Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

7. Exercise sheet
Hand in solutions until Monday, 13 December 2010, 23:59h.

Exercise 7.1 (Phase estimation revisited). (5+3 points)

In the lecture we discussed a quantum algorithm for phase estimation. There we wanted to approximate a phase φ using a t-bit binary number $b/2^t$ (with $b \in [0, 2^t - 1]$), where the error $\delta = \varphi - b/2^t$ satisfied $0 \leq \delta \leq 2^{-t}$. We computed the amplitudes of $|(b + \ell) \text{ rem } 2^t\rangle$ as

$$\alpha_\ell = \frac{1}{2^t} \frac{1 - \exp(2\pi i(2^t\delta - \ell))}{1 - \exp(2\pi i(\delta - \ell/2^t))}$$

in case $\delta \neq 0$ or $\ell \neq 0$. For $\delta = 0$ we have $\alpha_0 = 1$

(i) Set $\varphi = 1/7$. Plot the probabilities for the possible measurements for $t \in \{3, 5, 8, 12\}$ at the points $\ell/2^t$, where ℓ runs through $[-2^{t-1}, 2^{t-1}] \cap \mathbb{Z}$. 5

(ii) Interpret you results. +3

Exercise 7.2 (φ-asco). (3 points)

Let $p, q \in \mathbb{N}$ be two different prime numbers. Let $N = p \cdot q$. Then $\varphi(N) = (p - 1) \cdot (q - 1)$, where φ is Euler's totient function. Compute — without factoring N — p and q, if $N = 168149075693$ and $\varphi(N) = 168148245408$ are given. *Hint:* Look at the quadratic equation $x^2 - (p + q)x + pq = 0$. 3

Exercise 7.3 (Order mod N). (4 points)

(i) Compute the order of $x = 5$ in $\mathbb{Z}_{21}^\times$. 1

(ii) Compute $3^{1\,000\,003}$ in $\mathbb{Z}_{101}^\times$ by hand. *Note*: Only a small calculation is needed! 3

Exercise 7.4 (Another unitary operation). (13 points)

Let N be a natural number, $x \in \mathbb{Z}_N^\times$ and $y \in \{0, 1\}^L$. In the lecture we encountered the function

$$U|y\rangle = \begin{cases} |xy \text{ rem } N\rangle & \text{, if } 0 \leq y < N, \\ |y\rangle & \text{, if } N \leq y < 2^L. \end{cases}$$

(i) Show that U is unitary. 3

(ii) Sketch the circuit for order finding. 2

In the lecture be computed the eigenstates $|u_s\rangle$ of U as

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{0 \le k < r} \exp\left(\frac{-2\pi i s k}{r}\right) \left|x^k \text{ rem } N\right\rangle,$$

where r is the order of x in $\mathbb{Z}_N$.

[3] (iii) Prove that $\frac{1}{\sqrt{r}} \sum_{0 \le s < r} |u_s\rangle = |1\rangle$.

[2] (iv) Show that in the algorithm the state before the inverse Fourier transform is

$$|\psi\rangle = \sum_{0 \le j < 2^t} |j\rangle\, U^j\, |1\rangle = \sum_{0 \le j < 2^t} |j\rangle \left|x^j \text{ rem } N\right\rangle.$$

[3] (v) Starting from this $|\psi\rangle$ compute (again) the inverse Fourier transform of $|\psi\rangle$ with respect to $|j\rangle$.