RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova

Hausübungen zur Vorlesung

Quantenalgorithmen

WS 2013/2014

Blatt 6 / 23 January, 2014. 2 p.m.

Exercise 1 (4 Punkte)**:**
Let $N = pq, p, q$ – prime. Assume you are given an algorithm that for an input $(a, N) \in \mathbb{Z}_N^* \times N$ outputs the order $ord_{\mathbb{Z}_N^*}(a)$ in time $T(N)$. Use this algorithm as a black-box to construct an algorithm that factors N with running time $\mathcal{O}(\log^3 N \cdot T(N))$.

Exercise 2 (4 Punkte)**:**
Factor 187 using the period of the function $f(x) = 32^x \mod 187$.

Exercise 3 (5 Punkte)**:**
The goal of this exercise is to construct an adder that computes $|x\rangle \to |x + y \mod 2^n\rangle$ for a fixed constant y using QFT.

1. Using R-transformation defined by $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$ show how to construct a phase-shift transformation
$$|k\rangle \to e^{\frac{2\pi i y \cdot k}{2^n}} |k\rangle$$
Hint. Consider the binary representations of k, y and $y \cdot k$.

2. Using a phase-shift transformation as a black-box give a QC for $|x\rangle \to |x + y \mod 2^n\rangle$.