Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Präsenzübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 6 / 4. Juli 2016

AUFGABE 1:

Sei $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} |y\rangle$ und $W = -\mathrm{id} + 2|\psi\rangle\langle\psi|$ Zeigen Sie, dass für einen allgemeinen Zustand $\sum_k \alpha_k |k\rangle$ gilt

$$W\Big(\sum_k \alpha_k |k\rangle\Big) = \sum_k (2\widehat{\alpha} - \alpha_k)|k\rangle,$$

wobei $\widehat{\alpha} = \sum_x \frac{\alpha_x}{2^n}$. Interpretieren Sie dieses Ergebnis.

AUFGABE 2:

Geben Sie die unitäre Matrix an, die die Rotation W in der Grover-Iteration beschreibt (für allgemeines n).

AUFGABE 3:

Geben Sie einen Quantenschaltkreis (bestehend aus "Standard"-Gates) an, der die Rotation W der Grover-Iteration realisiert.

AUFGABE 4:

Sei $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ eine Hashfunktion. Wir arbeiten im Random-Oracle-Modell, d.h. f soll sich "wie eine zufällige Funktion verhalten". Wir nehmen an, wir haben U_f zur Verfügung.

(a) Geben Sie einen Quantenalgorithmus an, der zu gegebenem y ein x mit $f(x) = y$ findet (sofern existent)

(b) Geben Sie einen Quantenalgorithmus an, der zu gegebenem x ein $x' \neq x$ mit $f(x) = f(x')$ findet (sofern existent).

(c) Geben Sie einen Quantenalgorithmus an, der ein Paar $x \neq x'$ mit $f(x) = f(x')$ findet.

Was ist in jedem Fall die Quantenkomplexität? Wie vergleicht sich dies mit klassischen Algorithmen?