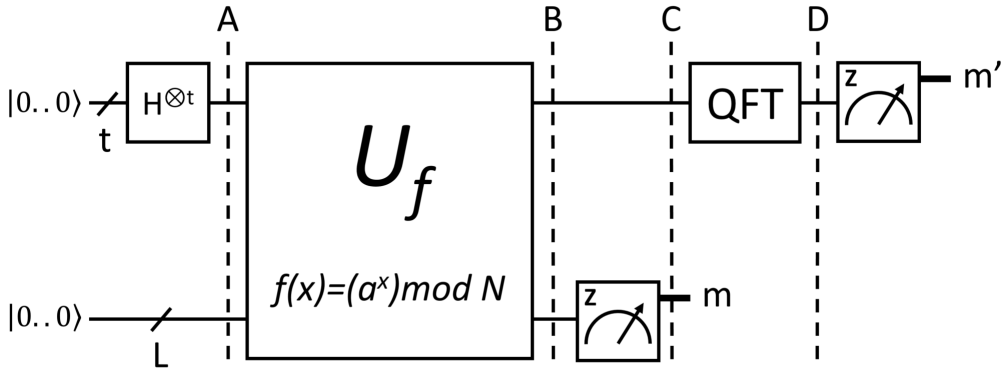
Homework #4

solutions

You've set up an encrypted channel between you and your friend with the public key ($N = 247, \quad e = 5$), but you forgot the private key d! You now have to implement Shor's algorithm and use it to recover d.



a) *(10 points)* How many qubits do you need for the top (t) and bottom (L) registers?

$$t = 2\lceil log_2 N \rceil + 1 = 17$$
$$L = \lceil log_2 N \rceil = 8$$

b) *(10 points)* What is the state Ψ_A of all the qubits at point A? Please write your answer using the summation symbol Σ.

$$|\Psi_A\rangle = H^{\otimes 17} \otimes I^{\otimes 8} |0\rangle |0\rangle = \frac{1}{\sqrt{2^{17}}} \sum_{x=0}^{2^{17}-1} |x\rangle$$

c) *(10 points)* How many candidates do you have for a? Out of all of them, pick the smallest value of a that would result in only four possible measurement outcomes for the lower register after applying U_f.

There are 215 numbers between 2 and N that are coprime with N. The smallest one that satisfies the required condition is $a = 18$ which results in outcomes $|1\rangle$, $|18\rangle$, $|77\rangle$ and $|151\rangle$ for the bottom register.

d) *(10 points)* What is the state $|\Psi_B\rangle$ of all the qubits at point B if you use

the a from c)? Please write your answer using the summation symbol Σ.

$$
\begin{aligned}
|\Psi_B\rangle = U_f\,|\Psi_A\rangle &= \frac{1}{\sqrt{2^{17}}}\sum_{x=0}^{2^{17}-1}|x\rangle\,|18^x \ mod\ 247\rangle \\
&= \frac{1}{\sqrt{2^{17}}}(|0\rangle\,|1\rangle + |1\rangle\,|18\rangle + |2\rangle\,|77\rangle + |3\rangle\,|151\rangle + |4\rangle\,|1\rangle + ... + |2^{17}-1\rangle\,|151\rangle) \\
&= \frac{1}{\sqrt{2^{15}}}\sum_{k=0}^{2^{15}-1}|4k\rangle \otimes \frac{1}{\sqrt{2^2}}\,|1\rangle + \frac{1}{\sqrt{2^{15}}}\sum_{k=0}^{2^{15}-1}|4k+1\rangle \otimes \frac{1}{\sqrt{2^2}}\,|18\rangle \\
&\quad + \frac{1}{\sqrt{2^{15}}}\sum_{k=0}^{2^{15}-1}|4k+2\rangle \otimes \frac{1}{\sqrt{2^2}}\,|77\rangle + \frac{1}{\sqrt{2^{15}}}\sum_{k=0}^{2^{15}-1}|4k+3\rangle \otimes \frac{1}{\sqrt{2^2}}\,|151\rangle
\end{aligned}
$$

e) *(10 points)* What is the state $|\Psi_C\rangle$ of the top register at point C if you measured $|1\rangle$ in the bottom register? Please write your answer using the summation symbol Σ.

$$|\Psi_C\rangle = \frac{1}{\sqrt{2^{15}}}\sum_{k=0}^{2^{15}-1}|4k\rangle$$

f) *(15 points)* What is the state $|\Psi_D\rangle$ of the top register at point D? Please write your answer using the summation symbol Σ.

The QFT transforms a qubit $|j\rangle$ into:

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^{17}}}\sum_{x=0}^{2^{17}-1} e^{\frac{2\pi i j x}{2^{17}}}\,|x\rangle$$

In our case, $|j\rangle = |4k\rangle$ *so by applying the QFT to* $|\Psi_C\rangle$ *we get:*

$$|\Psi_D\rangle = \frac{1}{\sqrt{2^{15}}}\frac{1}{\sqrt{2^{17}}}\sum_{k=0}^{2^{15}-1}\sum_{x=0}^{2^{17}-1} e^{\frac{2\pi i 4kx}{2^{17}}}\,|x\rangle$$

g) *(10 points)* If we define $\alpha_x \in \mathbb{C}$ as the probability amplitude of $|x\rangle$, we can write $|\Psi_D\rangle = \sum_x \alpha_x\,|x\rangle$. Write the expression for α_x and make a bar plot of the probabilities $|\alpha_x|^2$ of measuring $|x\rangle$ in the top register. What are the possible measurement outcomes?

$$\begin{aligned}
|\Psi_D\rangle &= \frac{1}{\sqrt{2^{15}}}\frac{1}{\sqrt{2^{17}}}\sum_{k=0}^{2^{15}-1}\sum_{x=0}^{2^{17}-1} e^{\frac{2\pi i 4kx}{2^{17}}}\,|x\rangle \\
&= \sum_{x=0}^{2^{17}-1}\sum_{k=0}^{2^{15}-1} \frac{1}{\sqrt{2^{32}}} e^{\frac{2\pi i 4kx}{2^{17}}}\,|x\rangle \\
\Rightarrow\ \alpha_x &= \sum_{k=0}^{2^{15}-1} \frac{1}{\sqrt{2^{32}}} e^{\frac{2\pi i 4kx}{2^{17}}}
\end{aligned}$$

The possible measurement outcomes are $|0\rangle$, $|32768\rangle$, $|65536\rangle$ *and* $|98304\rangle$, *all with equal probability.*

h) *(10 points)* For each measurement outcome for the top register, calculate r, p, q and finally, d.

Outcome $|0\rangle$ *can't be used. The other three outcomes can all result in* $r = 4$ *which successfully leads to* $p = 13$ *and* $q = 19$ *by finding* $gcd(a^{\frac{r}{2}} \pm 1,\ N)$. *Finally,* d *has to satisfy* $(ed)\ mod\ [(p-1)(q-1)] = 1$, *which results in* $d = 173$.

i) *(10 points)* What are the odds that the algorithm will succeed in finding p and q under these circumstances?

75%, because outcome $|0\rangle$ *is useless.*

j) *(5 points)* Does the algorithm still work if you don't measure the bottom register?

Yes, this is the common way of implementing Shor's algorithm. The difference will now be that the top register will have more possible outcomes (in our case, 4 for each possible measurement value of the bottom register).