystems J, d.h.

$$|\Gamma\rangle_{ARJ} \propto \sum_{i=1}^{4} |\eta^i\rangle_{AR} \otimes |\phi^i\rangle_J\,,$$

wobei $|\eta^i\rangle_{AR}$ die vier Bellzustände des Systems AR darstellen und $|\phi^i\rangle_J$ Zustände des Systems J sind, die Sie herausfinden sollen. (*2 Punkte*)

(d) Was passiert wenn Romeo eine Bellmessung an seinem Subsystem durchführt? (*2 Punkte*)

(e) Romeo kann die Informationen, die Julia benötigt um in ihrem System J den ursprünglichen Zustand $|\psi\rangle_A$ herzustellen, über den klassischen Kanal durch zwei klassische Bits übertragen, wenn sich die beiden vorher auf eine Art von Kode geeinigt haben. Wie kann Julia das Herstellen des Zustandes erreichen? (*2 Punkte*)

(f) Welche unitäre Transformation muss Julia durchführen nachdem sie die klassischen Informationen von Romeo empfangen hat um den gewünschten Zustand $|\psi\rangle_J = \alpha\,|\downarrow\rangle_J + \beta\,|\uparrow\rangle_J$ zu erhalten? (*2 Punkte*)

Jetzt ist Romeo doch noch glücklich.