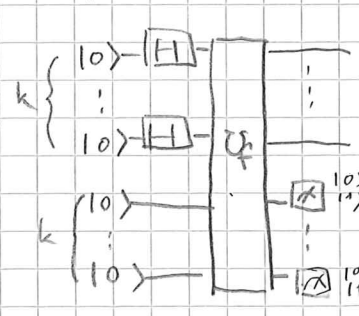
recap from yesterday.

- RSA cryptography $x \to y = x^e$, $x \to y^d \mod N$ ($N = pq$)
  is built on the assumption that
  - solving $ed = 1 \mod \operatorname{lcm}(p-1, q-1)$ (or $\mod (p-1)(q-1)$)
    is easy (polynom time in $\log N$)
  - knowing p, q from N is difficult
    (empirically exp. time in $\log N$).
  - once we know the period of $f(r) = x^r \mod N$
    $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, with high prob. it's easy to compute
    p, q.

- Period problem to Fourier transform (§19.2.2, 20.1)
  consider an analogue of quantum circuit for
  Simon's algorithm:
  $\forall x \quad Q = 2^k$ (will be $\sim N^2$; so we'll need about
  $4 \cdot \log_2 N$ qubits)
  consider the XOR query $U_f : |xy\rangle \mapsto |x\,(y \oplus f(x))\rangle$
  (interpret $f(x)$ as $f(\sum_{0 \le i < k} 2^i x_i)$.
  $U_f : (\mathbb{C}^2)^{\otimes 2k} \to (\mathbb{C}^2)^{\otimes 2k}$

then 

is the state given by
normalization of

$$\sum_{\substack{x \in \{0,1\}^k \\ f(x) = m}} |x\rangle.$$

(cf. Feb 23)

we know that $f(r)$ has a period s (that we want to know)

so we have $|\psi\rangle = \frac{1}{\sqrt{L}} \left(|r\rangle + |r+s\rangle + \cdots + |r+(L-1)s\rangle \right)$
use binary expansions

for some r and L.

treat $(\mathbb{C}^2)^{\otimes k}$ as $\mathbb{C}^Q$ $(Q = 2^k)$

ideally : find an ONB that contains all vectors of the form $\frac{1}{\sqrt{L}}(|r\rangle + \cdots + |r+(L-1)s\rangle)$, and do measurement in this basis to know s.

this is too optimistic, but something close is possible

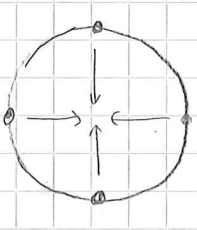
write $\omega = e^{\frac{2\pi i}{Q}}$ (Q-th root of unity)

Prop. 1 $(F_Q)_{j,k} = \frac{1}{\sqrt{Q}}\omega^{jk}$ $(0 \le j,k < Q)$ is unitary

i.e. $|\varphi_k\rangle = \frac{1}{\sqrt{Q}} \sum_{0 \le j < Q} \omega^{jk} |j\rangle$ $(0 \le k < Q)$ is an ONB

Proof. $(F_Q^\dagger)_{j,k} = \frac{1}{\sqrt{Q}}\omega^{*kj} = \frac{1}{\sqrt{Q}}\omega^{-jk}$

$(F_Q F_Q^\dagger)_{j,k} = \sum_\ell (F_Q)_{j,\ell}(F_Q^\dagger)_{\ell,k} = \frac{1}{Q}\sum_\ell \omega^{\ell(j-k)} = \begin{cases} 1 \\ 0 \end{cases}$



Prop 2 when s divides Q, and $L = \frac{Q}{s}$,

$F_Q \frac{1}{\sqrt{L}}(|r\rangle + \cdots + |r+(L-1)s\rangle) = \frac{1}{\sqrt{s}} \sum_{0 \le c < s} \omega^{rc} |cL\rangle$

Proof. in matrix form, we are adding r-th, $(r+s)$-th, $\cdots$ $(r+(L-1)s)$-th columns of F_Q.

$\rightsquigarrow$ j-th component is $\frac{1}{\sqrt{QL}} \sum_{0 \le p < L} \omega^{j\cdot(r+ps)} = \begin{cases} \frac{1}{\sqrt{s}} \cdot \omega^{jr} \\ 0 \end{cases}$

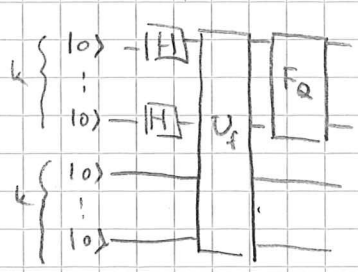
depending on $\omega^{js} = 1$ or not

Suppose s is small rel. to Q.

(for RSA, s divides $\mathrm{lcm}(p-1, q-1) \ll Q \sim p^2q^2$)

then $\frac{1}{\sqrt{s}} \sum_{0 \le c < s} \omega^{rc} |cL\rangle$ is concentrated on a small number of standard basis

(cont.) by measuring the output of



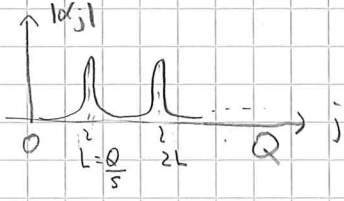
in the first k qubits, we know possible candidates of cL. ($0 \le c < s$)

⇝ can estimate L by taking gcd

⇝ get $s = \frac{Q}{L}$.

- What if s does not divide Q? ($\delta \ge 1$)

intuition: $F_Q |\psi_{r,s}\rangle$ would have coeffs α_j



⇝ measurement gives $|k\rangle$ with $k = c \cdot \frac{Q}{s} \pm \varepsilon$ $\quad |\varepsilon| < 1$

⇝ $\frac{k}{Q} = \frac{c}{s} \pm \varepsilon'$; Q is large and s is small ⇒ $|\varepsilon'| < \frac{1}{Q}$ ⇝ puts restr. on s

Soft answer: we know $s < \sqrt{N}$, so choosing Q big enough would give precise estimate for possible candidates of $\frac{c}{s}$, then get s

More precisely:

Prop 3. Let x $(= \frac{k}{Q})$ be a rational number. Suppose another rational number $\frac{n}{d}$ $(= \frac{c}{s})$ satisfies the estim. $\left|\frac{n}{d} - x\right| \le \frac{1}{2d^2}$

Then then $\frac{n}{d}$ can be computed from the continued fraction presentation of x;

if $x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_M}}}$ then $\frac{n}{d} = a_0 + \cfrac{1}{\ddots + \cfrac{1}{a_m}}$ $(m \le M)$