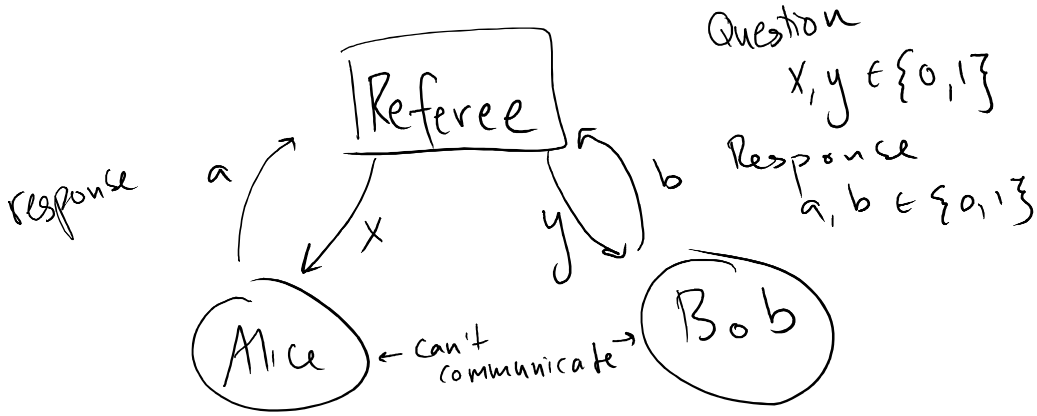
S. KIMMEL

More Qubits!

One qubit at a time → better crypto

Two " " → better game playing



Alice & Bob win if $x \wedge y = a \oplus b$

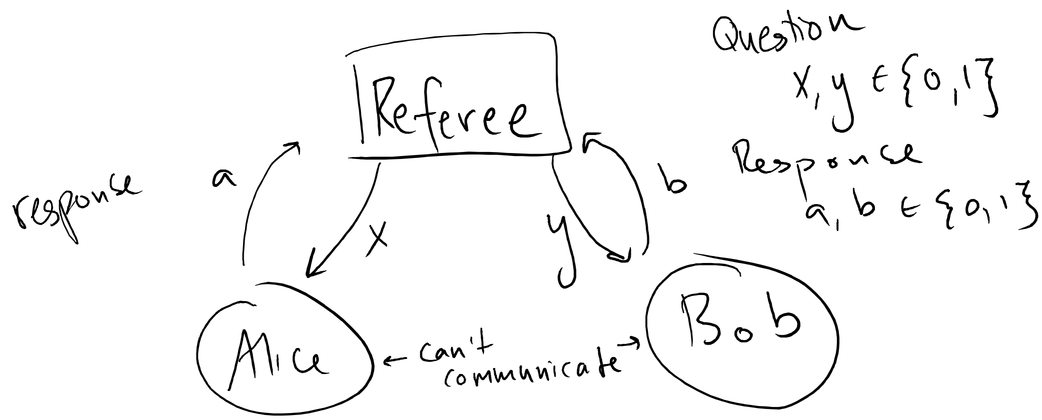
x	y	$x \wedge y$	$a \oplus b$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

Q: Figure out the best strategy for Alice and Bob, averaged over choice of x, y, chosen uniformly at random

S.KIMMEL

More Qubits!

One qubit at a time → better crypto
Two " " → better game playing



Alice & Bob win if $x \wedge y = a \oplus b$

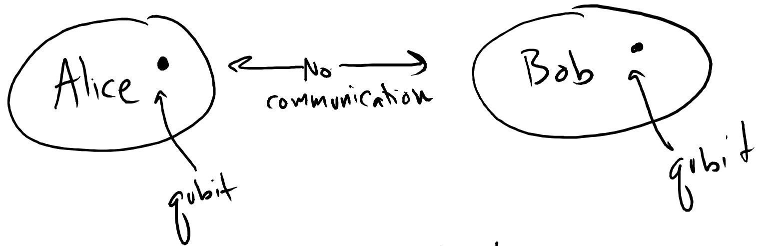
x	y	$x \wedge y$	$a \oplus b$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

Q: Figure out the best strategy for Alice and Bob, averaged over choice of x, y, chosen uniformly at random

A: Best strategy, always choose $a=0$ $b=0$. Will win 75% of time

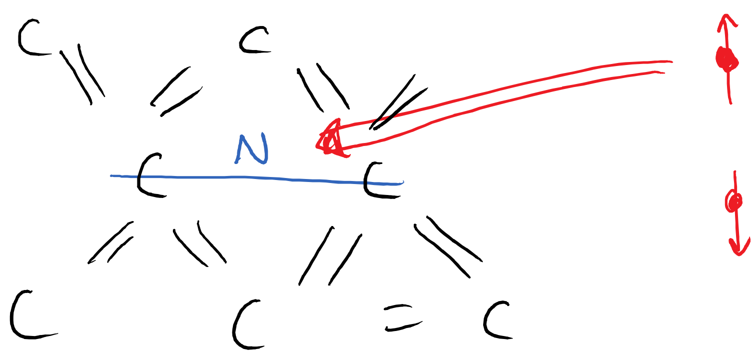
S. KIMMEL

Now:



Can they do better? ... Yes!

Imagine qubit not as photon, but as a piece of diamond



one extra electron.

Qubit stored in spin.

Very stable (1 second)

S.KIMMEL

Need math to describe $\boxed{2 \text{ qubits}}$:

Qubit A $\qquad$ Qubit B

$$|\psi_1\rangle_A = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \qquad |\psi_2\rangle_B = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}$$

state of 2 qubits

"Kronecker product"
Tensor product

$$|\psi\rangle_{AB} = |\psi_1\rangle_A \otimes |\psi_2\rangle_B = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \otimes \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{pmatrix}$$

Means "A" qubit is first in tensor product. "B" qubit is second term.

Using standard basis kets:

$\otimes$ distributes like regular multiplication

$$|\psi\rangle_{AB} = \left(a_0|0\rangle + a_1|1\rangle\right) \otimes \left(b_0|0\rangle + b_1|1\rangle\right)$$
$$= a_0 b_0 |0\rangle_A|0\rangle_B + a_0 b_1 |0\rangle_A|1\rangle_B + a_1 b_0 |1\rangle_A|0\rangle_B + a_1 b_1 |1\rangle_A|1\rangle_B$$
$$= a_0 b_0 |00\rangle_{AB} + a_0 b_1 |01\rangle_{AB} + a_1 b_0 |10\rangle_{AB} + a_1 b_1 |11\rangle_{AB}$$

Notation: $|x\rangle \otimes |y\rangle = |x\rangle_A |y\rangle_B = |x\,y\rangle_{AB}$

Count elements of vector in binary:
(2 qubits, 2 bits to label)

$$\begin{pmatrix} \square \\ \square \\ \square \\ \square \end{pmatrix} \begin{matrix} \leftarrow 00 \\ \leftarrow 01 \\ \leftarrow 10 \\ \leftarrow 11 \end{matrix} \qquad \text{so } |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

S. KIMMEL

Entanglement: can have 2-qubit states that are not tensor product

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

is quantum state iff $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = \langle\psi|\psi\rangle = \underline{1}$

(amplitudes square to 1)

<u>def</u>: A state $|\psi\rangle$ is <u>product</u> if $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

<u>def</u>: A state $|\psi\rangle$ is <u>entangled</u> if $\nexists$ $|\psi_1\rangle, |\psi_2\rangle$ such that $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

Q: • Let $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$

Is $|\beta_{00}\rangle$ entangled?

S.KIMMEL

Q: • Let $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ Entangled?

Assume for contradiction not entangled:

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \Rightarrow \begin{array}{l} a \text{ or } d = 0 \\ b \text{ or } c = 0 \end{array}$$

$\Downarrow$

$ac = 0$ or $bd = 0$

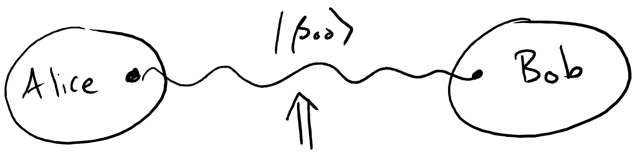
$\Downarrow$

But $ac = bd = 1/\sqrt{2}$, a contradiction

$\Downarrow$

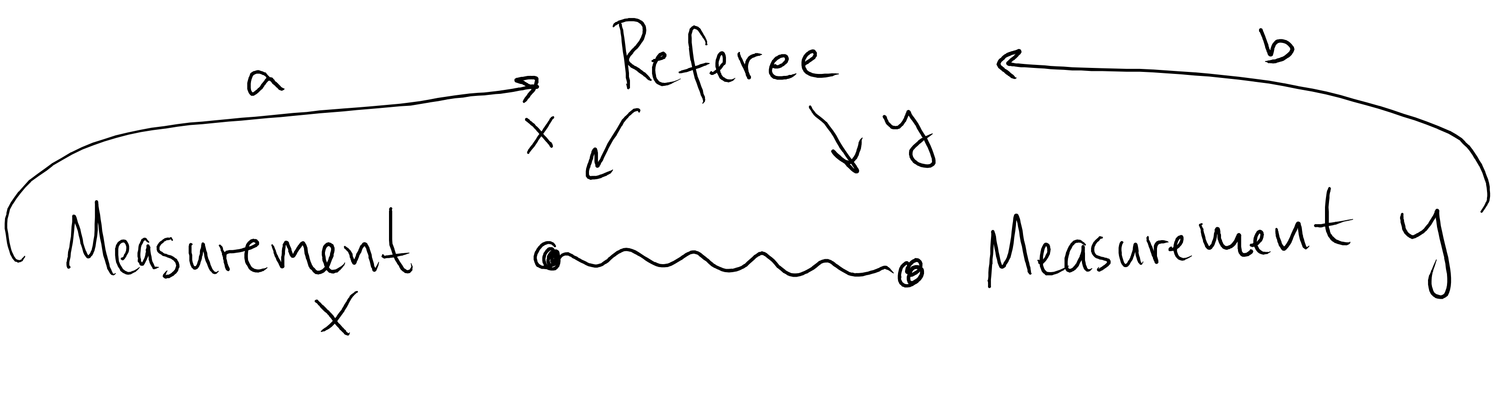
entangled

Idea



Entangled State of 2 qubits.

Each has a diamond qubit, but can't describe each qubit's state individually, only globally



S. KIMMEL

Alice and Bob can't communicate, but they can make a quantum measurement on their subsystem.

$$\underbrace{\begin{array}{ll} \text{Alice Measures} & M_A = \{|\phi_0\rangle, |\phi_1\rangle\} \\ \text{Bob Measures} & M_B = \{|\chi_0\rangle, |\chi_1\rangle\} \end{array}}$$

Effective measurement on $|\psi\rangle_{AB}$ (their combined state):

$$M_{AB} = M_A \otimes M_B = \{|\phi_0\rangle|\chi_0\rangle, |\phi_1\rangle|\chi_0\rangle, |\phi_0\rangle|\chi_1\rangle, |\phi_1\rangle|\chi_1\rangle\}$$

- Get outcome $\underset{\text{Alice's outcome}}{|\phi_i\rangle_A}\underset{\text{Bob's outcome}}{|\chi_j\rangle_B}$ with probability $|\langle\phi_i|_A\langle\chi_j|_B|\psi\rangle_{AB}|^2$
- State $|\psi\rangle_{AB} \rightarrow |\phi_i\rangle_A|\chi_j\rangle_B$ (collapse)

$$\boxed{\text{If } |\psi\rangle_{AB} \text{ was entangled} \rightarrow \text{collapses to unentangled}}$$

Measurement destroys/uses up entanglement

S.KIMMEL

Let

"phi" "theta"

$$M(\theta) = \{|\phi_0(\theta)\rangle, |\phi_1(\theta)\rangle\}$$

$$|\phi_0(\theta)\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

$$|\phi_1(\theta)\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$$

If $x=0$, Alice measures $M(0)$

If $x=1$, Alice measures $M(\pi/4)$

If $y=0$, Bob measures $M(\pi/8)$

If $y=1$, Bob measures $M(-\pi/8)$

Outcome	Answer To Referee
$\lvert\phi_0\rangle$	0
$\lvert\phi_1\rangle$	1

S.KIMMEL

Tensor Product Questions

(See slides for multiple choice)

- $|1\rangle \otimes \left(\sqrt{\tfrac{1}{3}}|0\rangle + \sqrt{\tfrac{2}{3}}|1\rangle\right) = \sqrt{\tfrac{1}{3}}|10\rangle + \sqrt{\tfrac{2}{3}}|11\rangle$
  - Distribute
  - $|1\rangle \otimes |0\rangle$ write as $|10\rangle$

- $|\psi\rangle_{AB} = \sqrt{\tfrac{1}{2}}|01\rangle_{AB} + i\sqrt{\tfrac{1}{2}}|10\rangle_{AB}$

  $\langle\psi|_{AB} = \frac{1}{\sqrt{2}}\langle 01|_{AB} \underbrace{-i}_{\text{complex conjugate}}\sqrt{\tfrac{1}{2}}\langle 10|_{AB}$

  Keep order of AB the same!

- $|\psi\rangle = |01\rangle_{AB}$ $\quad |\phi\rangle = |10\rangle_{AB}$ $\quad \langle\phi| = \langle 10|_{AB}$

  $|\psi\rangle = |0\rangle_A|1\rangle_B$ $\quad \langle\phi| = \langle 1|_A\langle 0|_B$

  $\langle\phi|\psi\rangle = \langle 1|_A\underbrace{\langle 0|_B|0\rangle_A}_{\text{switch order}}|1\rangle_B = \underbrace{\langle 1|0\rangle_A}_{0}\underbrace{\langle 0|1\rangle_B}_{0} = 0$

  multiply

  * Always match A to A, B to B.

  ☆ Can switch order of adjacent A, B terms

- $\langle\psi|\psi\rangle = \langle\psi_1|_A\langle\psi_2|_B|\psi_1\rangle_A|\psi_2\rangle_B = \overbrace{\langle\psi_1|\psi_1\rangle_A}^{1}\overbrace{\langle\psi_2|\psi_2\rangle_B}^{1} = 1$

  multiply

S.KIMMEL

Why care?

CHSH game can be used to

- prove a system is quantum
- create verifiably random bits
- do delegated quantum computation

(You want a quantum computer to do a calculation for you but you don't trust whether it will follow your instructions. By asking it to play game in the middle of computation, can verify it is doing the correct thing)