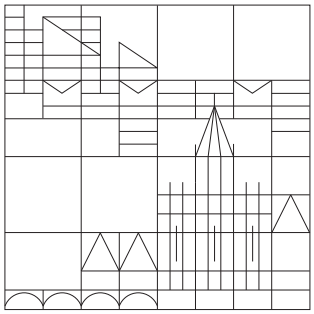
UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
Dr. Regina Finsterhoelzl
Dr. Balázs Gulácsi
https://tinyurl.com/QC-WS23



Quantencomputing und Quantensimulation
Wintersemester 2023 - Übungsblatt 11
Ausgabe: 26.01.2024, Abgabe: 02.02.2024, Übungen: 09.02.2024

Bonus-Aufgabe 26: Diffie-Hellman key exchange (3 bonuspoints)

The Diffie-Hellman key exchange describes a method by which two people (Alice and Bob) can exchange a common key via an insecure (interceptable) channel, which can then be used to encrypt further messages. First, Alice and Bob agree on a large prime number p and another small number g, which are exchanged via the insecure channel. Now both Alice and Bob choose a random secret number a and b with $0 \leq a, b \leq p-1$, which they each keep to themselves. Alice now calculates $A = g^a \bmod p$ and sends the result to Bob. Bob calculates $B = g^b \bmod p$ and sends the result to Alice. Alice now calculates the key K by $K = B^a \bmod p$. Bob receives the same key by $K = A^b \bmod p$.

a) (1 point) Calculate an example for $g = 21$ and $p = 101$.

b) (1 point) Show that $B^a \bmod p = A^b \bmod p$.

c) (1 point) The Diffie-Hellman key exchange is considered secure for sufficiently large prime numbers p. Describe how Eve could still calculate the secret key using a quantum computer by listening to the channel.

Bonus-Aufgabe 27: Implementing Grover's algorithm (3 bonuspoints)

Consider the circuit shown to implement an oracle U_f for 3 qubits. Sketch a circuit to find the desired states. How many iterations of the Grover algorithm are required? Which states are marked by the oracle?

Note: 5 extra points for implementing this problem on a real quantum computer, for example IBM Quantum or Quantum Inspire.