

Practical Quantum Computing

Lecture 5 No-Cloning, QKD, Quantum Games

based on *Quantum Computing: Lecture Notes* by Ronald de Wolf <https://homepages.cwi.nl/~rdewolf/qcnotesv2.pdf>

No-Cloning Theorem

One could, with high probability, **learn** a qubit state, if there was a way to make copies of a qubit

- prior to making the measurement
- without running the whole computation over again

Copy the state of $|q\rangle$ to the **clean register** $|0\rangle$

$$U|q\rangle|0\rangle = |q\rangle|q\rangle$$

Assume two arbitrary states $|a\rangle$ and $|b\rangle$

$$U(|a\rangle|0\rangle) = |a\rangle|a\rangle \text{ and } U(|b\rangle|0\rangle) = |b\rangle|b\rangle$$

Moreover

$$U(a|a\rangle + b|b\rangle)|0\rangle = U(a|a\rangle|0\rangle) + U(b|b\rangle|0\rangle) = a|aa\rangle + b|bb\rangle$$

$$U(a|a\rangle + b|b\rangle)|0\rangle = (a|a\rangle + b|b\rangle)(a|a\rangle + b|b\rangle) = a^2|aa\rangle + b^2|bb\rangle + ab|ab\rangle + ab|ba\rangle$$

No-Cloning Theorem

Moreover

$$U(a|a\rangle + b|b\rangle)|0\rangle = U(a|a\rangle|0\rangle) + U(b|b\rangle|0\rangle) = a|aa\rangle + b|bb\rangle$$

$$U(a|a\rangle + b|b\rangle)|0\rangle = (a|a\rangle + b|b\rangle)(a|a\rangle + b|b\rangle) = a^2|aa\rangle + b^2|bb\rangle + ab|ab\rangle + ab|ba\rangle$$

Such that

$$a = a^2$$

$$b = b^2$$

$$ab = 0$$

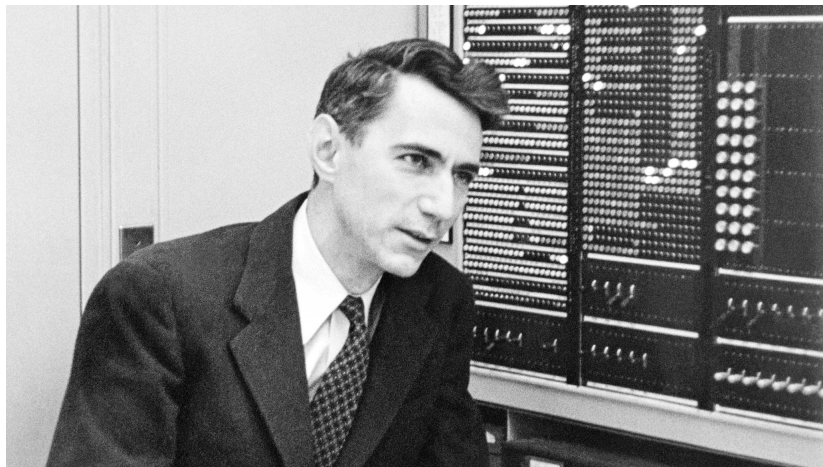
Only if $a=0$ and $b=0$

**Arbitrary quantum
states cannot be
copied !**

One-Time Pad (OTP)

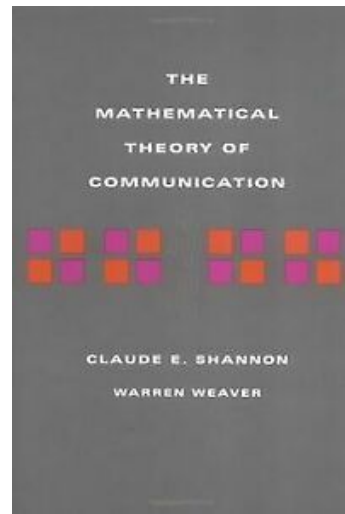
Encrypt a secret message with a *random key* is as long as the message itself

- cipher will not be crackable.
- communication partner must have the same key
- cannot use the same key twice



If Alice and Bob:

- share a secret key $K \in \{0,1\}^n$
- Alice can send $C = M \oplus K$ over the channel
- Bob learns M by adding K to what he received $C = (M \oplus K) \oplus K$
- if Eve didn't know anything about K then she learns nothing about M from tapping the message $M \oplus K$ that goes over the channel.

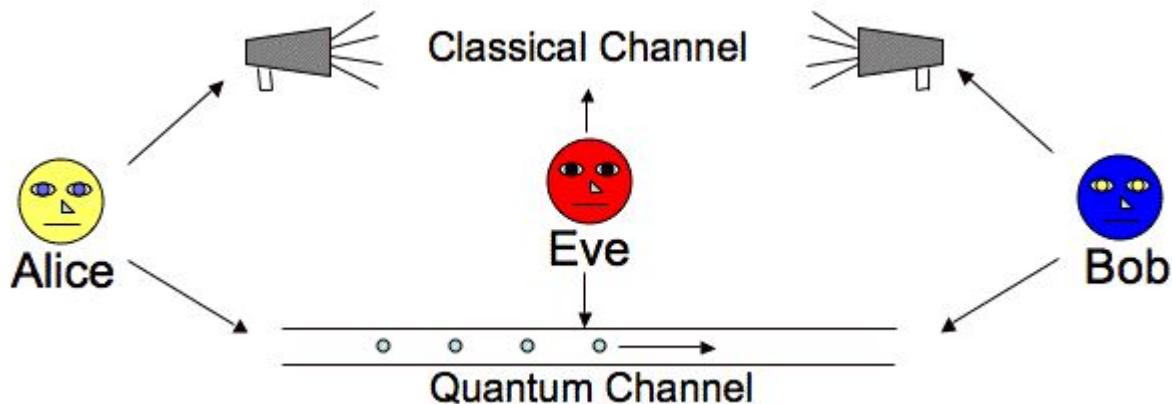


Quantum Key Distribution

How do you distribute a secret key without meeting in person?

The basic model for QKD protocols involves two parties

- wishing to exchange a key
- both with access to a classical public communication channel
- a quantum communication channel.



Fundamental: Eve cannot eavesdrop without affecting the qubit stream between Alice and Bob.

BB84: Bennett and Brassard 1984

The main property of quantum mechanics that we'll use:

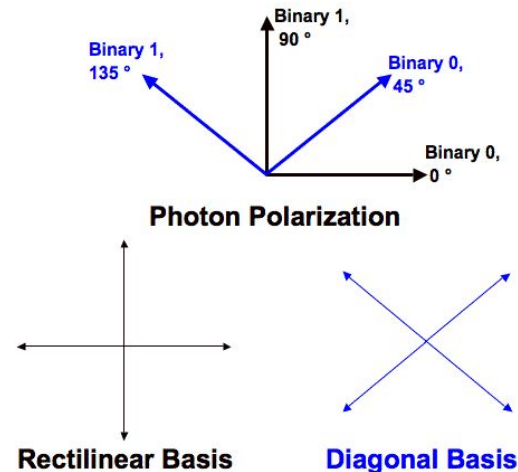
- if a bit b is encoded in an unknown basis
- Eve cannot get information about b without disturbing the state
- the latter can be detected by Alice and Bob

Consider two possible bases:

- 0: Z basis is the computational basis $|0\rangle, |1\rangle$
- 1: X basis is the Hadamard basis $|+\rangle, |-\rangle$

BB84 protocol:

1. Alice chooses n random bits a_1, \dots, a_n and n random bases b_1, \dots, b_n .
 - a. She sends a_i to Bob in basis b_i over the public quantum channel
 - b. For example, if $a_i = 0$ (value) and $b_i = 1$ (basis) then the i th qubit that she sends is in state $|+\rangle$
2. Bob chooses random bases b'_1, \dots, b'_n
 - a. measures the qubits he received in those bases
 - b. yielding bits a'_1, \dots, a'_n



BB84: Bennett and Brassard 1984

3. Bob sends Alice all b_i , and Alice sends Bob all b_i
 - a. For roughly $n/2$ of the i 's, Alice and Bob used the same basis $b_i = b_i$
 - b. For those i 's Bob should have $a_i = a_i$
 - i. if there was no noise
 - ii. Eve didn't tamper with the i -th qubit on the channel
 - c. Both Alice and Bob know for which i 's this holds
 - d. Let's call these roughly $n/2$ positions the **shared string**
4. Alice randomly selects $n/4$ locations in the shared string, and sends Bob those locations as well as the value of a_i at those locations.
 - a. Bob then checks whether they have the same bits in those positions
 - b. If the fraction of errors is bigger than some number p , then they suspect some eavesdropper was messing with the channel, and they abort
 - c. The number p can for instance be set to the natural error-rate that the quantum channel would have if there were no eavesdropper

Quantum Key Distribution

4. If the test is passed
 - a. then they discard the $n/4$ test-bits,
 - b. have roughly $n/4$ bits left in their shared string. This is called the **raw key**
5. Now they do some classical post processing on the raw key:
 - a. “information reconciliation” to ensure they end up with exactly the same shared string
 - b. “privacy amplification” to ensure that Eve has negligible information about that shared string

Might in fact better be called *quantum eavesdropper detection*

- Assume that the classical channel used in steps 3–5 is “authenticated”
 - Alice and Bob know they are talking to each other, and
 - Eve can listen but not change the bits sent over the classical channel
- In contrast to the qubits sent during step 1 of the protocol, which Eve is allowed to manipulate in any way she wants

BB84 - Example

QUANTUM TRANSMISSION															
Alice's random bits.....	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases.....	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends.....	↗	↑	↘	↔	↑	↑	↔	↔	↘	↗	↑	↘	↗	↗	↑
Random receiving bases.....	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob.....	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits.....	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct.....		OK			OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)...		1			1			0				1		0	1
Bob reveals some key bits at random.....					1									0	
Alice confirms them.....					OK									OK	
OUTCOME															
Remaining shared secret bits.....		1						0				1			1

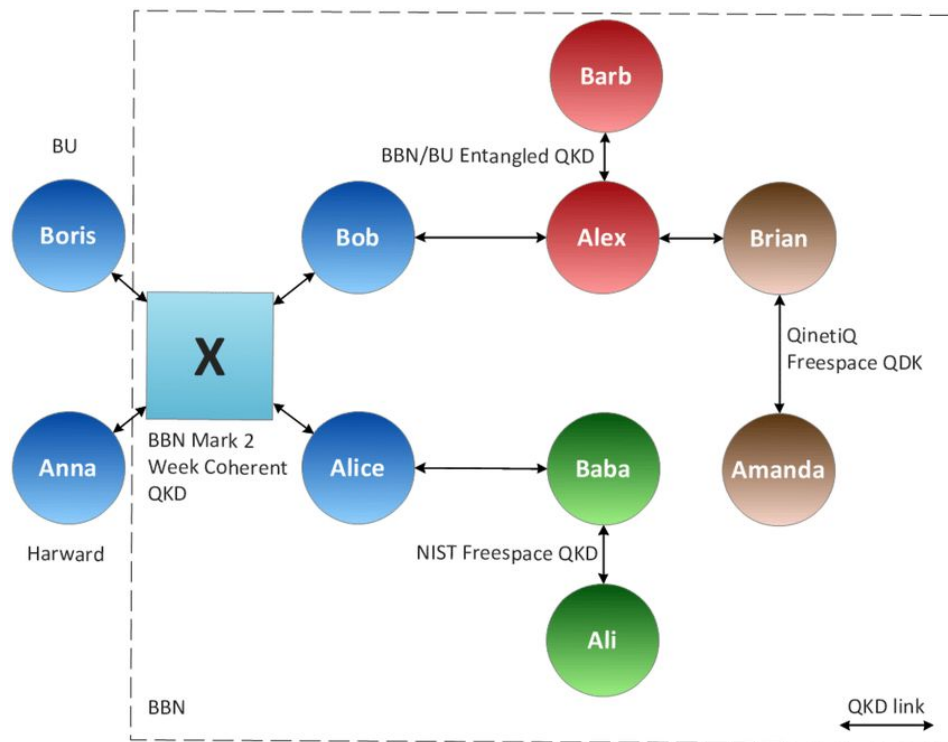
QKD Networks

DARPA QKD Network

- The world's first QKD network
- presented in December 2002 by BBN Technologies and Harvard and Boston Universities
- laid the foundation for the further development of trusted repeater QKD networks
- demonstrated practically the disadvantages of a *switched* QKD network type

The network consisted of:

- a weak-coherent BB84 transmitter pair (Anna and Alice)
- a pair of compatible receivers (Boris and Bob)
- one 2×2 optical switch to connect any sender to any receiver



Entanglement Swapping

A ---- B C ---- D

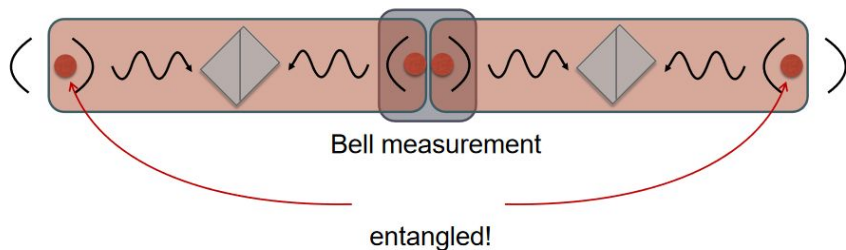
A and D can be arbitrarily distant, B and C next to each other

A -----D
entangled

After performing an operation on B and C -> A and D are entangled

Quantum repeater networks

- make end-to-end entanglement
- entanglement is a consumable resource



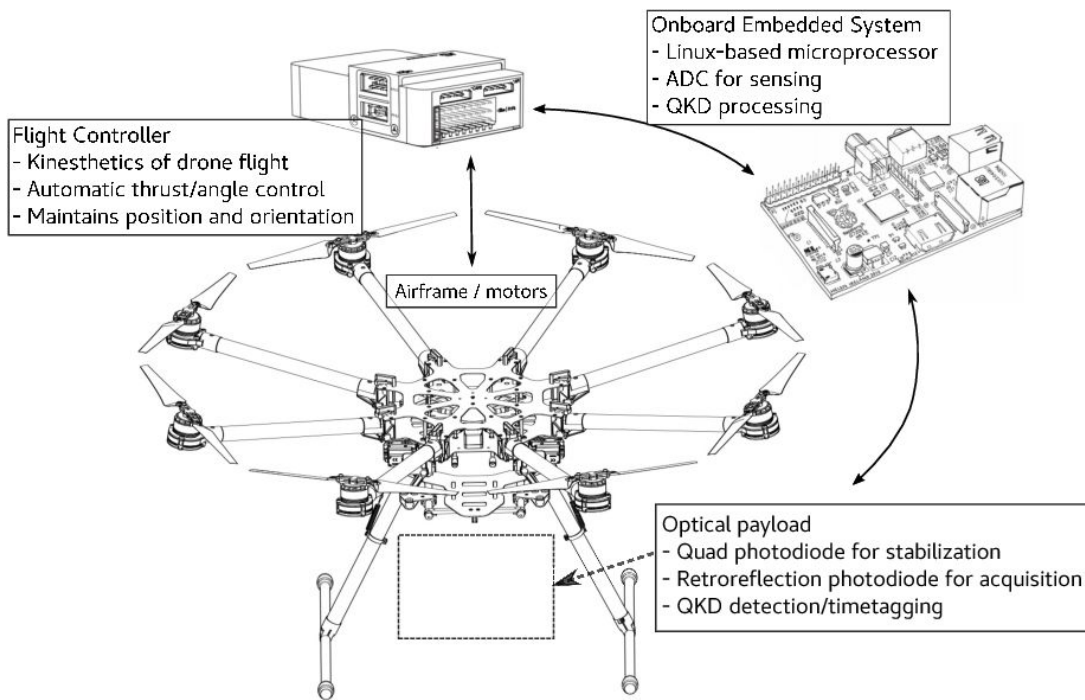
$$\begin{array}{c} |0\rangle \text{ --- } [H] \text{ --- } \bullet \\ |0\rangle \text{ --- } \oplus \end{array} \left. \vphantom{\begin{array}{c} |0\rangle \\ |0\rangle \end{array}} \right\} \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Create Bell pair state

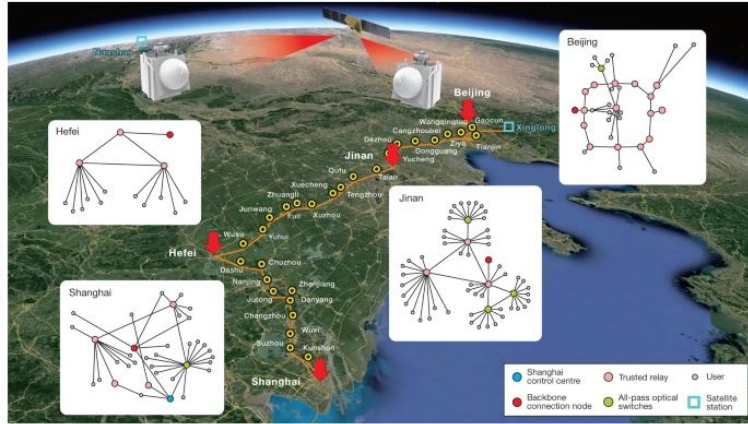
$$\frac{\langle 11 | + \langle 00 |}{\sqrt{2}} \left\{ \begin{array}{c} \bullet \text{ --- } [H] \text{ --- } \langle 0 | \\ \oplus \text{ --- } \langle 0 | \end{array} \right.$$

Inverse operation: Bell measurement

Drone-to-Drone QKD

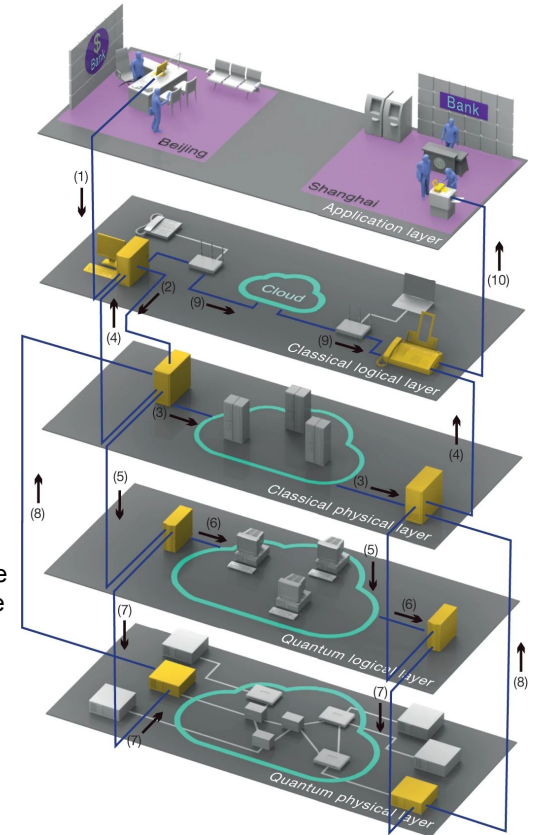


An integrated space-to-ground quantum communication network over 4,600 kilometres



The network consists of four QMANs (in Beijing, Jinan, Shanghai and Hefei; red arrows), a backbone fibre link over 2,000 km (orange line) and two ground-satellite links that connect Xinglong and Nanshan (blue squares), separated by 2,600 km. There are three types of node in the network: user nodes (purple circles), all-pass optical switches (green circles) and trusted relays (pink circles). Each QMAN consists of all three node types (see insets). The backbone is connected by trusted relays (shown as yellow and black circles in the main image and red circles in the insets). A quantum satellite is connected to the Xinglong and Nanshan ground stations; Xinglong is also connected to the Beijing QMAN via fibre. In Beijing, the Beijing control-centre node is located at the same location as the backbone connection node (indicated by the red circle). Map data: Google, Data SIO, NOAA, US Navy, NGA, GEBCO, Landsat/Copernicus; copyright ZENRIN.

The network consists of five layers: the application layer, the classical logical layer, the classical physical layer, the quantum logical layer and the quantum physical layer. As an example, we consider how a secure transmission from Beijing to Shanghai works. The message transmission order is sent from the user in Beijing to the computer (1). The computer sends an order to the key management system to ask for the key (2) and to the router to find the classical route for classical information transfer (3). The key management system checks whether the key is sufficient. If it is, it sends the key to the computer (4); otherwise, it sends an order to the quantum system server to generate more keys (5). The quantum system server sends the order to the quantum control system (6), which finds the optimal key generation route and sends the order to generate keys (7). The keys are generated in the quantum physical layer and stored in the key management system (8). After encoding or decoding the message with the key (9), the information can be transferred securely to the user in Shanghai (10).



Entangled State

$$1/\sqrt{2} * (|01\rangle - |10\rangle) \quad \text{often called the } \textit{spin singlet state}$$

whenever the measurement is performed along the Z axis

It is always possible for Alice to predict what Bob's result was

Alice measures $|0\rangle$, Bob measures $|1\rangle$

Alice measures $|1\rangle$, Bob measures $|0\rangle$

They share a state that **remains invariant if each apply the same unitary transformation**

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad |0\rangle = a|a\rangle + b|b\rangle \quad \text{and} \quad |1\rangle = c|a\rangle + d|b\rangle$$

$$\text{Replace } |0\rangle \text{ and } |1\rangle: 1/\sqrt{2} (|\underline{01}\rangle - |\underline{10}\rangle) = (ad - bc)/\sqrt{2} (|\underline{ab}\rangle - |\underline{ba}\rangle)$$

U is unitary, $(ad-bc)$ is a global phase factor of the form $e^{i(\theta)}$

Measurement results in a rotated basis on both qubits will be correlated too

Entanglement and Games

Entangled states

- cannot be written as a tensor product of separate states
- the most famous one is the Bell pair

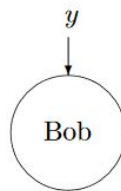
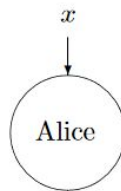
Non-local games (remember teleportation)

- explore some of the consequences of entanglement
- involves a referee and two *non-communicating* parties
- Alice and Bob are *cooperatively* trying to win the game

The game

- one round of interaction between referee and Alice and Bob:
- the referee sends
 - a (classical) question x to Alice
 - a (classical) question y to Bob
 - questions are sampled from some known probability distribution
- Alice and Bob respectively respond with a (classical) answer

Inputs:



Outputs:

CHSH Game

CHSH game where two players Alice and Bob

- receive an input bit x and y respectively
- produce an output a and b based on the input bit
- Alice's output bit depends solely on her input bit x , and similarly for Bob

The goal is to maximize the probability to satisfy the condition:

$$a \text{ XOR } b = x \text{ AND } y$$

Consider the case of classical deterministic strategies

- without any randomness
- *the highest probability achievable is 75%*
- four bits completely characterize any deterministic strategy
 - Let a_0, a_1 be the outputs that Alice outputs if $x=0$ and $x=1$
 - Let b_0, b_1 be the outputs Bob gives on inputs $y=0$ and $y=1$

Not possible to satisfy all four equations simultaneously, since summing them modulo 2 yields $0 = 1$

$$a_0 \oplus b_0 = 0,$$

$$a_0 \oplus b_1 = 0,$$

$$a_1 \oplus b_0 = 0,$$

$$a_1 \oplus b_1 = 1.$$

CHSH Game

With quantum correlations

- it can achieve higher success probability
- two players start with a shared Bell-pair entangled state
- the **random input x and y** is provided by referee for Alice and Bob

The success probability of satisfying the above condition will be **$\cos(\theta/2)^2$** if Alice and Bob measure their entangled qubit in measurement basis V and W where angle between V and W is θ .

Maximum success probability is

- **$\cos(\pi/8)^2 \sim 85.3\%$** when $\theta = \pi/4$.
- In the usual implementation, Alice and Bob share the Bell state with the same value and opposite phase. If the input x (y) is 0, Alice (Bob) rotates in Y -basis by angle $-\pi/16$ and if the input is 1, Alice (Bob) rotates by angle $3\pi/16$

CHSH Game

What Alice does:

- if $x=0$ then Alice applies $R(-\pi/16)$ to her qubit
- if $x=1$ she applies $R(3\pi/16)$
- then Alice measures her qubit in the computational basis
- outputs the resulting bit a

Bob's procedure is the same, depending on his input bit y

After the measurements

- the probability that $a \oplus b = 0$ is $\cos(\theta_1 + \theta_2)^2$
- the first condition is satisfied with probability $\cos(\pi/8)^2$ for all four input possibilities

CHSH Game

Start with

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$


Consider the rotation matrix

$$R(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

After Alice uses θ_1 and Bob uses θ_2

$$\frac{1}{\sqrt{2}} (\cos(\theta_1 + \theta_2)(|00\rangle - |11\rangle) + \sin(\theta_1 + \theta_2)(|01\rangle + |10\rangle)).$$

Product-to-sum ^[32]
$2 \cos \theta \cos \varphi = \cos(\theta - \varphi) + \cos(\theta + \varphi)$
$2 \sin \theta \sin \varphi = \cos(\theta - \varphi) - \cos(\theta + \varphi)$
$2 \sin \theta \cos \varphi = \sin(\theta + \varphi) + \sin(\theta - \varphi)$
$2 \cos \theta \sin \varphi = \sin(\theta + \varphi) - \sin(\theta - \varphi)$
$\tan \theta \tan \varphi = \frac{\cos(\theta - \varphi) - \cos(\theta + \varphi)}{\cos(\theta - \varphi) + \cos(\theta + \varphi)}$
$\prod_{k=1}^n \cos \theta_k = \frac{1}{2^n} \sum_{e \in S} \cos(e_1 \theta_1 + \dots + e_n \theta_n)$ where $S = \{1, -1\}^n$


PHASECRAFT

$|00\rangle \rightarrow \cos a |00\rangle + \sin a |10\rangle$
 $\rightarrow \cos a \cdot \cos b |00\rangle + \cos a \sin b |10\rangle$
 $+ \sin a \cos b |01\rangle + \sin a \sin b |11\rangle$

$|11\rangle \rightarrow -\sin a |01\rangle + \cos a |11\rangle$
 $\rightarrow -\sin a \cos b |01\rangle + \sin a \sin b |11\rangle$
 $+ \cos a \sin b |01\rangle + \cos a \cos b |11\rangle$

$(\cos a \cos b - \sin a \sin b) |00\rangle + (\cos a \cos b - \sin a \sin b) |11\rangle$
 $= (\cos a \cos b - \sin a \sin b) (|00\rangle + |11\rangle)$
 $= \frac{1}{2} (\cos(a+b) + \cos(a-b) - \cos(a-b) + \cos(a+b)) (|00\rangle + |11\rangle)$
 $= \cos(a+b) (|00\rangle + |11\rangle)$

\Rightarrow That is the prob of $ab=0$?

$P(00) + P(11) = \frac{\cos^2(a+b)}{2} + \frac{\cos^2(a+b)}{2}$
 $= \cos^2(a+b)$

\Rightarrow Find angles a, b such that for x, y the value of $\cos^2(a+b)$ is maximized

INSPIRATION ISN'T CLASSICAL

Bell States

$B_0 = 1/\sqrt{2}(|00\rangle + |11\rangle)$ very often called a Bell pair state

$B_1 = 1/\sqrt{2}(|01\rangle + |10\rangle)$ flip the second state $|0\rangle$ to $|1\rangle$

$B_2 = 1/\sqrt{2}(|00\rangle - |11\rangle)$ flip the phase from $+$ to $-$

$B_3 = 1/\sqrt{2}(|01\rangle - |10\rangle)$ the spin singlet state from the previous slide

B_0, B_1, B_2 are also invariant if transformed according to their relation to B_3

For example, for B_0 considering the observables Z and X :

- Alice measures in Z and sees $|0\rangle$
- the state on Bob's side is $|0\rangle$: measures X (rotated basis) and sees with equal probability $|+\rangle$ or $|-\rangle$

Bell's Inequalities

Is there a set of instructions that tells the particles how to react when they are measured?

Bell Inequalities are a test for *locality* by considering the correlations between measurement outcomes obtained by two parties who share an entangled state

- classical correlations
 - encoded in a set of instructions using hidden variables with known values
 - there is a joint probability distribution that governs the possible outcomes of all measurements
 - then the outcome of any measurement can be predicted with certainty
- quantum correlations

One possible approach:

- take three binary properties A, B and C
- model classic probabilistic behaviour by an inequality
- test on multiple quantum states by collecting statistics

Classical: Count the number of events satisfying a condition

- Assume that the binary properties are randomly measured
- $A = \{+1, -1\}$, $B = \{+1, -1\}$, $C = \{+1, -1\}$
- Formulate an inequality that is classically correct (see below)
 - $N(AB') =$ number of times A is +1 and B is -1
 - $N(BC') =$ number of times B is +1 and C is -1
 - $N(AC') =$ number of times A is +1 and C is -1

$$N(AB') + N(BC') \geq N(AC')$$

$$N(AB') = N(AB'C) + N(AB'C'), \text{ because } C \text{ can be either } +1 \text{ or } -1$$

$$N(BC') = N(ABC') + N(A'BC'), \text{ because } A \text{ can be either } +1 \text{ or } -1$$

$$N(AC') = N(ABC') + N(AB'C'), \text{ because } B \text{ can be either } +1 \text{ or } -1$$

$$N(AB'C) + \underline{N(AB'C')} + \underline{N(ABC')} + N(A'BC') \geq \underline{N(ABC')} + \underline{N(AB'C')}$$

$$N(AB'C) + N(A'BC') \geq 0 \rightarrow \text{it is correct, sum of two positive values} > 0$$

Quantum: Validate experimentally by measuring repeatedly

Given an ensemble of entangled states, for example, B_0

- Three axis: Z and two others rotated by angle θ and 2θ
- Alice and Bob **randomly choose along which axis A, B, or C to measure**

$$\cos(\text{angle}/2)|A+\rangle ; \sin(\text{angle}/2)|A-\rangle > \begin{pmatrix} \cos(\text{angle}/2) \\ \sin(\text{angle}/2) \end{pmatrix}$$

$$N(AB') + N(BC') \geq N(AC')$$

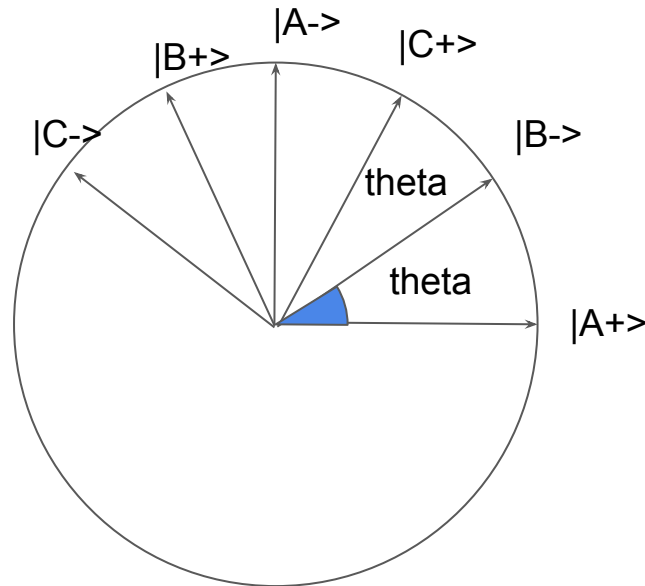
$$P(A+, B-) + P(B+, C-) \geq P(A+, C-)$$

$$\sin^2(\theta/2) + \sin^2(\theta/2) \geq \sin^2(\theta)$$

For small angles $\sin(x) = x$

$$2 * (\theta^2/4) \geq \theta^2$$

Violates Inequality



Instructions: Hidden Variables -> Counting is the value of N

- Before:
1. each experiment
 2. the Bell pair is constructed
 3. sent to Alice and Bob

The particles decide how to react *locally* to the measurements

→ **instructions**

A	B	C
+	+	+
+	+	-
+	-	+
+	-	-
-	+	+
-	+	-
-	-	+
-	-	-

On next slide: Instead of three properties(e.g. A,B,C) use three devices and a single property