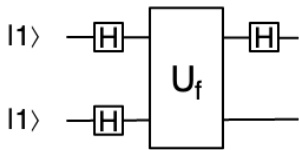


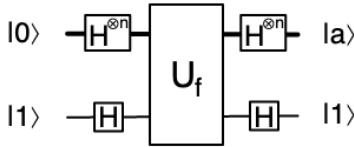
1.



$|1\rangle \quad f(0)=f(1)$
 $|0\rangle \quad f(0)\neq f(1)$

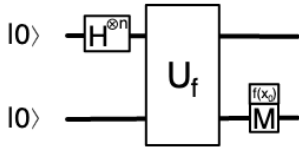
Deutsch '92 (p.44), factor of 2 speedup to determine whether or not 1bit \rightarrow 1bit function $f(x)$ is constant

2.



Bernstein-Vazirani '93 (p.52), $f(x) = a \cdot x \equiv \oplus_i a_i x_i$, factor of n speedup to determine a

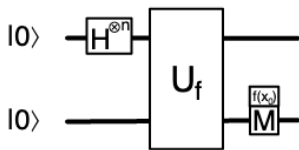
3.



$$\frac{1}{2^{1/2}} (|x_0\rangle + |x_0 \oplus a\rangle) \xrightarrow{\text{H}^{\otimes n}} \text{M}$$

Simon '94 (p.56), $f(x) = f(x \oplus a)$, measured y has $a \cdot y = 0$ (equivalently $\sum_i a_i y_i = 0 \pmod{2}$), exponential speedup ($2^{n/2} \rightarrow O(n)$) to determine a

4.

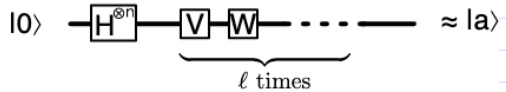
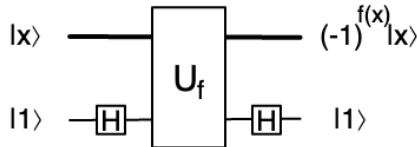


$$\frac{1}{m^{1/2}} \sum_{k=0}^{m-1} |x_0 + kr\rangle \xrightarrow{\text{U}_{\text{FT}}} \text{M}$$

Shor '94 (p.70), $f(x) = f(x + r)$, resulting y is measured with probability $p(y) = \frac{1}{2^{nm}} \left| \sum_{k=0}^{m-1} e^{2\pi i k r y / 2^n} \right|^2$, gives $|y - 2^n/r| < 1/2$ with $p > .4$, sufficient to determine

period r via partial fraction expansion, exponential speedup ($n2^n, \exp(n^{1/3}) \rightarrow O(n^3)$).
 (Note: replaces $\mathbf{H}^{\otimes n} |x\rangle = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{i\pi x \cdot y} |y\rangle$ with $\mathbf{U}_{\text{FT}} |x\rangle = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{2\pi i x y / 2^n} |y\rangle$.)
 Practical application is $f(x) \equiv b^x \pmod{N}$, where $b \equiv a^c \pmod{N}$ is an encrypted message, from which d' , satisfying $cd' \equiv 1 \pmod{r}$, can be calculated, and d' recovers unencrypted message $a \equiv b^{d'} \pmod{N}$ (in contrast to using d , with $cd = 1 \pmod{(p-1)(q-1)}$, where $N = pq$ and r divides $(p-1)(q-1) = |G_{pq}|$).

5.



Grover '96 (p.90), $f(x) = 1$ only for (m) marked value(s) $x = a$, uses "phase kickback" to express \mathbf{U}_f in terms of $\mathbf{V} = \mathbf{1} - 2|a\rangle\langle a|$, and $\mathbf{W} = 2|\phi\rangle\langle\phi| - \mathbf{1} = \mathbf{H}^{\otimes n} (2|0\rangle\langle 0| - \mathbf{1}) \mathbf{H}^{\otimes n}$ is easily constructed. Applying $\ell \approx \frac{\pi}{4} \frac{2^{n/2}}{\sqrt{m}}$ times gives probability $p(a) \approx 1 - O(m/2^n)$, for square-root speedup ($2^n/m \rightarrow \sqrt{2^n/m}$).

$|\varphi\rangle$

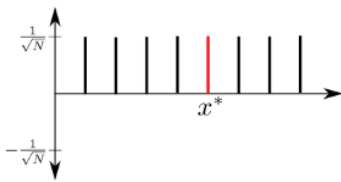


Figure 22.1: The initial amplitudes of the system, an even superposition state.

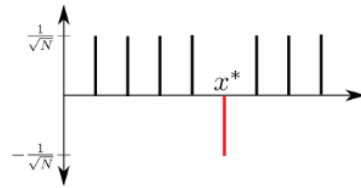


Figure 22.2: The amplitudes following the first application of the phase oracle. Note that the amplitude of the marked item has had its sign flipped.

$V|\varphi\rangle$

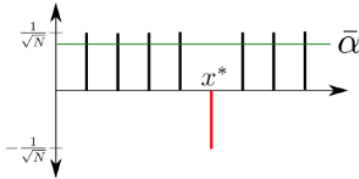


Figure 22.3: The average amplitude $\bar{\alpha}$ has been explicitly drawn in.

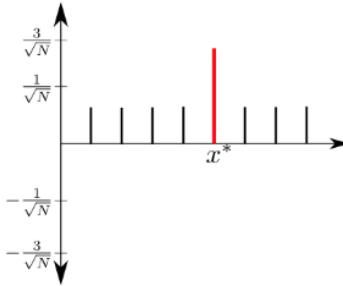


Figure 22.4: The amplitudes following the first Grover diffusion operator.

$WV|\varphi\rangle$

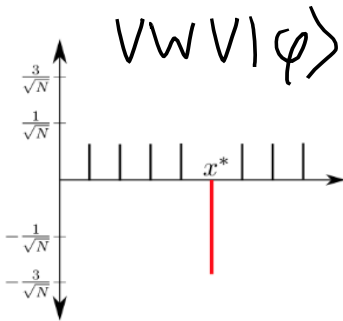


Figure 22.5: Amplitudes following the second application of the phase oracle. Note that the amplitude of the marked item has had its sign flipped again.

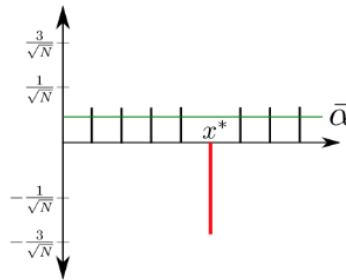


Figure 22.6: Amplitudes following the second application of the phase oracle with the new average amplitude $\bar{\alpha}$ explicitly drawn in.

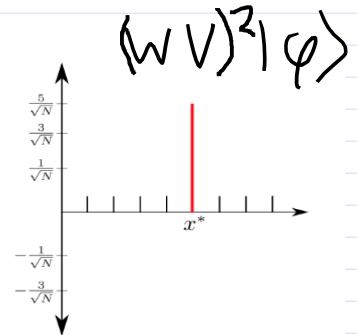


Figure 22.7: Amplitudes following the second Grover diffusion operator.

$(WV)^2|\varphi\rangle$

m marked states

$$f(x) = \begin{cases} 1 & x \in Y \\ 0 & x \notin Y \end{cases}$$

$$V|x\rangle = (-1)^{f(x)} |x\rangle$$

$Y =$ set of marked states

$$|Y| = m$$

$$|\varphi\rangle = \frac{1}{\sqrt{2^n}} \sum_{0 \leq x < 2^n} |x\rangle = \cos\theta |no\rangle + \sin\theta |yes\rangle$$

$$|yes\rangle = \frac{1}{\sqrt{m}} \sum_{x | f(x)=1} |x\rangle$$

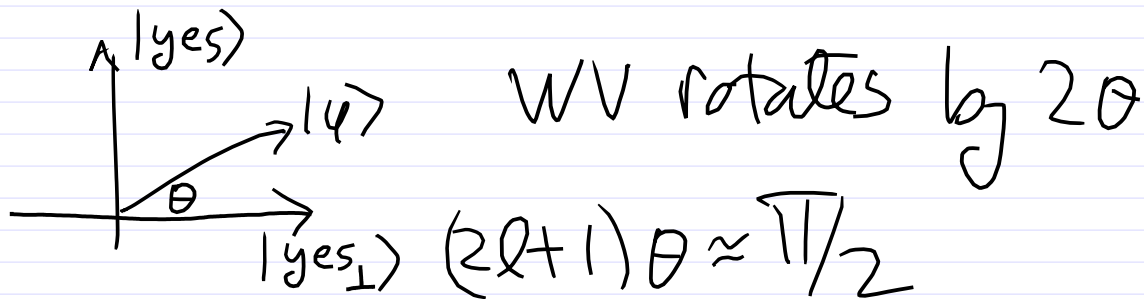
$$|no\rangle = \frac{1}{\sqrt{2^n - m}} \sum_{x | f(x)=0} |x\rangle$$

$$\sin\theta = \langle yes | \varphi \rangle = \sqrt{\frac{m}{2^n}}$$

$$\cos\theta = \langle no | \varphi \rangle = \sqrt{1 - \frac{m}{2^n}}$$

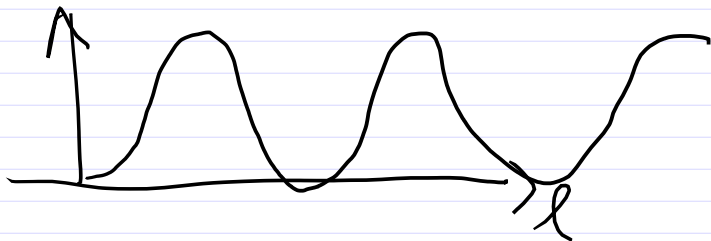
$$V = | -2 | \text{yes} \rangle \langle \text{yes} |$$

$$W = 2 | \varphi \rangle \langle \varphi | - 1$$



$$\theta \approx \sqrt{\frac{m}{2^n}} = \sqrt{\frac{m}{N}}$$

$$l \approx \frac{\pi}{4} \sqrt{\frac{N}{m}}$$



$\langle \text{yes} | (WV)^n | \varphi \rangle$ is periodic

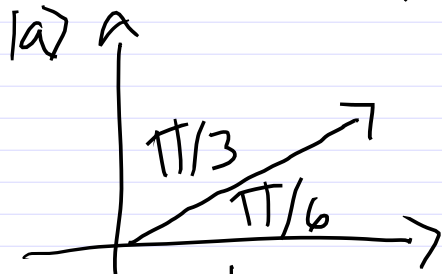
$\approx \sin 2l\theta$ in $l \pm \pi/\theta$

so period = $\frac{\pi 2^{n/2}}{\sqrt{m}}$.

Run QFT to get period, gives m
then Grover $\frac{\pi}{4} \sqrt{N/m}$ times

A special case: $m=1$ $n=2$ ($N=4$)

$$\sin \theta = \langle a | \varphi \rangle = \frac{1}{2^{n/2}} = \frac{1}{2} \quad \theta = \pi/6$$



WV rotates by $\pi/3$
single WV exactly $|a\rangle$

Q.M.: $\frac{1}{4}$ | classically: $\frac{1}{4} \cdot 1 + \frac{3}{4} \frac{1}{3} 2 + \frac{1}{2} 3$
expect $= 2 \frac{1}{4}$

Just choose N/m states

$$N = 200 \quad m = 10 \quad \text{pick } \frac{200}{10} = 20$$

prob of
at least
one

$$1 - \left(\frac{19}{20}\right)^{20} \approx 1 - e^{-1}$$

prob of exactly one $\approx e^{-1}$ (Poisson)

Then run ordinary Grover

$$\sqrt{\frac{N}{m}}$$

Collision problem

N items, classically check m

$$N \sim \frac{1}{2} m(m-1) \quad \text{so need } m \sim N^{1/2}$$

Quantum: look at some fraction

$m \sim N^a$, call them marked

Grover $\sqrt{\frac{N}{m}} \sim \left(\frac{N}{N^a}\right)^{1/2}$

optimum $N^a \sim N^{(1-a)/2}$

$$a = \frac{1-a}{2}$$

$$\Rightarrow \boxed{a = 1/3}$$

So both

$$N^{1/3}$$

Parity of n bits QM $n/2$ (barely speed up)

OR (any one is on) NO speed up

Why $N^{1/2}$?

classically work with probabilities
 $1/N, 2/N, \dots, m/N \sim 1$

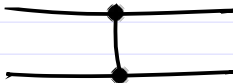
QM: work with amplitudes
 $1/\sqrt{N}, 2/\sqrt{N}, 3/\sqrt{N}, \dots, T/\sqrt{N} \quad T^2/N \sim 1$

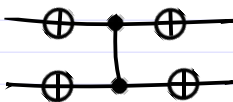
How to implement W

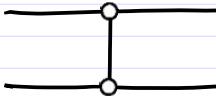
$$-W = | -2| \psi \rangle \langle \psi |$$

$$= H^{\otimes n} \left(| -2| \underbrace{0 \rangle_n \langle 0|_n}_{X^{\otimes n} C^{n-1} Z X^{\otimes n}} \right) H^{\otimes n}$$

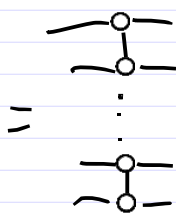
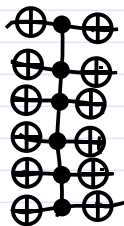
$n=2$

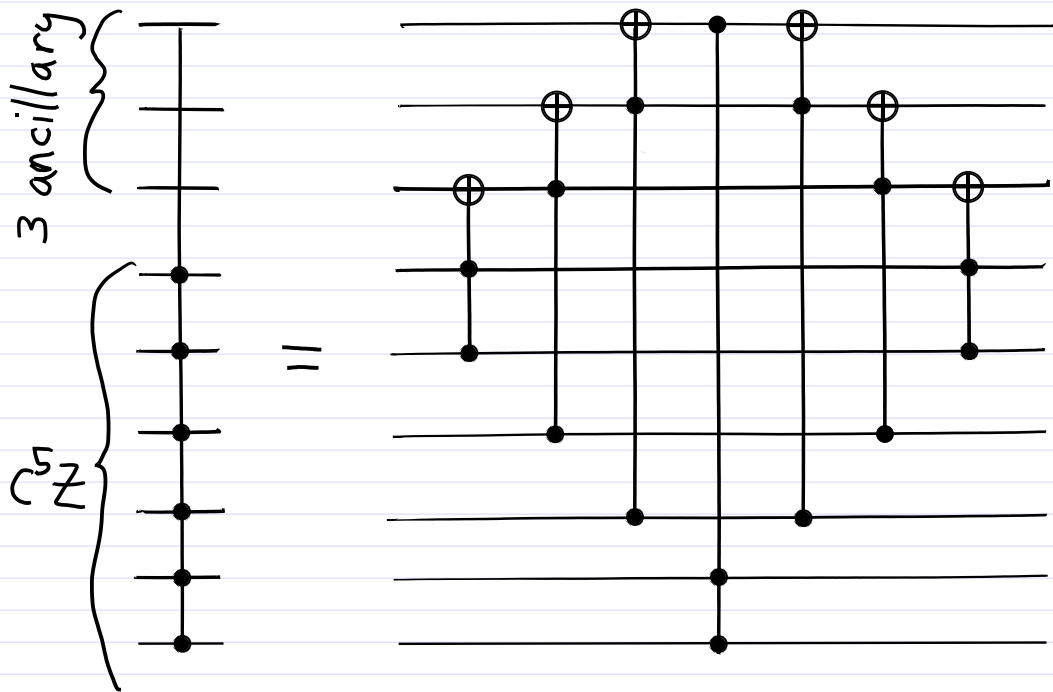
$$| -2| 111 \rangle \langle 111 | =$$


$$| -2| 00 \rangle \langle 00 | =$$


$$=$$


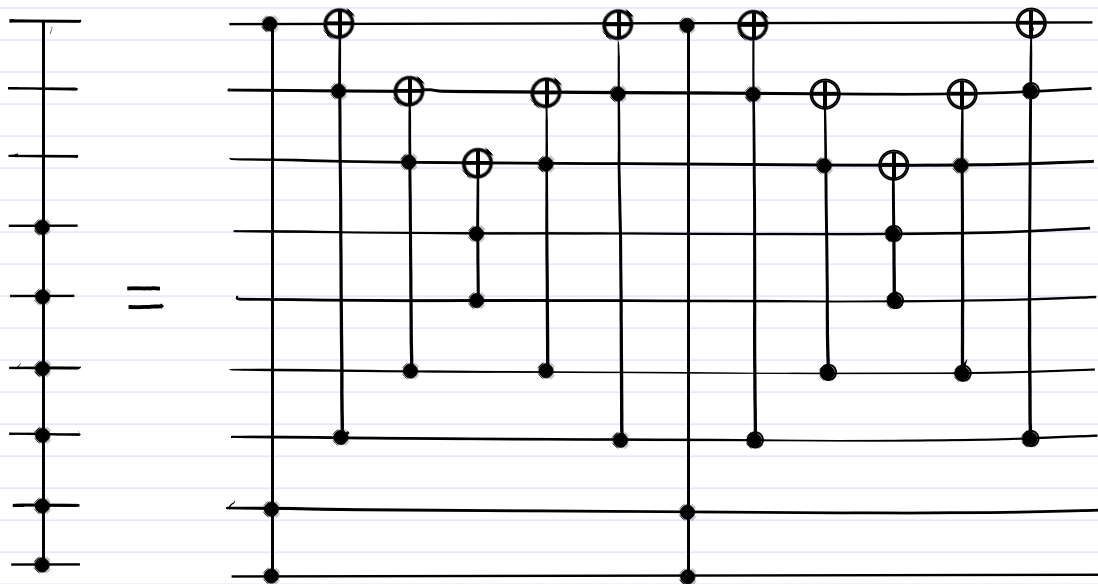
n





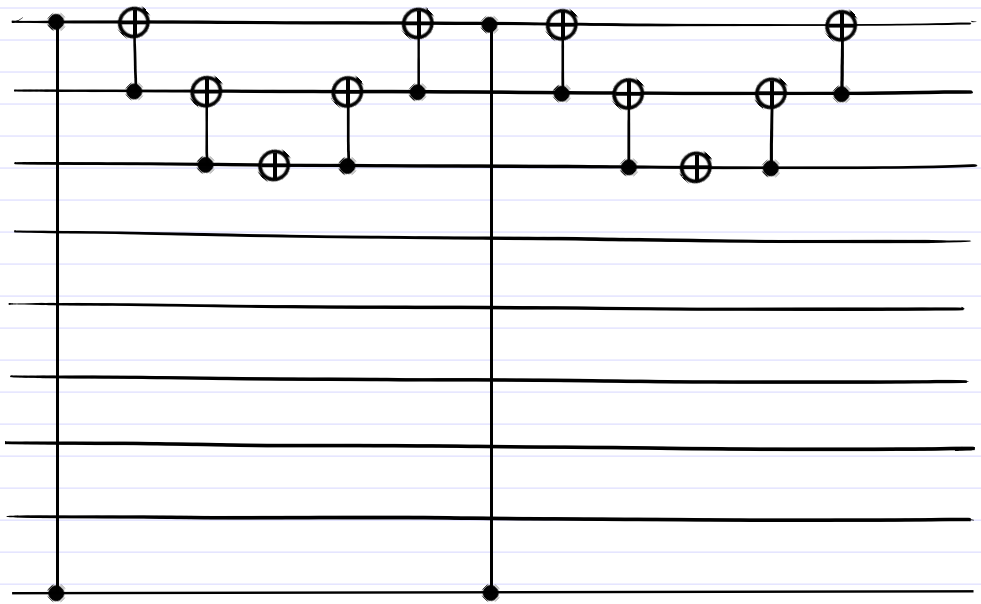
One way to construct
multiple $C^{n-1}Z$ and W

For n -fold $C^{n-1}Z$, needs $n-3$ ancillary
initialized to $|0\rangle$

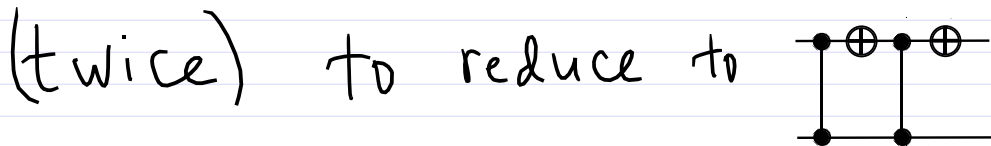
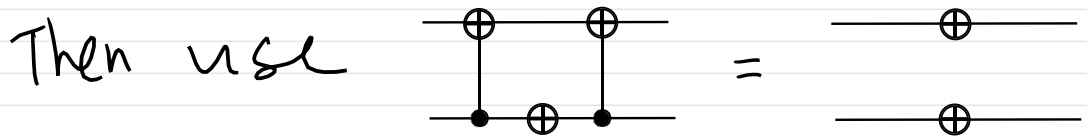


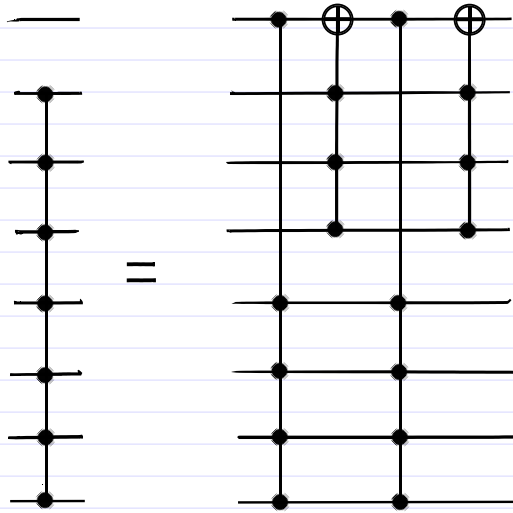
Now the ancillaries can have any states (or even be entangled with other qubits)

If any of the upper four (of six) are $|0\rangle$, then reduces to identity (pairwise cancellation)



If the upper five (of six) are all on, becomes the above.





Above a construction where the ancillaries of some can be the control bits of others

Quantum Key Distribution

100% provably secure encryption

One-time pad

m = message, n bits

r = n random bits

$C = m \oplus r$ encoded message

never reuse r

[Careful $m_0 \oplus r = C_0$ $m_1 \oplus r = C_1$

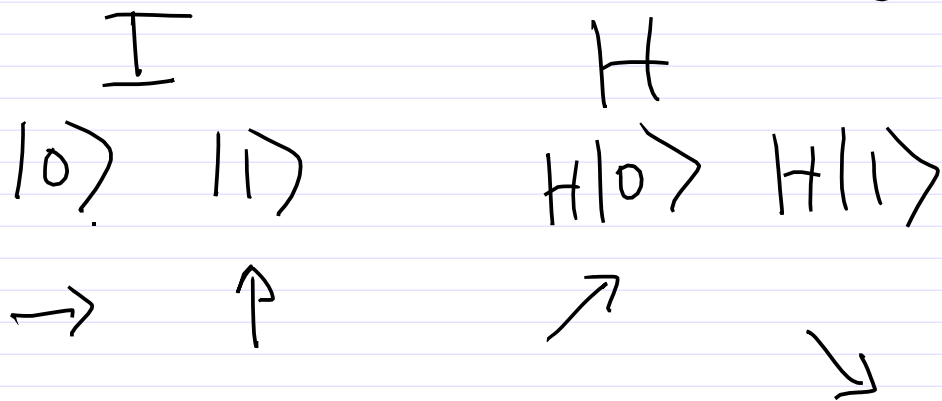
Then $C_0 \oplus C_1 = m_0 \oplus m_1$

has direct info on m_0, m_1

(r cancels if reused)]

QKD is a secure way of transmitting a one-time pad

Alice & Bob can agree on a one-time pad and they know if intercepted by Eve



Alice sends photons to Bob and each chooses independently H, I. If they choose same + measure then get same result.

But if e.g. Alice $H|0\rangle$ and Bob measures -- only 50% agreement w/o H

Alice prepares	I	H	H	H	I	I	H	I	H
Bob measures	H	H	H	I	I	H	I	I	I
	0	1	0	1	1	0	1	0	0
	1	1	0	0	1	1	1	0	0

By classical channel,
communicate sequence of H, I,
identify the roughly 50% same choice.

Discard the rest!

How do they know if intercepted by
Eve? she has to guess I, H
and measure. But if she guesses
wrong, e.g., doesn't apply H, measures,

$H|0\rangle \xrightarrow{E} |0\rangle$ then forwards to
 \searrow Bob, he applies H
 $E \rightarrow |1\rangle$ and half the time
his measurement will disagree with Alice.

Alice and Bob sacrifice some of their good bits and exchange via public channel.

Eve guesses H, I correctly

50% of time. If guesses wrong, then Bob's measurement corrupted half of those times.

so $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ of the sacrificed bits will disagree if eavesdrop:

$$P_{\text{detect}}^{\text{Eve}} = 1 - \left(\frac{3}{4}\right)^n \quad \text{For } n=72 \text{ Sacrificed,}$$

(all agree)

$$\approx .999999999 \approx 1 - 10^{-9}$$

Can Eve do anything more?

$$|\varphi_m\rangle = |0\rangle_0 |1\rangle_1 |H0\rangle_2 |H1\rangle_3$$

$$U|\varphi_m\rangle|\varphi\rangle_n = |\varphi_m\rangle|\varphi_m\rangle_n$$

U preserves inner product

$$\langle\varphi_\nu|\varphi_m\rangle\langle\varphi|\varphi\rangle = \langle\varphi_\nu|\varphi_m\rangle\langle\varphi_\nu|\varphi_m\rangle$$

$$\langle\varphi_\nu|\varphi_m\rangle \neq 0 \quad \text{for } \nu, m = \begin{matrix} 0 & 2 \\ 0 & 3 \\ 1 & 2 \\ 1 & 3 \end{matrix} \quad |\varphi_0\rangle = |\varphi_2\rangle \\ = |\varphi_1\rangle \\ = |\varphi_3\rangle$$

so can't obtain distinguishing info
and leave state $|\varphi_m\rangle$ uncorrupted

What if Alice, Bob share an entangled $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$?

Still need random choice of H

$$(H \otimes H) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

doesn't buy an advantage:

Once measured, equivalent to earlier protocol.

Only difference: QM makes choice of $|0\rangle, |1\rangle$ (or $H|0\rangle, H|1\rangle$)
(BB84) see also Eq 1



Vienna

