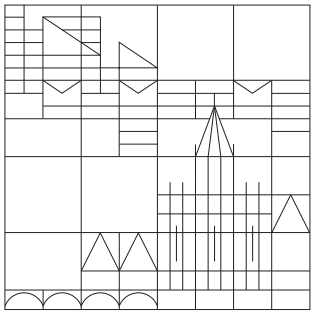
UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
Dr. Regina Finsterhoelzl
https://tinyurl.com/QC-S22



Quantencomputing und Quantensimulation
Sommersemster 2022 - Übungsblatt 11
Ausgabe: 11.07.2022, Abgabe: 18.07.2022, Übungen: 21.07.2022

Bonus-Aufgabe 27: Diffie-Hellman-Schlüsselaustausch (3 Bonuspunkte)

Der Diffie-Hellman-Schlüsselaustausch beschreibt ein Verfahren mittels dessen zwei Personen (Alice und Bob) einen gemeinsamen Schlüssel über einen unsicheren (abhörbaren) Kanal austauschen könenn, welcher dann zur Verschlüsselung weiterer Nachrichten verwendet werden kann. Zunächst einigen sich Alice und Bob auf eine große Primzahl p und eine weitere, kleine Zahl g, welche über den unsicheren Kanal ausgetauscht werden. Nun wählen sowohl Alice als auch Bob eine zufällige Geheimzahl a und b mit $0 \leq a, b \leq p-1$, welche Sie jeweils für sich behalten. Alice berechnet jetzt $A = g^a \bmod p$ und schickt das Resultat an Bob. Bob berechnet $B = g^b \bmod p$ und schickt das Resultat an Alice. Alice berechnet nun den Schlüssel K durch $K = B^a \bmod p$. Bob erhält den selben Schlüssel durch $K = A^b \bmod p$.
a) (1 Punkt) Berechnen Sie ein Beispiel für $g = 21$ und $p = 101$.

b) (1 Punkt) Zeigen Sie, dass $B^a \bmod p = A^b \bmod p$.

c) (1 Punkt) Der Diffie-Hellman-Schlüsselaustausch gilt als sicher für hinreichend große Primzahlen p. Beschreiben Sie, wie Eve durch abhören des Kanals dennoch den geheimen Schlüssel mithilfe eines Quantencomputers berechnen könnte.

Bonus-Aufgabe 28: Implentierung des Grover-Algorithmus (5 Bonuspunkte)

Betrachten Sie den abgebildeten Schaltkreis zur Implementerierung eines Orakels U_f für 3 Qubits. Skizzieren Sie einen Schaltkreis durch den die gesuchten Zustände gefunden werden. Wie viele Iterationen des Grover-Algorithmus werden benötigt? Welche Zustände werden durch das Orakel markiert?
Hinweis: 1 Punkt wird für die Lösung der Aufgabe auf einem realen Quantencomputer mithilfe des IBM Quantencomputers vergeben.