Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

9. Exercise sheet
Hand in solutions until Monday, 10 January 2011, 23:59h.

This sheet shall help you to recall the basic ideas of quantum computation, the elementary operations we use, and the more involved techniques like QFT, order finding and factoring. To get the intuition which aspects of quantum computation are of greatest importance, it is *necessary* that you really do the work of restating the important results.

Exercise 9.1 (Discrete Logarithms). (10 points)

In the course we discussed a quantum algorithm for the discrete logarithm problem. An instance of the problem is given by a natural number N and $a, b \in \mathbb{Z}_N^\times$ with $b = a^s$ for some integer s and the goal is to find s. Write $r = \mathrm{ord}_N(a)$. To solve the problem we employed the transformation

$$U \left|x_1\right\rangle \left|x_2\right\rangle \left|y\right\rangle = \left|x_1\right\rangle \left|x_2\right\rangle \left|y \oplus f(x_1, x_2)\right\rangle$$

with $f(x_1, x_2) = b^{x_1} a^{x_2}$.

(i) Construct a quantum circuit for the operation U. How many basic operations do you need? [4]

(ii) In the lecture we defined [3]

$$\left|\hat{f}(\ell_1, \ell_2)\right\rangle = \sum_{0 \le x_1 < r} \sum_{0 \le x_2 < r} e^{-2\pi i(\ell_1 x_1 + \ell_2 x_2)/r} \left|f(x_1, x_2)\right\rangle .$$

Show that it equals $\frac{1}{\sqrt{r}} \sum_{0 \le j < r} e^{-2\pi i \ell_2 j / r} \left|f(0, j)\right\rangle$, where this expression is defined to be non-zero if $\ell_1 s - \ell_2$ is an integer multiple of r.

(iii) Show that [3]

$$\frac{1}{r} \sum_{0 \le \ell_1 < r} \sum_{0 \le \ell_2 < r} e^{2\pi i(\ell_1 x_1 + \ell_2 x_2)/r} \left|\hat{f}(\ell_1, \ell_2)\right\rangle = \left|f(x_1, x_2)\right\rangle$$

Exercise 9.2 (Qubit transformations). (11 points)

A reminder:

(i) Restate the six important one bit gates H, S, T, X, Y and Z. [2]

(ii) Recall the definitions for the rotation operators R_x, R_y and R_z and $R_{\vec{n}}$ for a unit-vector $\vec{n}$. [2]

(iii) Specify the matrices for the CNOT and the Toffoli-gate. [1]

(iv) Sketch how we showed that one-qubit gates and CNOT are quantum-universal. [3]

(v) How did we reduce the number of necessary one qubit gates to a finite set, at least if we want to be quantum-universal in the approximate sense? [3]

Exercise 9.3 (From QFT to quantum-polynomial-time factorization). (8 points)

We are now ready to recall the basic steps to do factorization of integers in quantum polynomial time.

[2] (i) Describe on a high level perspective the different steps to construct an efficient quantum circuit from the quantum Fourier transform for the factorization of integers.

[6] (ii) Explain in more detail the different steps used in your high-level description.

Exercise 9.4 (Factoring 143 – the high-level view). (7+5 points)

You are now going to show how to factor $N = 143$ using the quantum factorization algorithm.

[1] (i) Show that N is neither even nor a perfect power.

[2] (ii) Take $x = 2$. Check that it is co-prime to N. Compute the order r of x in $\mathbb{Z}_N^\times$. (How do you do that?)

[2] (iii) Now show that $x^{r/2} \neq -1$ in $\mathbb{Z}_N^\times$. And compute a factor of N.

[2] (iv) Why does this algorithm not give you a classical polynomial time algorithm?

[+5] (v) Perform statistics! Select x randomly from $\mathbb{Z}_N^\times$ and check how often the above procedure gives you a factor of N. Do the same for other values of N. A computer algebra system might be a big help here!

Exercise 9.5 (Factoring 21 – the bit-level view). (18 points)

You are now going to show from a bit-level perspective how to factor $N = 21$ using the quantum factorization algorithm. Choose $x = 4 \in \mathbb{Z}_N^\times$.

[1] (i) Suppose you want to have error probability $\varepsilon = 1/4$. Compute the corresponding value of the number t of bits that are necessary.

[1] (ii) Begin with the state $|0\rangle\,|0\rangle$. Write down the state after the t Hadamard transforms.

[3] (iii) Compute the transformation U, where $U\,|x\rangle\,|y\rangle = |x\rangle\,\big|y + x^k\big\rangle$ in $\mathbb{Z}_{21}$, leaving the result in the second register.

[2] (iv) Suppose while measuring the second register you obtain the value for the number 16. Write down the (collapsed) state of the first register after this measurement.

[4] (v) Perform the inverse Fourier transform on the sequence of coefficients of the state. How many peeks do you see in the amplitude statistics? You will need a computer to do the computation.

3 (vi) Take the peak at amplitude $\alpha = 5461$. Perform the continued fraction expansion on $\alpha/2^t$ and write down the convergents.

2 (vii) Where do you find the order r of x in $\mathbb{Z}_N$?

(viii) Describe how you compute now the factors of N. 2

Exercise 9.6 (Cryptographic implications). (0+10 points)

Argue that the main cryptographic primitives like RSA, Diffie-Hellman key exchange or DSA are not secure anymore once quantum computers can be built. +10