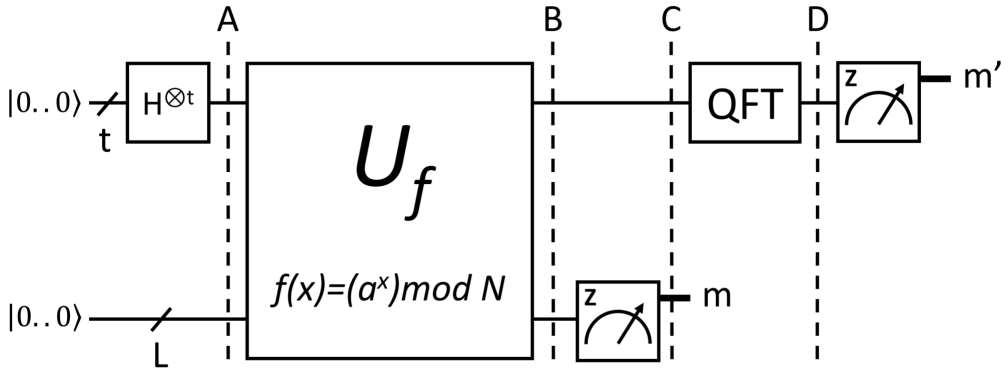
Homework #4

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?

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.

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.

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.

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.

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.

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?

h) *(10 points)* For each measurement outcome for the top register, calculate

r, p, q and finally, d.

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

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