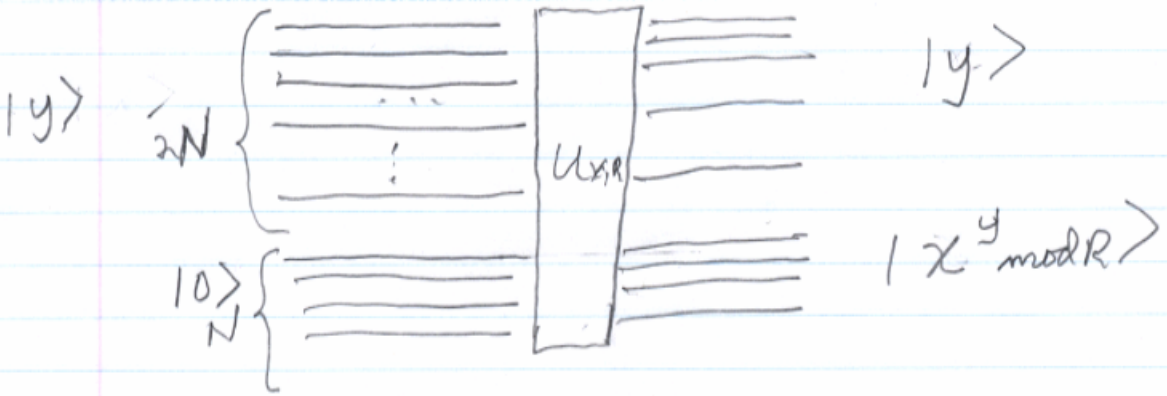
$R = pq$ $\quad 2^N > R > 2^{N-1}$



choose "randomly" so x, R relatively prime (no common factors)

x, R "classical" (known).

Feed in $\sum_{y}^{2^N} \frac{|y\rangle}{2^N}$

Measure second reg of $2N$.

At least 2^N values of y with same value of $(x^y \bmod R)$. spaced "r" apart.

$$\sum_{\lambda=0}^{\geq 2^N} \underbrace{\frac{|\bar{y}_0 + \lambda r\rangle}{\sqrt{\#\lambda}}} |x^{y_0} \bmod R\rangle$$

$\Delta r < \frac{\pi}{2^N}$

$$\Rightarrow \sum_k e^{i k y_0 / 2^{2N}} \sum_\lambda \frac{e^{i\pi k \lambda r / 2^{2N-1}}}{\sqrt{\#\lambda}} = \sum_k \frac{e^{i k y_0 / 2^{2N}}}{\sqrt{\Lambda}} \frac{1 - e^{2\pi i k \Lambda / 2^{2N-1}}}{1 - e^{i k r}}$$

$|k|$

$$P_k = \left(\frac{\sin \pi k r / 2^{2N}}{\sin \pi k r / 2^{2N-2N}} \right)^2$$