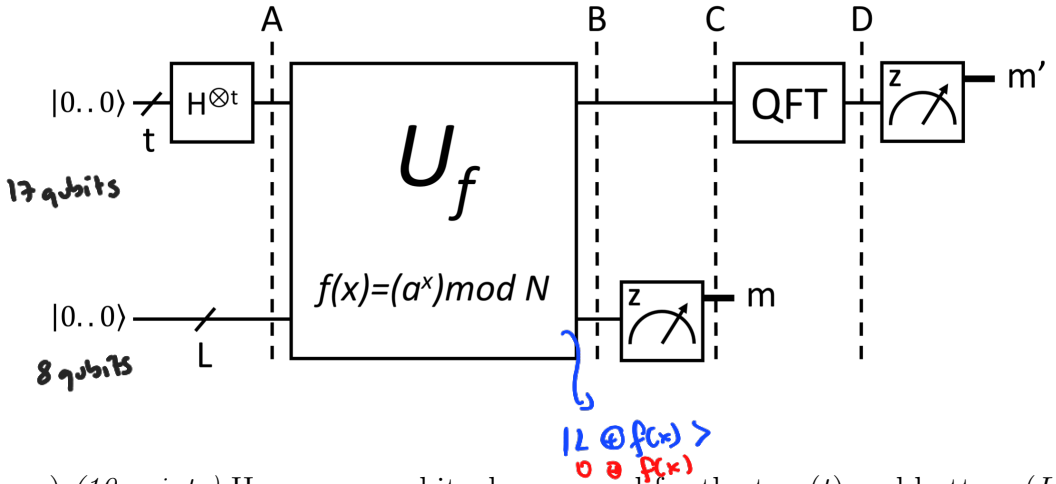
Zeynepnur Sahinel

1) Alice takes 2 prime numbers p, q
   ↓
   N = p·q
2) Alice choose e coprime with (p-1)(q-1)
3) Alice announces N, e

Encryption
1) $P_i = (M_i)^e \mod N$
2) Decoding key: $(de) \mod (p-1)(q-1) = 1$
3) Decryption $M_i = (P_i)^d \mod N$

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?

$N = 247$

$t = 2\lceil \log_2 N \rceil + 1 = 2 \log_2 247 + 1 = 2 \times 7.948 + 1 = 16.896$

$\simeq 17$ qubits

$L = \log_2 N \simeq \log_2 247 \simeq 8$ qubits

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.

$$\left[H^{\otimes 17} |0\rangle\right] |0\rangle^{\otimes 8}$$

$x_0 y_0 \oplus x_1 y_1 \oplus \dots x_{N-1} y_{N-1} = 0$

Note that $H^{\otimes N} |x\rangle = \frac{1}{2^{N/2}} \sum_{y=0}^{2^N - 1} (-1)^{x \odot y} |y\rangle$

$(-1)^0 = 1$

$$H^{\otimes 17} |0\rangle = \frac{1}{2^{17/2}} \sum_{y=0}^{2^{17}-1} |y\rangle$$

$$|\Psi_A\rangle = \left[\frac{1}{2^{17/2}} \sum_{y=0}^{2^{17}-1} |y\rangle\right] |0\rangle^{\otimes 8}$$

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.

Candidates for a are all the numbers which are coprime with N up to 2^{17}.

To have 4 possible outcomes, period (r) should be 4.

$f(x) = a^x \bmod N = a^x \bmod 247 \rightarrow a^4 \equiv 1 \pmod{247}$

$a = \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, \cancel{7}, \cancel{8}, \cancel{9}, \cancel{10}, \cancel{11}, \cancel{12}, \cancel{13}, \cancel{14}, \cancel{15}, \cancel{16}, \cancel{17}, (18)$

Smallest $a = 18$

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.

$$\Psi_A = \left[\frac{1}{2^{17/2}} \sum_{y=0}^{2^{17}-1} |y\rangle_{17} \right] |0\rangle^{\otimes 8}$$

$$\Psi_B = \frac{1}{2^{17/2}} \Big[|0\rangle_{17} |0 \oplus 18^{0} \bmod 247\rangle + |1\rangle_{17} |0 \oplus 18^{1} \bmod 247\rangle$$
$$|2\rangle_{17} |0 \oplus 18^{2} \bmod 247\rangle + |3\rangle_{17} |0 \oplus 18^{3} \bmod 247\rangle$$
$$+ |4\rangle_{17} |0 \oplus 18^{4} \bmod 247\rangle + \dots \Big]$$

$$\Psi_B = \frac{1}{2^{17/2}} \left[\sum_{k=0} |4k\rangle_{17} |1\rangle_8 + \sum_{k=0} |4k+1\rangle_{17} |18\rangle_8 + \sum_{k=0} |4k+2\rangle_{17} |77\rangle_8 + \sum_{k=0} |4k+3\rangle |151\rangle_8 \right]$$

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.

$|0\rangle + |4\rangle + \dots + |244\rangle \Rightarrow \#62$

$$\Psi_C = \frac{1}{\sqrt{62}} \left[\sum_{k=0} |4k\rangle_t \right] |1\rangle_L$$

Normalization

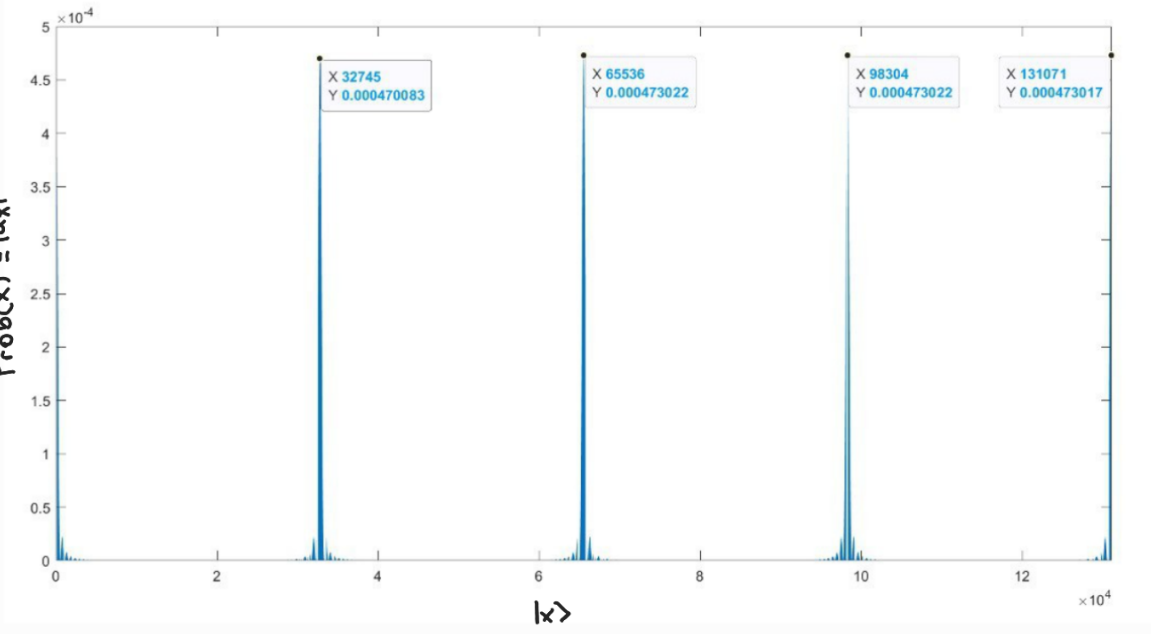
f) *(15 points)* What is the state $|\Psi_D\rangle$ of the top register at point D? Please write your answer using the summation symbol Σ.

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} jk} |k\rangle$$

$$|\Psi_D\rangle = \frac{1}{\sqrt{2^{17} \cdot 62}} \left(\sum_{k=0}^{2^{17}-1} e^{\frac{2\pi i}{2^{17}} \cdot 0k} |k\rangle + \sum_{k=0}^{2^{17}-1} e^{\frac{2\pi i}{2^{17}} \cdot 4k} |k\rangle + \sum_{k=0}^{2^{17}-1} e^{\frac{2\pi i}{2^{17}} \cdot 8k} |k\rangle + \dots + \sum_{k=0}^{2^{17}-1} e^{\frac{2\pi i}{2^{17}} 244k} |k\rangle \right)$$

$$|\Psi_D\rangle = \frac{1}{\sqrt{2^{17} \cdot 62}} \left(\sum_{k=0}^{61} |0\rangle + \sum_{k=0}^{61} e^{\frac{2\pi i (4k)}{2^{17}}} |4\rangle + \sum_{k=0}^{61} e^{\frac{2\pi i (8k)}{2^{17}}} |8\rangle + \dots + \sum_{k=0}^{61} e^{\frac{2\pi i (244 \times 4) k}{2^{17}}} |244\rangle \right)$$

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?



$\frac{2^{17}}{4} = 2^{15} = 32768$

Maxs occur at $\{0, 32768, 65536, 98304\}$

These 4 results are more possible to obtain.

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

For $x=0$ → no information can be extracted

For $x=32768$ → $\frac{32768}{2^{17}} = \frac{s}{r} = \frac{1}{4}$ ← $r=4$

$a=18 \Rightarrow y = a^{r/2} \pmod N = 18^2 \pmod{247} = 77$

$y+1 = 78$, $y-1 = 76$

$p = \gcd(78, 247) = 13$ ✓ success

$q = \gcd(76, 247) = 19$

for $r=4$

$p = 13$

$q = 19$

$d = 173$

From the protocol ↓ RSA encryption

$de \equiv 1 \mod (p-1)(q-1)$

$5 \quad 12 \quad 18$

$5d \equiv 1 \mod(216)$

173

$4 \times 216 + 1$

For $x = 65536 \rightarrow \frac{65536}{2^{17}} = \frac{2^{15} \times 2}{2^{17}} = \frac{1}{2} \rightarrow \boxed{r=2}$

$a=18 \Rightarrow y = a^{rh} \pmod N = 18^{1} \pmod{247} = 18$

$y+1 = 19$, $y-1 = 17$

$p = \gcd(17, 247) = 1$ → partial solution

$q = \gcd(76, 247) = 19$ ✓

for $r=2$

$q = 19$

$p = \cancel{X} \cdot 17$

$d = 173$

For $x = 98304 \rightarrow \frac{98304}{2^{17}} = \frac{2^{15} \times 3}{2^{17}} = \frac{3}{4} \rightarrow \boxed{r=4}$

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

Near to these max points. Such as 32745. we can obtain $\boxed{r=4}$ from this odd value as well. (From continued fraction equation)

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

No, it does not work. Since the state should collapse to one of states (such as $4k$, $4k+1$, $4k+2$, $4k+3$). So that after applying QFT we can get eligible results to obtain the period.

Appendix

Matlab Code

```
klength=62;
ilength=2^17;

elmk=zeros(klength,1);
sumk=zeros(klength,1);
total_sum_i=zeros(ilength,1);
amplitude=zeros(ilength,1);

for i=0:1:ilength-1
    for k=0:1:klength-1
        elmk(k+1,1)=exp(2*pi*1j/(2^17)*4*i*k);
        sumk(1,1)=elmk(1,1);

        if(k ~= 0)
            sumk(k+1,1)=elmk(k+1,1)+sumk(k,1);
        end
    end

    total_sum_i(i+1,1)=sumk(klength,1)*(1/sqrt(2^17*62));

    amplitude(i+1,1)=abs(total_sum_i(i+1,1))^2;
end

bar(0:1:2^17-1,amplitude);
```