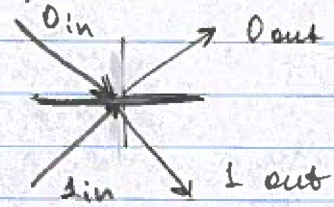
General qubit form

$|Q\rangle = \alpha|0\rangle + \beta|1\rangle$

Single qubit transformation

example: Hadaman transformation (gate) H

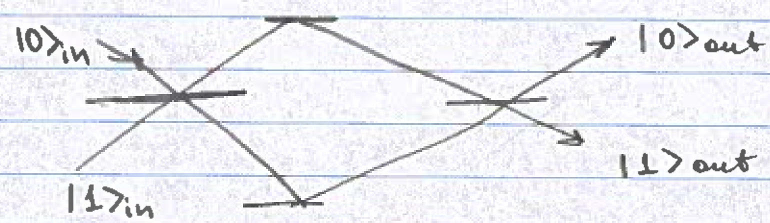
quantum beam splitter



$$|Q\rangle_{out} = \frac{1}{\sqrt{2}}\left((\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle\right)$$

$$= H|Q_{in}\rangle$$

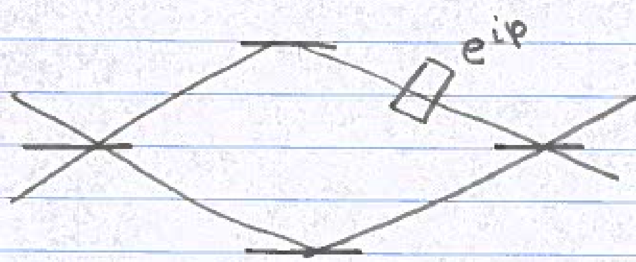
Balanced Mach-Zender interferometer



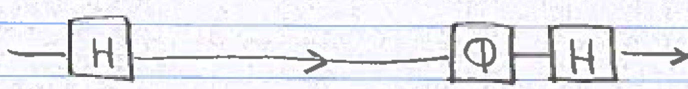
$$|Q\rangle_{out} = HH|Q_{in}\rangle = |Q_{in}\rangle$$

General Mach-Zender interferometer

2 Hadaman + 1 phase-shifter gates



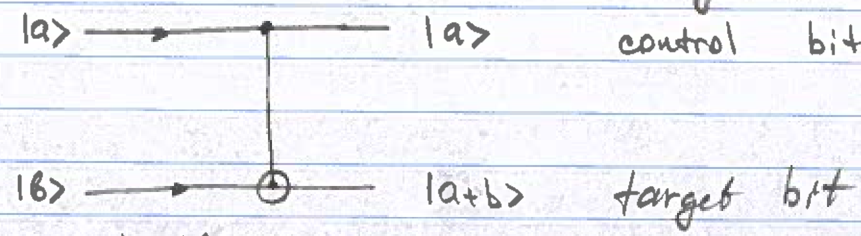
$$\Phi|0\rangle = e^{i\varphi}|0\rangle$$
$$\Phi|1\rangle = |1\rangle$$



$$|Q\rangle_{out} = H\Phi H|Q\rangle_{in} = \frac{1}{2}\left\{(e^{i\varphi}+1)|0\rangle + (e^{i\varphi}-1)|1\rangle\right\}$$

Another type of gates required
two-qubit gates

CNOT (controlled NOT gates)



$|a\rangle|b\rangle$

$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$

$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle$

$|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$

$|1\rangle|1\rangle \longrightarrow |1\rangle|0\rangle$

To realize these gates experimentally, a single-photon nonlinearity must be realized — very challenging, not yet demonstrated

CNOT gates can be used to entangle two particle

control: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\Rightarrow$ output

target: $|0\rangle$ $\qquad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

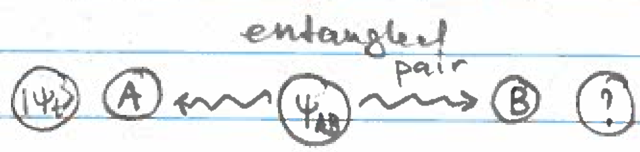
Quantum teleportation

It is impossible to copy a quantum state - no clone theorem

The goal of teleportation is to replicate an unknown quantum state from one location to another

We here will consider a test quantum state $|\psi_t\rangle$ that is a superposition of two known quantum states

$$|\psi_t\rangle = c_0|0\rangle + c_1|1\rangle$$



$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

Total quantum state of a system with three particles:

$$|\Phi_3\rangle = |\psi_t\rangle \otimes |\psi_{AB}\rangle = (c_0|0\rangle + c_1|1\rangle)\otimes$$

$$\otimes \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) =$$

$$= \frac{1}{\sqrt{2}}\Big(c_0|0\rangle|0\rangle_A|0\rangle_B + c_0|0\rangle|1\rangle_A|1\rangle_B + c_1|1\rangle|0\rangle_A|0\rangle_B + c_1|1\rangle|1\rangle_A|1\rangle_B$$

Step 1: Alice performs Bell's measurements. The key to the quantum teleportation is to measure the joint state of the test state and the A state, using Bell's basis

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle_A \pm |1\rangle|1\rangle_A\right)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle_A \pm |1\rangle|0\rangle_A\right)$$

$\Downarrow$

$$|0\rangle|0\rangle_A = \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle + |\Phi^-\rangle\right)$$
$$|1\rangle|1\rangle_A = \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle - |\Phi^-\rangle\right)$$

$$|0\rangle|1\rangle_A = \frac{1}{\sqrt{2}}\left(|\Psi^+\rangle + |\Psi^-\rangle\right)$$
$$|1\rangle|0\rangle_A = \frac{1}{\sqrt{2}}\left(|\Psi^+\rangle - |\Psi^-\rangle\right)$$

$$|\Phi_3\rangle = \frac{1}{2}\Big(c_0(|\Phi^+\rangle + |\Phi^-\rangle)|0\rangle_B + c_0(|\Psi^+\rangle + |\Psi^-\rangle)|1\rangle_B +$$

$$+ c_1(|\Psi^+\rangle - |\Psi^-\rangle)|0\rangle_B + c_1(|\Phi^+\rangle - |\Phi^-\rangle)|1\rangle_B\Big) =$$

$$= \frac{1}{2}\Big\{|\Phi^+\rangle\left(c_0|0_B\rangle + c_1|1\rangle_B\right) + |\Phi^-\rangle\left(c_0|0\rangle_B - c_1|1\rangle_B\right) +$$

$$+ |\Psi^+\rangle\left(c_0|1\rangle_B + c_1|0\rangle_B\right) + |\Psi^-\rangle\left(c_0|1\rangle_B - c_1|0\rangle_B\right)\Big\}$$

Alice performs the measurements in the basis of $|\Phi^{\pm}\rangle; |\Psi^{\pm}\rangle$ states. That projects Bob's particle in one of four states:

$$\langle\Phi_3|\Phi^{\pm}\rangle \;/\; \langle\Phi_3|\Psi^{\pm}\rangle$$

Alice measures:	Bob's state
$\|\Phi^+\rangle$	$c_0\|0\rangle_B + c_1\|1\rangle_B$
$\|\Phi^-\rangle$	$c_0\|0\rangle_B - c_1\|1\rangle_B$
$\|\Psi^+\rangle$	$c_0\|1\rangle_B + c_1\|0\rangle_B$
$\|\Psi^-\rangle$	$c_0\|1\rangle_B - c_1\|0\rangle_B$

↑
each of these measurements occures with probability 1/4

Step 2: Bob may need to tweak his particle, depending on Alice's result

Alice's outcome	Bob has to	For photons
$\|\Phi^+\rangle$	do nothing	—
$\|\Phi^-\rangle$	$\|1\rangle_B \to -\|1\rangle_B$	add 180° phase shift to one of the polarizations
$\|\Psi^-\rangle$	$\|1\rangle_B \to \|0\rangle_B$ $\|0\rangle_B \to -\|1\rangle_B$	rotate both polarizations
$\|\Psi^+\rangle$	$\|1\rangle_B \to \|0\rangle_B$ $\|0\rangle_B \to \|1\rangle_B$	both rotate polarization and flip the phase

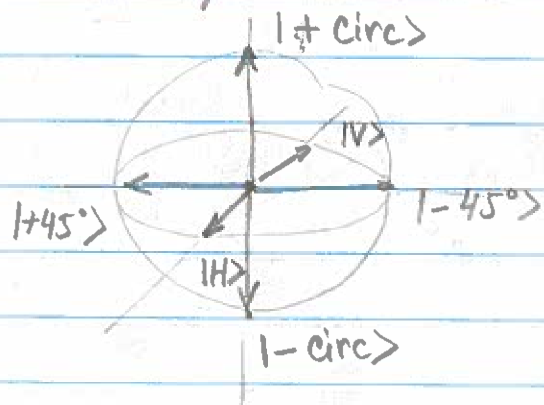
Quantum information

Information is recorded and transmitted in a quantum state (i.e. in a superposition of known energy states)

Example: polarization of a single photon: $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$
$= \alpha|0\rangle + \beta|1\rangle$ (quantum binary)

As a result, unlike classical digital state, a qubit is continuously-valued

It is customary to use a Poincare sphere to desribe possible states of a polarization qubit.



It is possible to modify qubit state using linear opics elements (i.e waveplates) polariz- or quantum gates (later)

Qubit is a minimum unit of quantum information.

No-teleportation theorem (confusing name!)

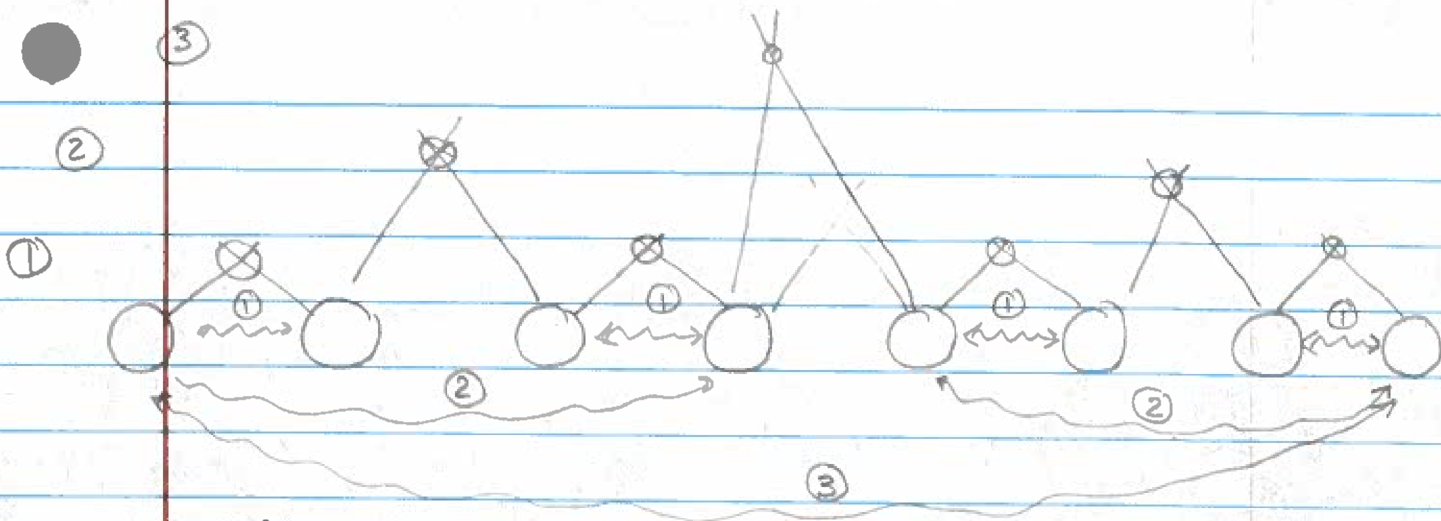
No qubit can be fully converted into a sequence of classical bits (no complete measurements)

No - cloning and no - deleting theorems
An arbitrary qubit cannot be
copied or destroyed completely

No broadcast theorem : a qubit cannot be delivered to multiple recipients.

Transmission of quantum information

Quantum information (i.e a string of qubits) is very susceptable to losses (which act like partial measurements, altering the state, but without providing any useful information)
Consequence: long - distance quantum channels are one of the biggest challenges right now.
Teleportation may be a solution (if an entanglement is established b/w two distant locations, it should be possible to teleport a state, rather than send it along a lossy channel)
↳ need for efficient quantum repeater protocols that allow extending quantum entanglement



Efficient quantum repeater requires quantum memory — ability to preserve qubit/node quantum state in case any other steps fail and have to be repeated.

Quantum information applications

A lot of motivation (and funding) is motivated by the information security.

On one hand: a quntum computer may destroy existing classical cryptography principles.

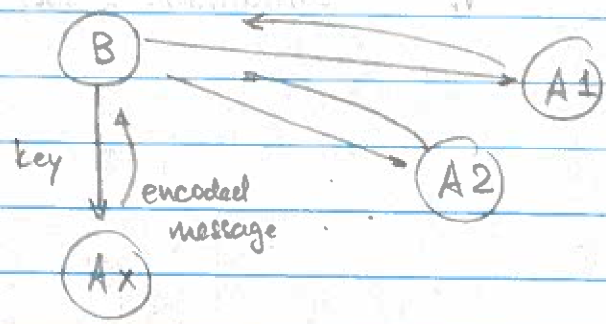
On the other hand, quantum telecommunication may offer a new, fundamentally secure, way of data transmision

1. Most secure information channel - private. Alice and Bob are the only two individuals who know the information. Very resource - intensive

2. Private key for encryption / decryption, information is encoded and moved along public channel (anyone can access the information)
Eve → malicious and very resourceful being, able to retrieve any classical information transmitted over the public channel. (eavesdropper)
Challenge - safe private key sharing, especially in case of many participants.
Also, an encoding algorithm should be complicated enough so that when used repeatedly, Eve cannot figure it out

Currently used cryptoghaphy model

Public key → known to everyone



all information channel involved a public (i.e. Eve has access to <u>all</u> the information)

Only Bob knows how to desipher the messages.

RSA protocol: – pick to prime numbers p, q $(>10^{1000})$

ex: 23, 11

– calculate $N = p \cdot q$ [253] and $p \cdot q(N)$ [220] ← totient

– find a number e that is co-prime with $pq(N)$ (i.e does not have any common factors, greater than 1) [$220 = 2 \cdot 5 \cdot 11$, so $e = 7$]

– (e, N) become a public key (broadcasted), and Alice can encode her message m using the rule: code $c = m^e \pmod N$

– The hardest part is to decode the message. Since Bob knows all the numbers, he can find the modular multipicative inverse d, such that $(m^e)^d \pmod N = m$

$$d = e^{-1} \pmod{pq(N)}$$

– Decoded message $m = c^d \pmod N$

In principle, Eve can crack the code easily if she figures out the factors of $N = p \cdot q$

However, with larger numbers this is a computationally very hard, so the security relies on that fact.

Quantum computers can potentially change that.

Shore's algorithm → quantum algorithm that can factor the numbers in polynomial time (not exponential)

So far the largest factored # = 21 (2012)

Adiabatic quantum computation

largest factored # - 56153

Alternative → quantum cryptoghaphy

Quantum key distribution

A & B are able to create a private key over public channel

Security is guaranteed by QM principles of impossibility to obtain a complete information about the quantum state

BB - 84

Alice creates bits (single photons) in two bases: $|H\rangle$ or $|V\rangle$ ($|0\rangle$, $|1\rangle$)

$|+\rangle$ or $|-\rangle$ $\left(|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)\right)$

(in optics it is equivalent to horizontal / vertical polarizations or $+45°/-45°$ polarizations)

Bob measures in the same to bases (independently of Alice)

They compare the sequence of bases used over the public channel, discard any mismatches, remaining bits can be used as an encryption key.

If Eve intersepts any bits and replaces them with "best guesses", she still will be wrong 50% of the time, and comparison of A&B measurements will reveal her presence.

B 92 protocol

Alice & Bob generate 2 random sequences $a(A)$ and $a'(B)$

A sends only 2 states: $\begin{cases} \text{"0"} & |H\rangle \\ \text{"1"} & |+\rangle \end{cases}$

to transmit a

(non- orthogonal states!)

Bob uses two detection bases to detect; according to a': "0" – $|H\rangle$ & $|V\rangle$

"1" – $|+\rangle$ & $|-\rangle$ (or $|0'\rangle$ & $|1'\rangle$)

Four possible outcomes

Alice has...		Bob has.	Bob measures
$a=$ 0	$\lvert H\rangle$ →	$a'=$ 0	0
1	$\frac{1}{\sqrt{2}}(\lvert H\rangle+\lvert V\rangle)$ →	0	0 or 1
0	$\frac{1}{\sqrt{2}}(\lvert +\rangle+\lvert -\rangle)$ →	1	0 or 1
1	$\lvert +\rangle$ →	1	0

If we keep only the "1" outcomes, that means $a \neq a'$; so Alice and Bob can figure out the key.

(again, statistical analysis of the results will reveal Eve's presence)

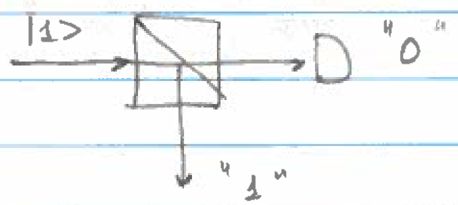
Ekert protocol

A&B share entangled pair
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

Similar to BB84, each person measures in its own random basis, then compare the results, and keep only matching measurements.

Quantum random number generators
Classical random numbers are often generated using a rapidly oscillating function → but if the function is known, Eve can figure ~~out~~ what bases sequence will be used

Quantum mechanics provides an excellent source of true randomness:
single photon



quantum noise