RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae

Hausübungen zur Vorlesung

Quantenalgorithmen

WS 2011/2012

Blatt 5 / 12 Dezember 2011

Abgabe bis 09. Januar 2012, 14 Uhr (vor der Übung)

AUFGABE 1 (4 Punkte)**:**
Sei $N = pq$, p, q prim. Gegeben sei ein Algorithmus, der bei Eingabe $(a, N) \in \mathbb{Z}_N^* \times \mathbb{N}$ die Ordnung $\mathrm{ord}_{\mathbb{Z}_n^*}(a)$ in Zeit $T(N)$ berechnet. Beweisen Sie, dass dann N in erwarteter Laufzeit $\mathcal{O}(T(N)\log^3 N)$ faktorisiert werden kann.

Hinweise: Nutzen Sie die Darstellung $ord(a) = 2^k t$ *mit* t *ungerade. Falls* $a^{2^i t} \neq \pm 1$ *und* $a^{2^{i+1}t} = 1$ *für ein* $i \in \mathbb{Z}_k$*, dann berechnen Sie* $ggT(a^{2^i t}, N)$*.*

AUFGABE 2 (5 Punkte)**:**
Geben Sie die Abbildungsmatrix von QFT_8 an und zeigen Sie, dass diese Abbildung unitär ist.

AUFGABE 3 (5 Punkte)**:**
Führen Sie eine QFT auf folgendem Zustand aus.

$$|z\rangle = \frac{1}{2}\sum_{i=0}^{7} \cos\left(\frac{2\pi i}{8}\right)|i\rangle$$

AUFGABE 4 (4 Punkte)**:**
Betrachten Sie das folgende Quanten-Münzwurfprotokoll:
Alice wählt $a \in \{0, 1\}$ und sendet an Bob $|0\rangle$ falls $a = 0$ und $W_2|0\rangle$ falls $a = 1$. Bob möchte a mit möglichst großer Wahrscheinlichkeit bestimmen. Dazu misst er Alices Zustand in der orthonormalen Basis $|\psi_0\rangle = \cos\beta|0\rangle - \sin\beta|1\rangle$, $|\psi_1\rangle = \sin\beta|0\rangle + \cos\beta|1\rangle$. Er setzt $b = 0$ falls seine Messung $|\psi_0\rangle$ ergibt und $b = 1$ falls er $|\psi_1\rangle$ misst.
Wie muss Bob den Parameter β wählen, um die Wahrscheinlichkeit $\Pr(a = b)$ zu maximieren?