

9. Übung Kryptographie II

1. Aufgabe Messen ohne Zerstörung eines Zustandes

(6 Punkte)

Bob gibt ein System A vor das in einem der beiden nicht-orthogonalen Zustände $|\varphi\rangle_A$ oder $|\tilde{\varphi}\rangle_A$ ist. Nun soll Alice herausfinden in welchen Zustand sich A befindet, ohne aber dabei den Zustand von A selbst zu zerstören. Alice hat nun folgende Idee:

Sie möchte ein zweites System B vorgeben welches den Zustand $|\beta\rangle_B$ hat um dann auf der Komposition AB beider Systeme eine unitäre Transformation U operieren zu lassen wie folgt:

$$\begin{aligned}
 U : \quad |\varphi\rangle_A \otimes |\beta\rangle_B &\longrightarrow |\varphi\rangle_A \otimes |\beta'\rangle_B \\
 |\tilde{\varphi}\rangle_A \otimes |\beta\rangle_B &\longrightarrow |\tilde{\varphi}\rangle_A \otimes |\tilde{\beta}'\rangle_B
 \end{aligned}
 \tag{1}$$

Dabei soll der Zustand von A nicht zerstört werden. Nun möchte sie ein Maß auf B einführen mit dem sie die Zustände $|\beta'\rangle_B$ und $|\tilde{\beta}'\rangle_B$ eindeutig unterscheiden kann. Beweise oder widerlege, ob Alice Idee immer funktioniert. Begründe deine Antwort ausführlich.

2. Aufgabe Quantenalgorithmen

(10 Punkte)

Schreibe in KASH ein Programm zur Simulation von Quantencomputern und Quantenalgorithmen.

Bemerkung: Quantensimulatoren gibt es bereits heute, natürlich auf herkömmlichen Rechnern. Es gibt in Deutschland Arbeitsgruppen an verschiedenen Universitäten, die sich mit der Implementation von Quantenalgorithmen auf sogenannten Quantensimulatoren beschäftigen.