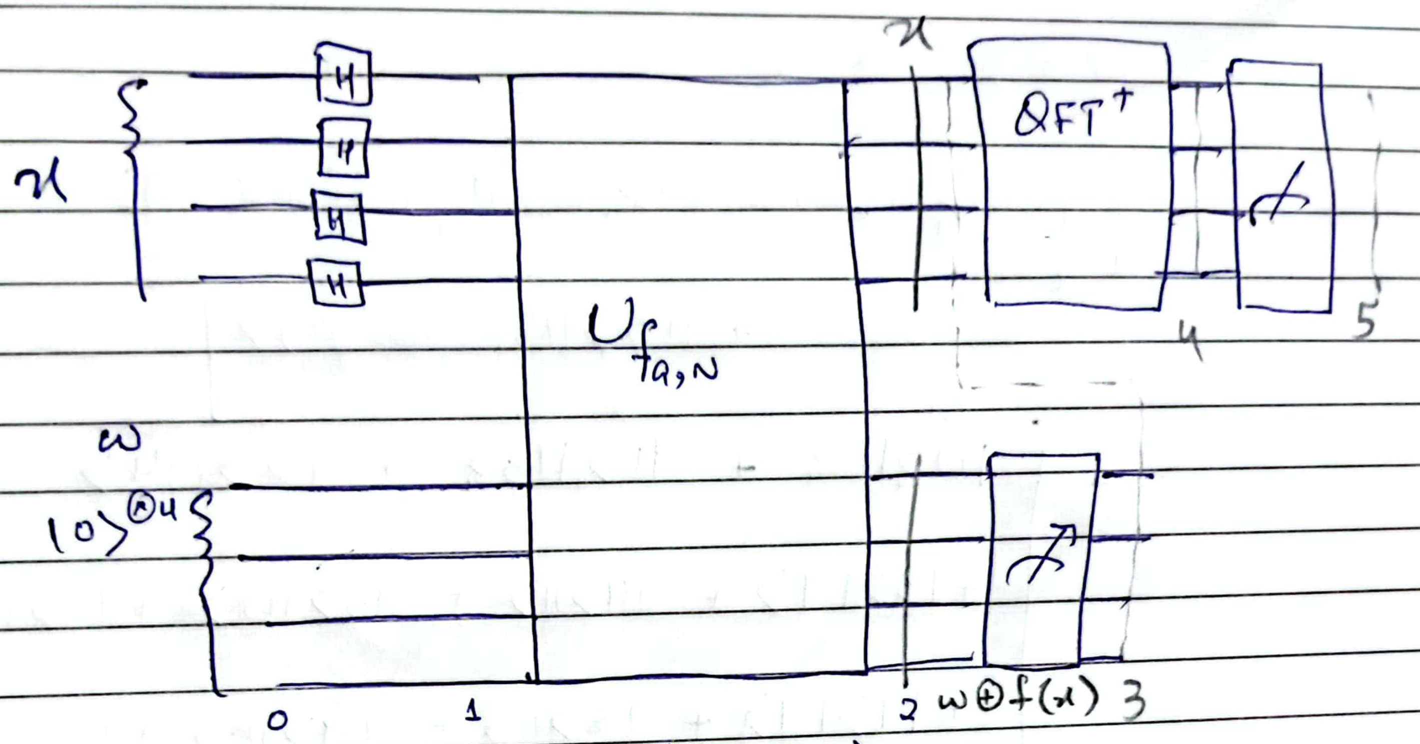


$$f_{a,N}(x) \equiv a^x \, (\text{Mod } N)$$

$$U_{N,a}|y\rangle = |ay \, (\text{Mod } N)\rangle$$

$$|x\rangle|\omega\rangle \longrightarrow |x\rangle|\omega \oplus f_{a,N}(x)\rangle$$

Step 0: $|0\rangle_x^{\otimes 4} \; |0\rangle_\omega^{\otimes 4}$

Step 1 : $H^{\times 4}|0\rangle \; |0\rangle^{\otimes 4}$

$$= \frac{1}{\sqrt{16}}\Big[|0\rangle + |1\rangle + |2\rangle + \dots + |15\rangle\Big]|0\rangle^{\times 4}$$

$$= \frac{1}{4}\Big[|0\rangle|0 \oplus 13^0 (\text{mod } 15)\rangle + |1\rangle|0 \oplus 13^1 (\text{mod } 15)\rangle + \dots + |15\rangle|0 \oplus 13^{15} (\text{mod } 15)\rangle\Big]$$

$$0 \oplus z = z$$

$$= \frac{1}{4}\Big[|0\rangle_4 \, |13^0 (\mathrm{mod}\ 15)\rangle + |1\rangle_4 \, |13^1 (\mathrm{mod}\ 15)\rangle + \dots + |15\rangle |13^{15} (\mathrm{mod}\ 15)\rangle \Big]$$

$$= \frac{1}{4}\Big[\overset{x}{|0\rangle_4}\overset{w}{|1\rangle_4} + \overset{x}{|1\rangle_4}\overset{w}{|13\rangle_4} + \overset{x}{|2\rangle_4}\overset{w}{|4\rangle} + |3\rangle|7\rangle + |4\rangle|1\rangle + |5\rangle|13\rangle + |6\rangle|4\rangle + |7\rangle|7\rangle + |8\rangle|1\rangle + |9\rangle|13\rangle + |10\rangle|4\rangle + |11\rangle|7\rangle + |12\rangle|1\rangle + |13\rangle|13\rangle + |14\rangle|4\rangle + |15\rangle|7\rangle \Big]$$

Step3 : let's measure 7

$|x\rangle$ becomes

$$|x\rangle|w\rangle = \frac{1}{2}\Big[|3\rangle + |7\rangle + |11\rangle + |15\rangle \Big] \otimes |7\rangle$$

Date:

Sun Mon Tue Wed Thu Fri Sat

Step 4: Apply QFT$^+$

$$QFT|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i xy}{N}} |y\rangle$$

$$QFT^+ |\tilde{x}\rangle = |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-\frac{2\pi i xy}{N}} |y\rangle$$

0.38 − i0.92

−0.92 − i0.38

−0.38 + i0.92

$$QFT^+ |3\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{N-1} e^{-\frac{2\pi i 3y}{16}} |y\rangle$$

$$QFT^+ |7\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{N-1} e^{-\frac{2\pi i 7y}{16}} |y\rangle$$

$$QFT^+ |11\rangle = \frac{1}{\sqrt{16}} \sum_{y=0}^{N-1} e^{-\frac{2\pi i 11y}{16}} |y\rangle$$

$$QFT^+ |15\rangle = \frac{1}{\sqrt{16}} \sum_{y=0}^{N-1} e^{-\frac{2\pi i 15y}{16}} |y\rangle$$

$$QFT^+ |x\rangle = \frac{1}{8} \sum_{y=0}^{15} \left[e^{-i\frac{3\pi}{8}y} + e^{-i\frac{7\pi}{8}y} + e^{-i\frac{11\pi}{8}y} + e^{-i\frac{15\pi}{8}y} \right]$$

$$= \frac{1}{8} \left[4|0\rangle + 4i|4\rangle - 4|8\rangle - 4i|12\rangle_4 \right] |y\rangle$$

$$\sum_{k=0}^{r-1} e^{-\frac{2\pi i k}{r}} = 0 \qquad \sum_{y=0}^{N-1} e^{-\frac{2\pi i y}{N}} = 0$$

Step 5: measure $|x\rangle$

$0, 4, 8, 12$ with equal probability

Remaining steps are classical post-processing

You will get only one value

Measurement results peak near $j\frac{N}{r}$ / $j \in \mathbb{Z}$ Period

e.g measure $|4\rangle$ $\quad j\frac{16}{r} = 4$ true $j=1$ $r=4$

$j\frac{16}{r} = 4$

$r=4$

$2 \quad 2 \times \frac{16}{4} = 8 \quad j=2 \quad r=4.$

$16 = 12 \quad j=1 \quad r=2$

$j=2 \quad r=4$

$\frac{s}{r} \quad s \in \quad N\frac{s}{r} = 4 \quad$ r is even.

$r=8$

$j\frac{s}{r}16 = 8 \qquad \frac{s}{r} = 4$

$c = \frac{s}{r}N$

$4 = \frac{s}{r}16 \qquad r=4 \quad s=1$

$s = 0 - r-1$

$\gcd(s,r)=1 \quad 0 \leq s < r$ int

Date
Sun Mon Tue Wed Thu Fri Sat

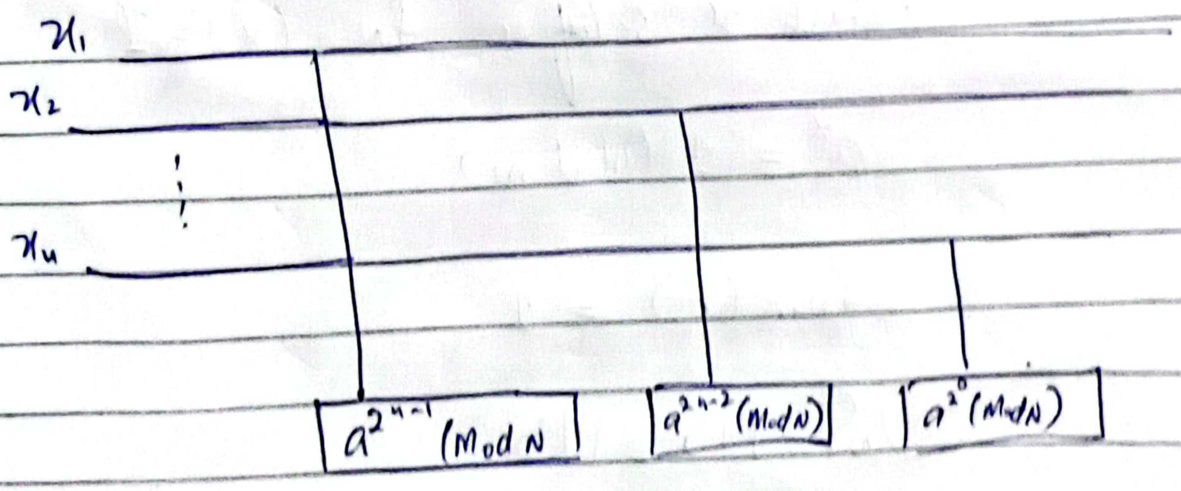
$$f_{a,N}(x) \equiv a^x \ (\mathrm{Mod}\ N)$$

$$x = [x_1 \ x_2 \ x_3 \ \ldots \ x_n] = 2^{n-1}x_1 + 2^{n-2}x_2 + \ldots 2^0 x_n$$

$$f_{a,N}(x) \equiv a^x (\mathrm{Mod}\ N)$$

$$= a^{2^{n-1}x_1 + 2^{n-2}x_2 + \ldots 2^0 x_n} \ (\mathrm{Mod}\ N)$$

$$= a^{2^{n-1}x_1} \cdot a^{2^{n-2}x_2} \ldots a^{2^0 x_n} \ (\mathrm{Mod}\ N)$$



$$U^{2^x} = a^{2^x} \ (\mathrm{Mod}\ N)$$

$$x^2 \equiv 1 \pmod{N}$$

$$x^r \equiv 1 \pmod{N} \qquad r = 2r'$$

$$(x^{r'})^2 \equiv 1 \pmod{N}$$

non trivial square root

$$f_{a,N}(x) = a^x \pmod{N}$$

which x satisfies $f_{N,a}(x) = 1$

$$a^x \equiv 1 \pmod{N}$$

$$f_{N,a}(r) = 1$$

$$U_{N,a}^r |1\rangle \equiv |1\rangle$$

$$U_{N,a}^m |1\rangle = |f_{N,a}(m)\rangle$$