Quantum Nonlocality and

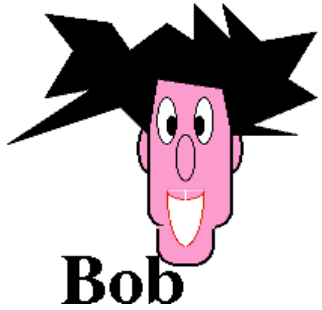
Pseudo Telepathy

Gilles Brassard
Université de Montréal

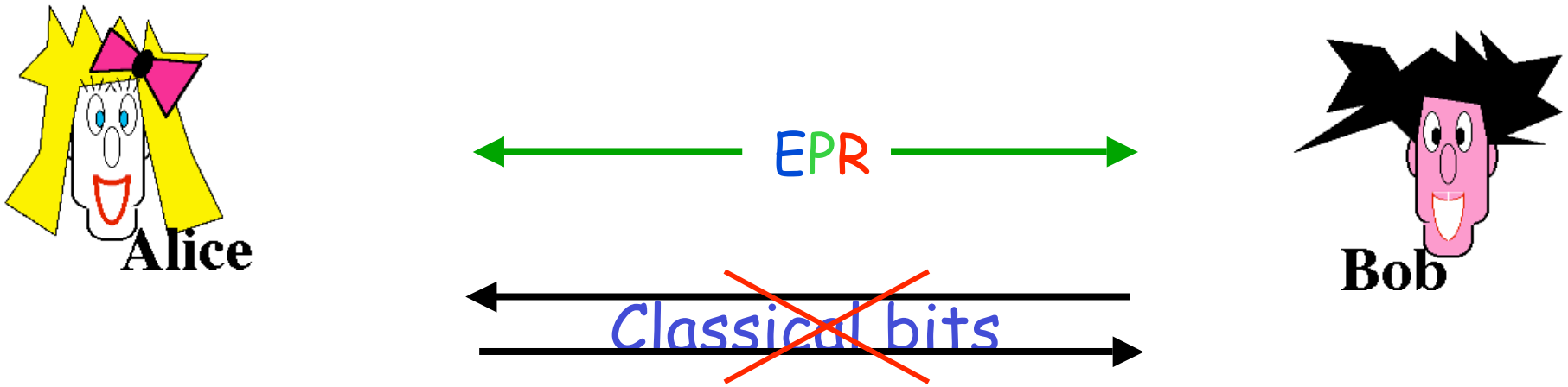
QIP Summer School, 2 August 2005

Pseudo Telepathy

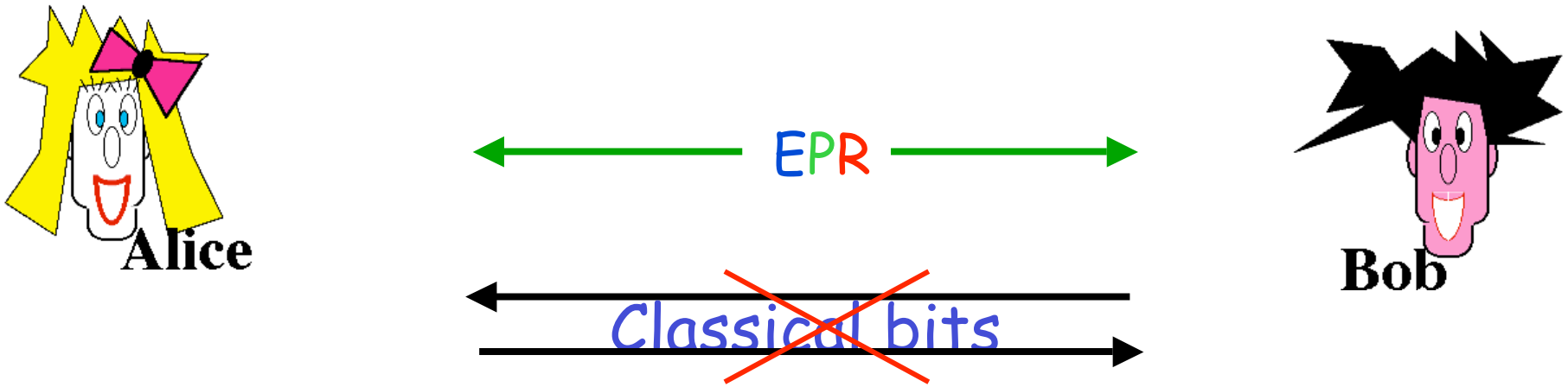
EPR



Pseudo Telepathy

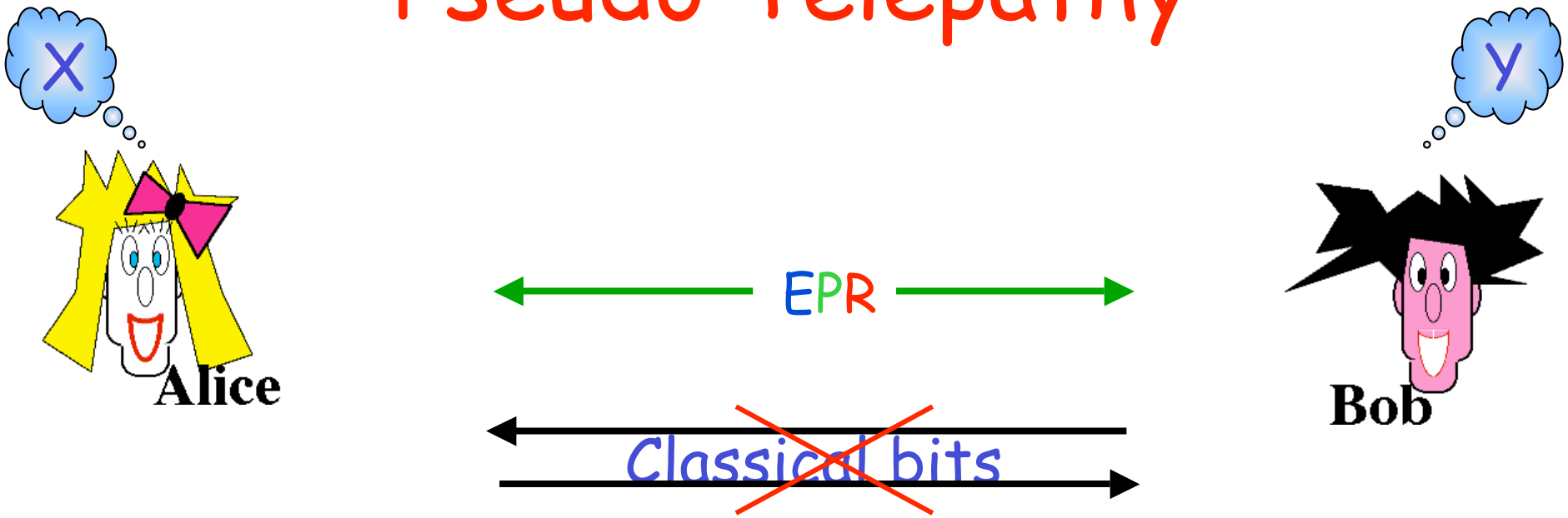


Pseudo Telepathy

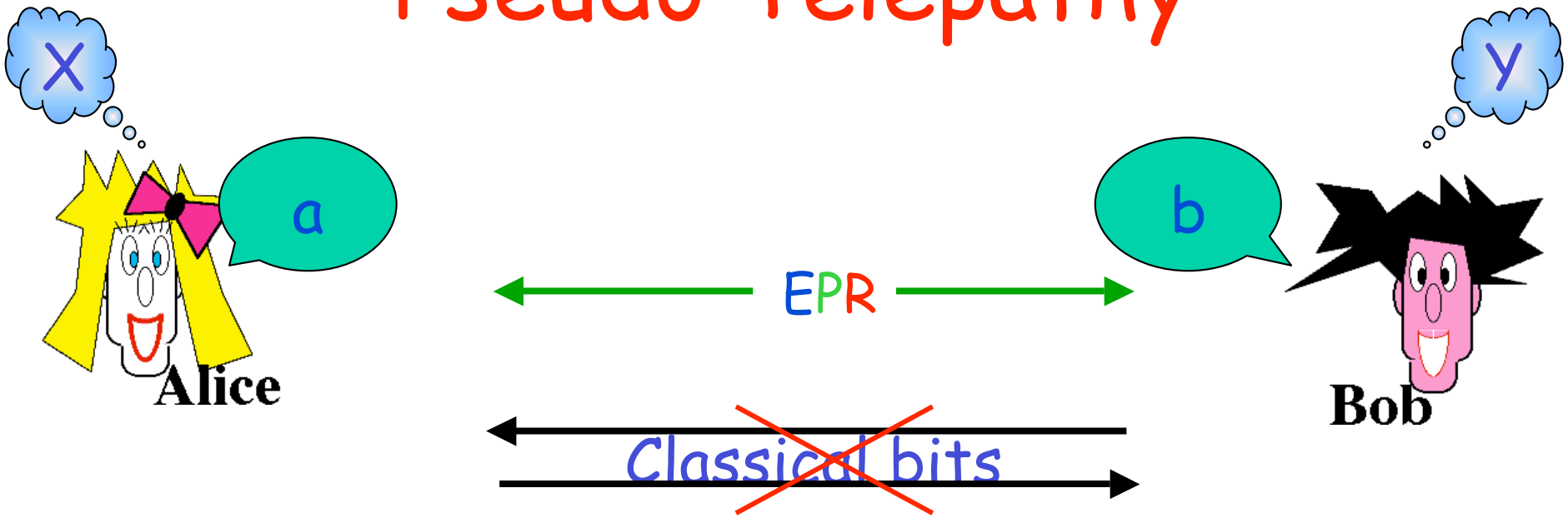


Can entanglement *eliminate*
the need for communication?

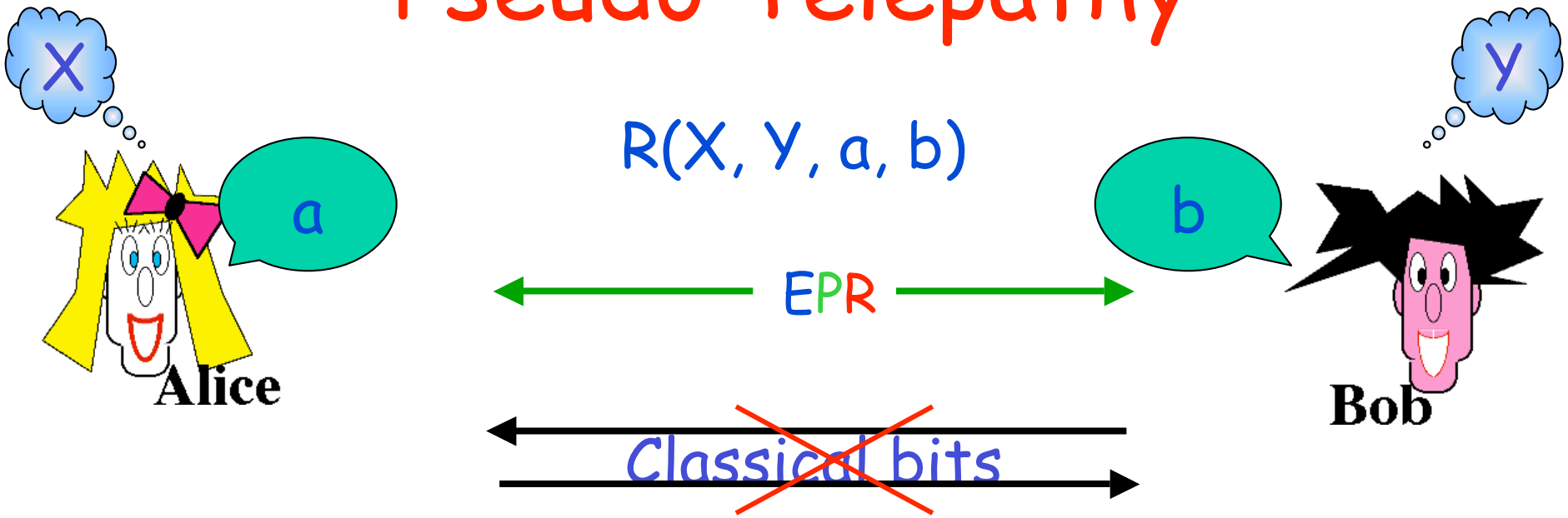
Pseudo Telepathy



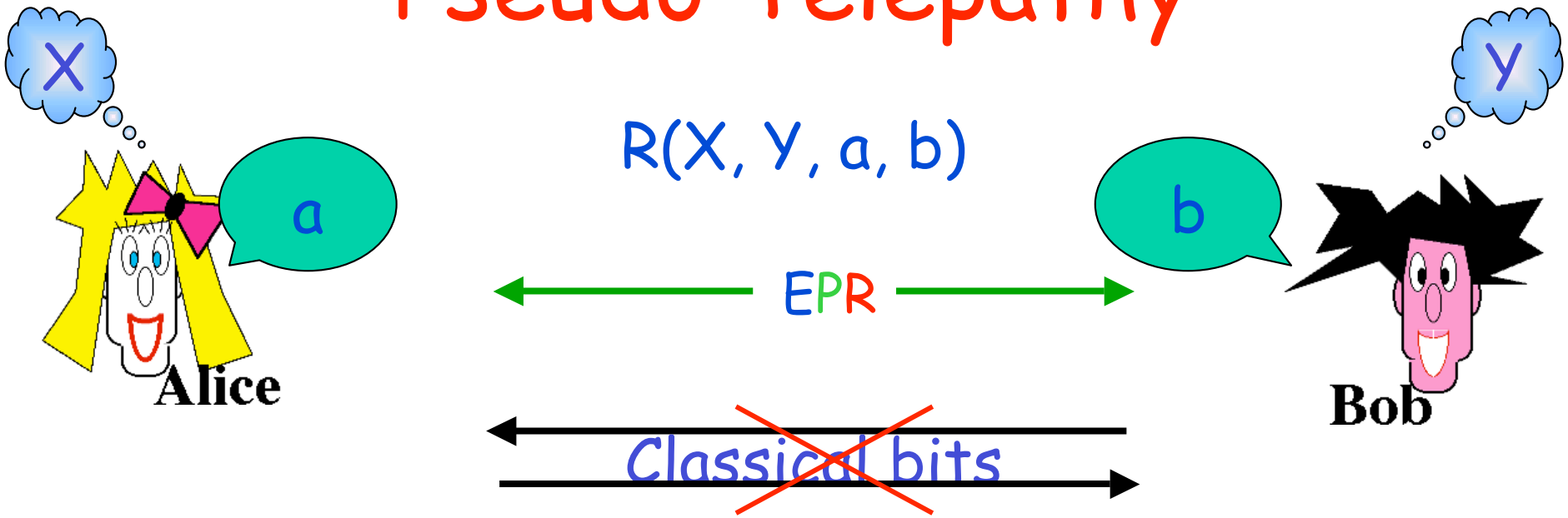
Pseudo Telepathy



Pseudo Telepathy

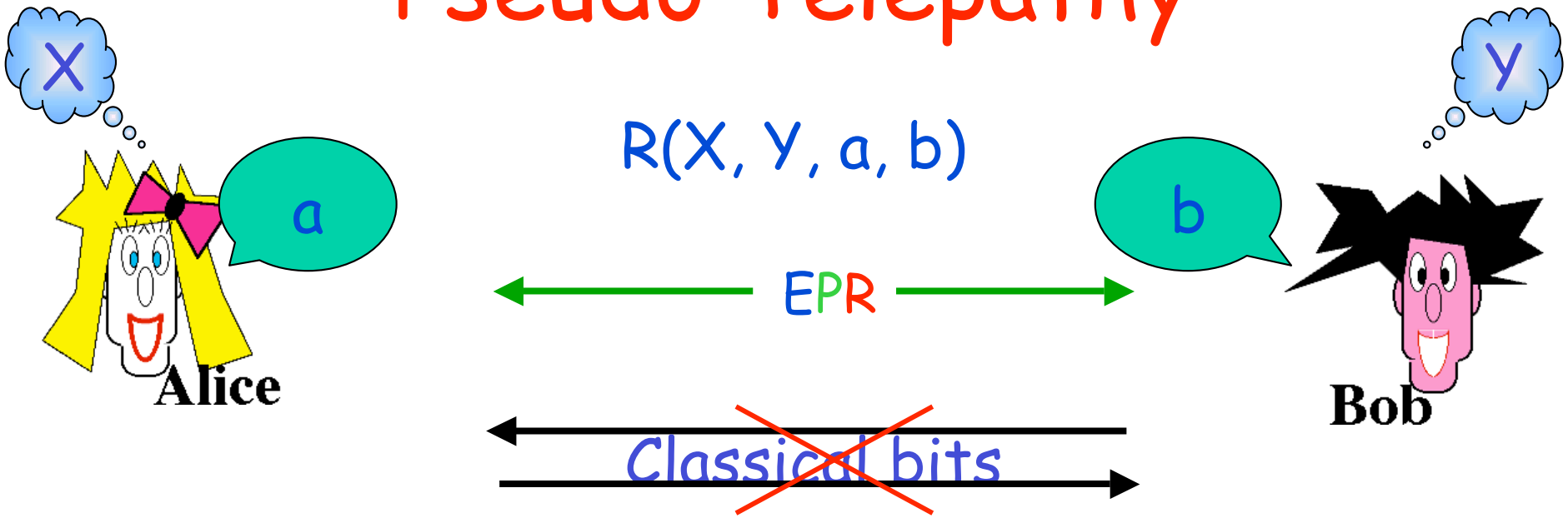


Pseudo Telepathy



This is interesting when
(a,b) depends on (X,Y)

Pseudo Telepathy



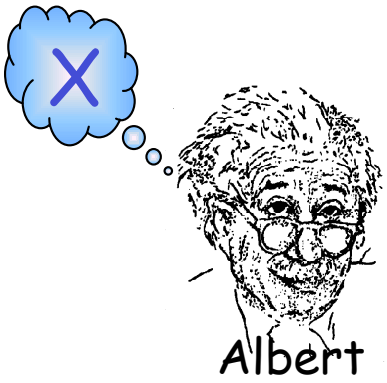
In other words, when

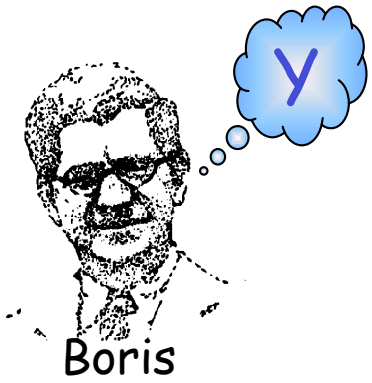
$X \rightarrow a \qquad Y \rightarrow b$

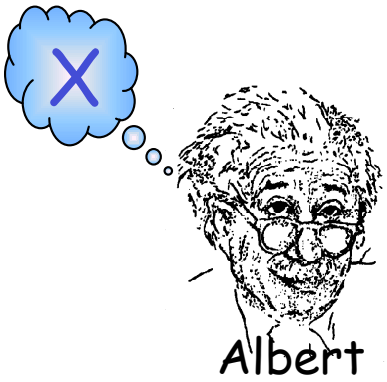
is classically impossible without communication

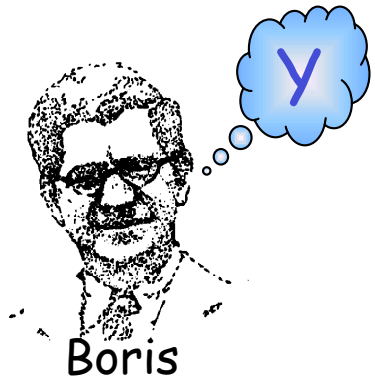
Albert

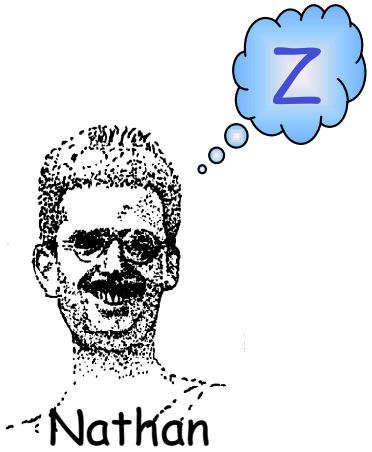
Boris

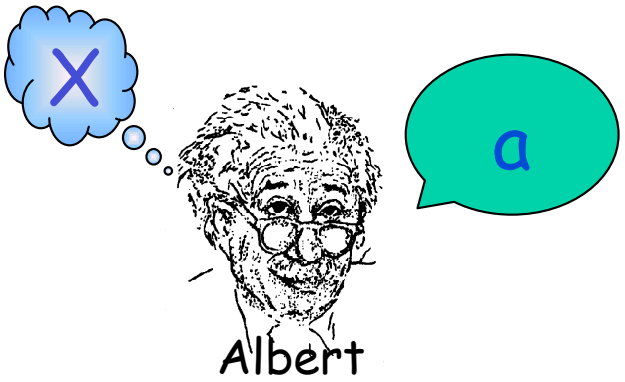

X
Albert

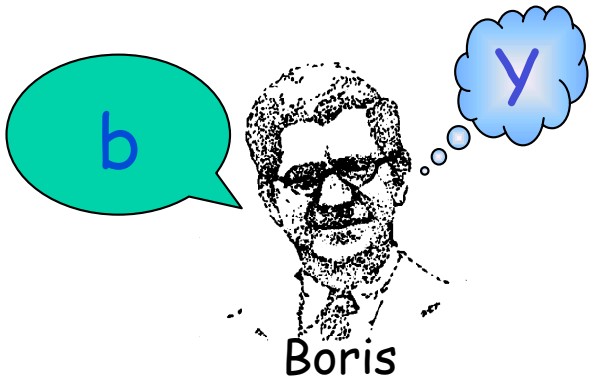

Y
Boris

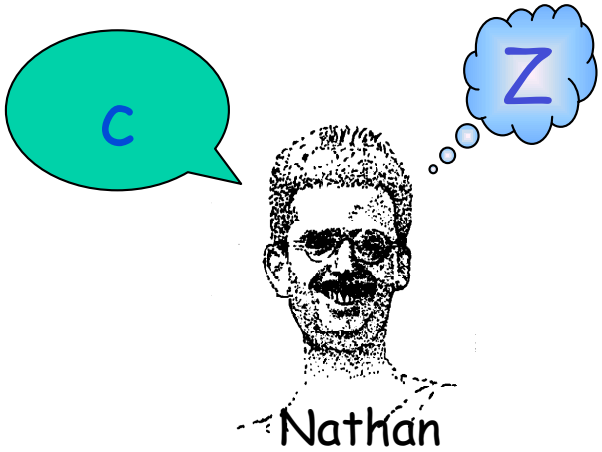

X
Albert

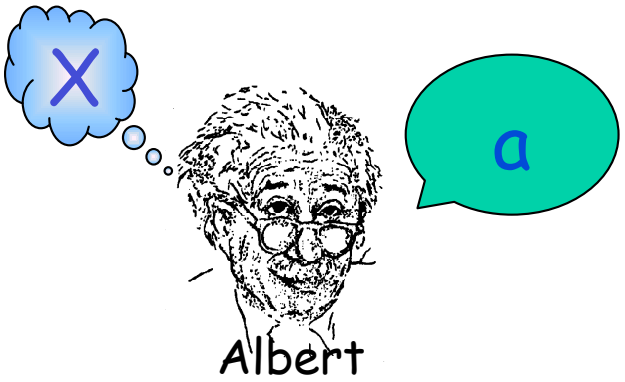

Y
Boris

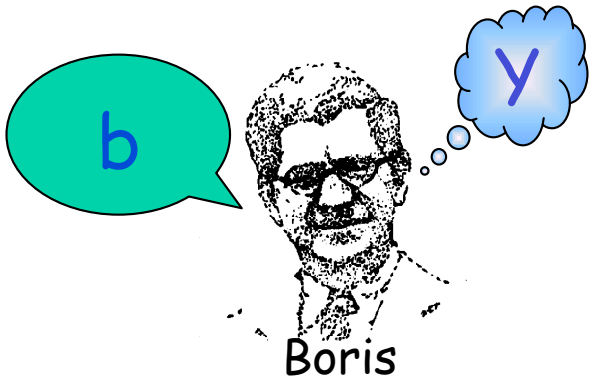

Z
Nathan


X
a
Albert

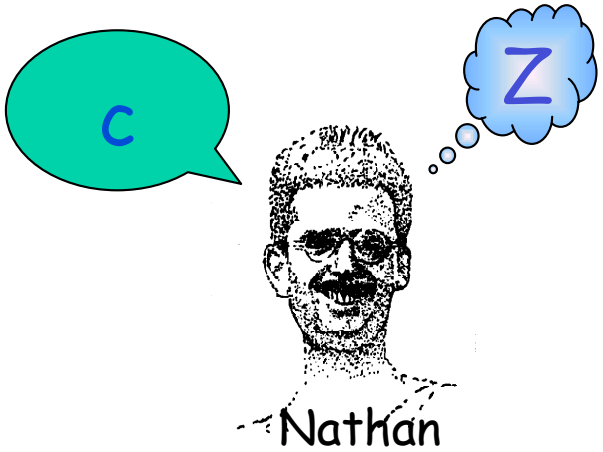

b
y
Boris

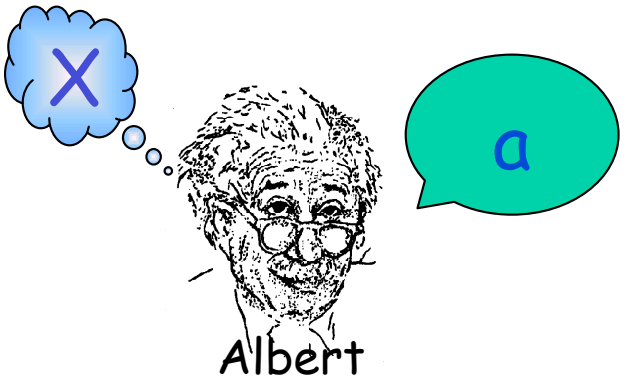

c
Z
Nathan

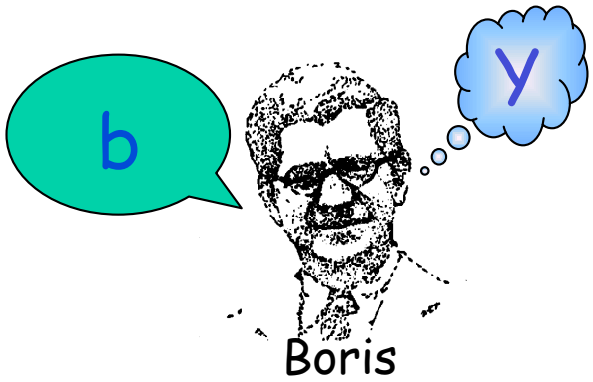




Goal: $a \oplus b \oplus c = XYZ$

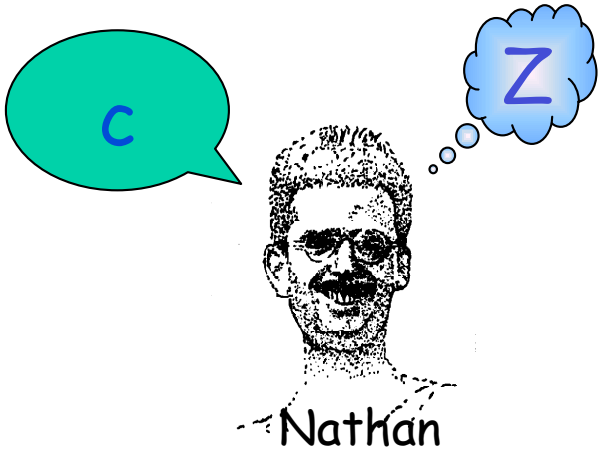






Goal: $a \oplus b \oplus c = XYZ$

Promise: $X \oplus Y \oplus Z = 1$



Quantum Versus Classical

Best classical protocol:

Correct with probability 75%

Quantum Versus Classical

Best classical protocol:

Correct with probability 75%

Best quantum protocol:

Always correct!

Quantum Protocol

Consider three-party entangled state $|\Psi\rangle$

$$|000\rangle + |001\rangle + |010\rangle + |100\rangle - |011\rangle - |101\rangle - |110\rangle - |111\rangle$$

Quantum Protocol

Consider three-party entangled state $|\Psi\rangle$

$$|000\rangle + |001\rangle + |010\rangle + |100\rangle - |011\rangle - |101\rangle - |110\rangle - |111\rangle$$

The qubits are sent to Albert, Boris & Nathan

Quantum Protocol

Consider three-party entangled state $|\Psi\rangle$

$$|000\rangle + |001\rangle + |010\rangle + |100\rangle - |011\rangle - |101\rangle - |110\rangle - |111\rangle$$

The qubits are sent to Albert, Boris & Nathan

Each party applies a Walsh-Hadamard Transform H to his qubit if and only if his input is 1

Quantum Protocol

Goal: $a \oplus b \oplus c = XYZ$

Promise: $X \oplus Y \oplus Z = 1$

Quantum Protocol

Goal: $a \oplus b \oplus c = XYZ$

$HII\ (|\Psi\rangle)$

$IHI\ (|\Psi\rangle)$

$IIH\ (|\Psi\rangle)$

$HHH\ (|\Psi\rangle)$

Promise: $X \oplus Y \oplus Z = 1$

Quantum Protocol

Goal: $a \oplus b \oplus c = XYZ$

$$HII\,(|\Psi\rangle) = |000\rangle - |011\rangle + |101\rangle + |110\rangle$$

$$IHI\,(|\Psi\rangle) = |000\rangle + |011\rangle - |101\rangle + |110\rangle$$

$$IIH\,(|\Psi\rangle) = |000\rangle + |011\rangle + |101\rangle - |110\rangle$$

$$HHH\,(|\Psi\rangle)$$

Promise: $X \oplus Y \oplus Z = 1$

Quantum Protocol

Goal: $a \oplus b \oplus c = XYZ$

$$HII\,(|\Psi\rangle) = |000\rangle - |011\rangle + |101\rangle + |110\rangle$$

$$IHI\,(|\Psi\rangle) = |000\rangle + |011\rangle - |101\rangle + |110\rangle$$

$$IIH\,(|\Psi\rangle) = |000\rangle + |011\rangle + |101\rangle - |110\rangle$$

$$HHH\,(|\Psi\rangle) = |001\rangle + |010\rangle + |100\rangle - |111\rangle$$

Promise: $X \oplus Y \oplus Z = 1$

N-Party Generalization

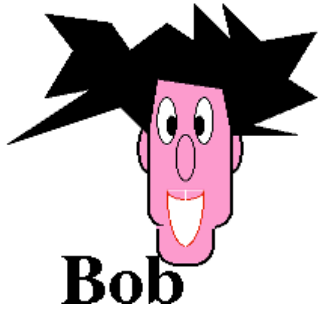
Best classical protocol:

Correct with probability $50\% + 2^{-n/2}$

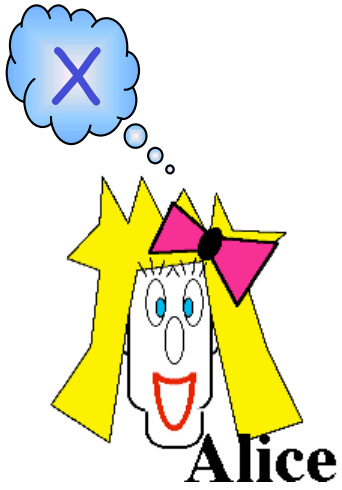
Best quantum protocol:

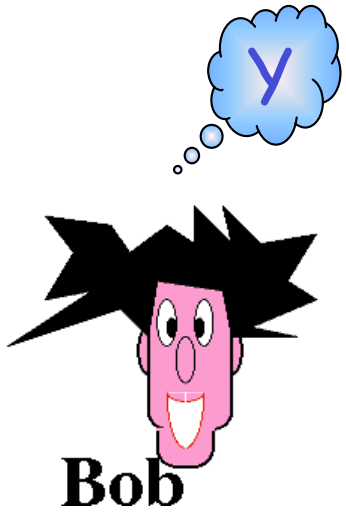
Still always correct!

Spooky Deutsch-Jozsa

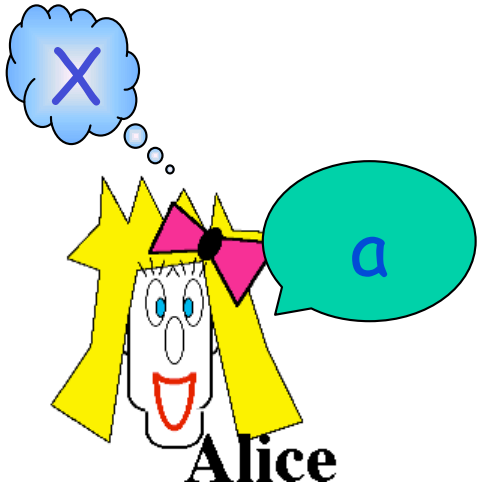


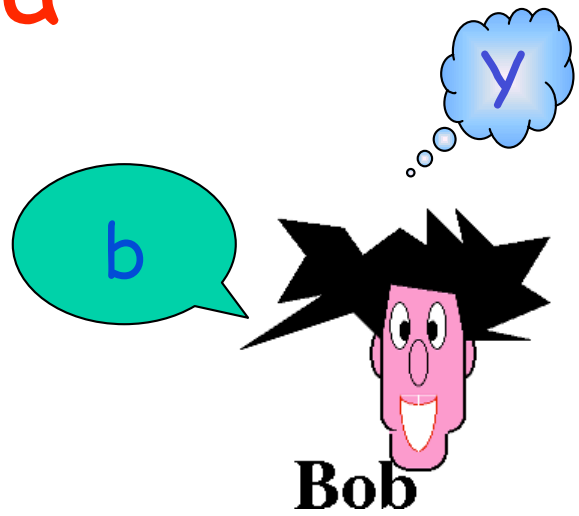
Spooky Deutsch-Jozsa



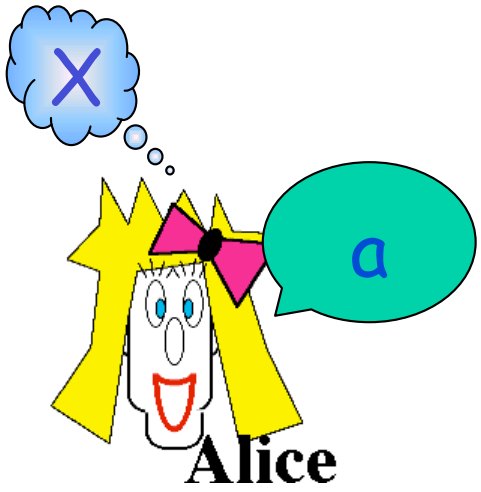


Spooky Deutsch-Jozsa

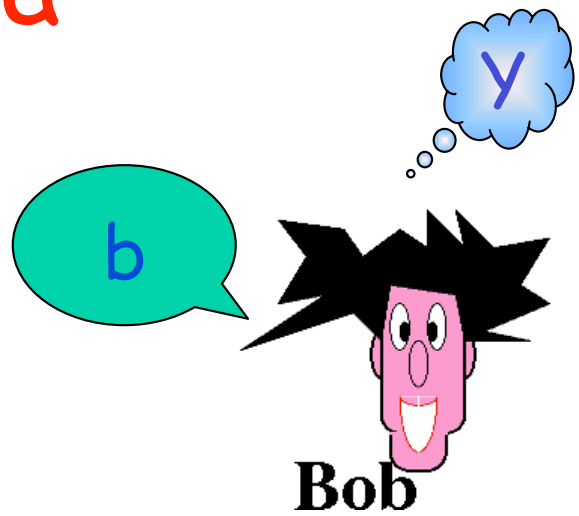




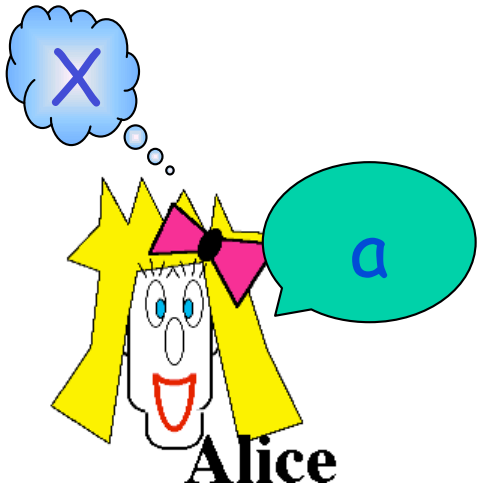
Spooky Deutsch-Jozsa

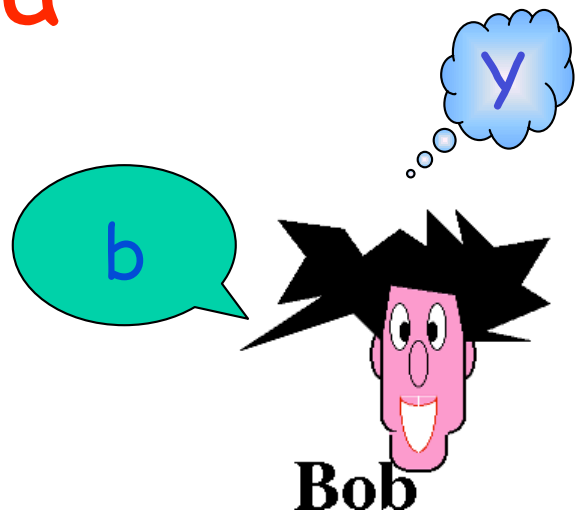


$a = b \iff X = Y$



Spooky Deutsch-Jozsa

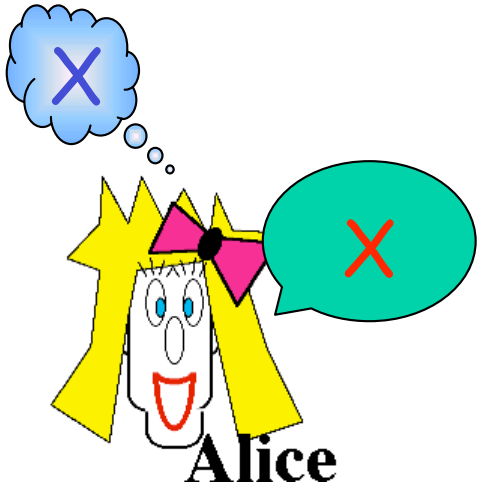




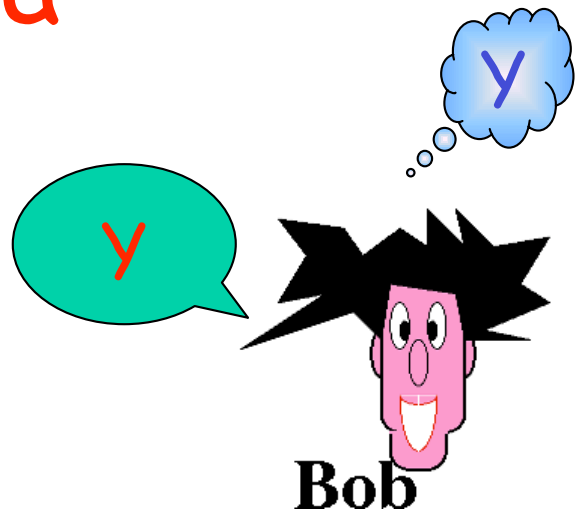
$a = b \iff X = Y$

Too easy!

Spooky Deutsch-Jozsa



$a = b \iff X = Y$

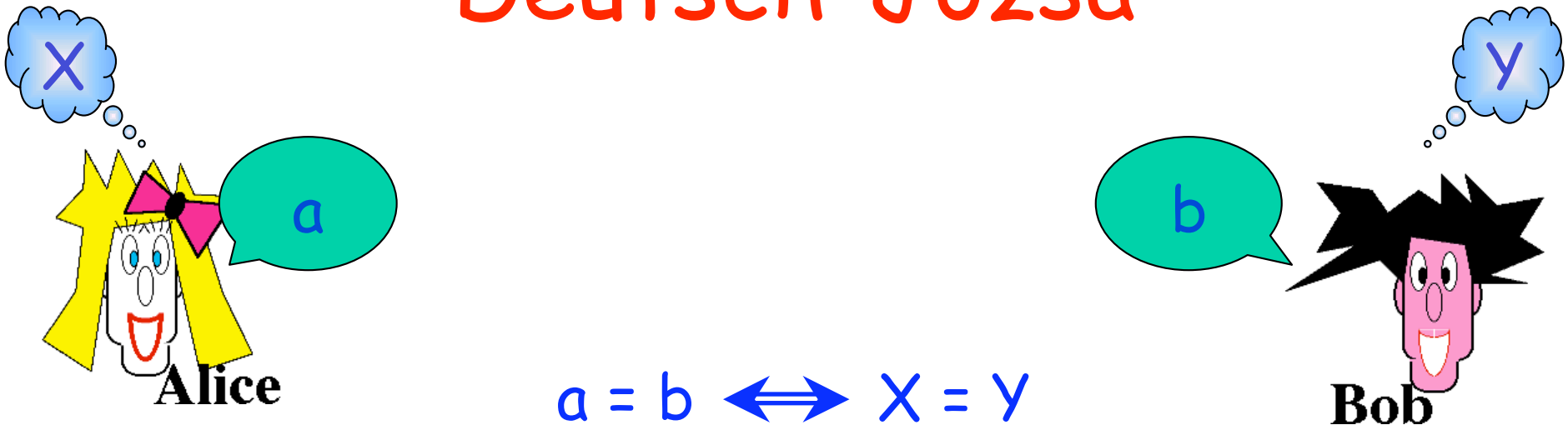


Too easy!

Alice outputs a=X

and Bob outputs b=Y

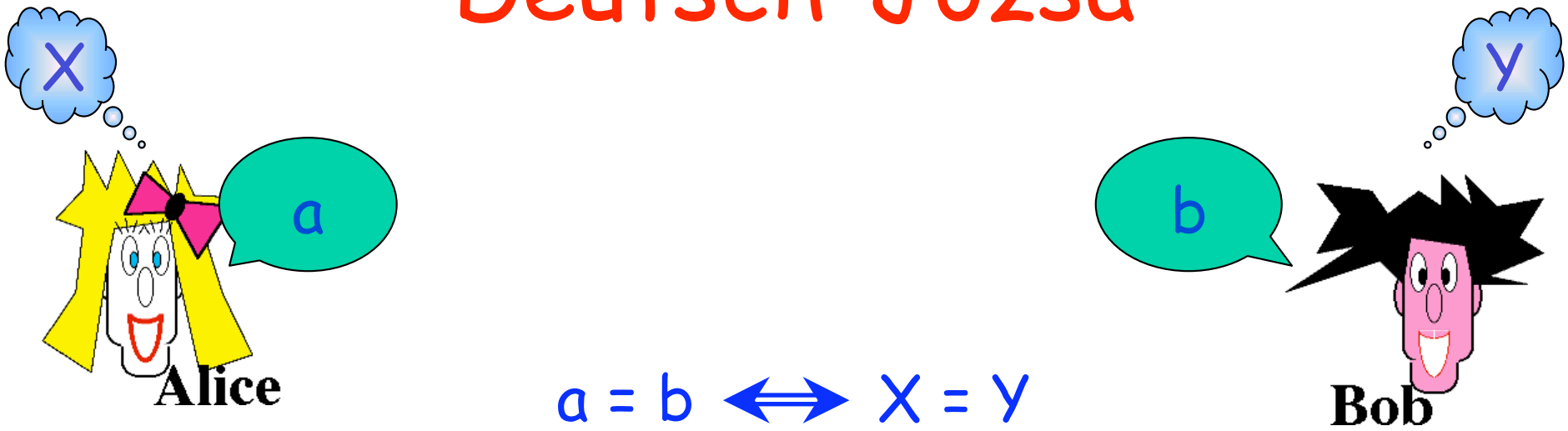
Spooky Deutsch-Jozsa



$a = b \iff X = Y$

Condition to make it interesting

Spooky Deutsch-Jozsa

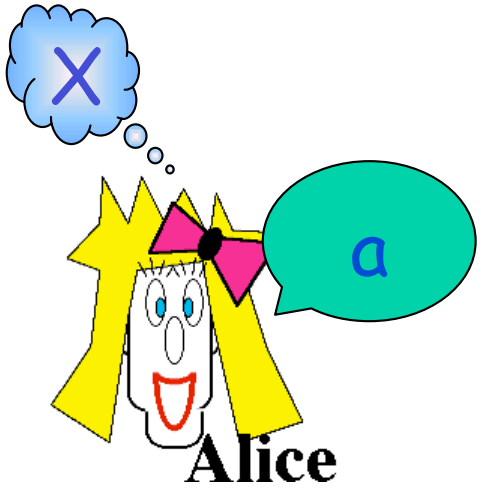


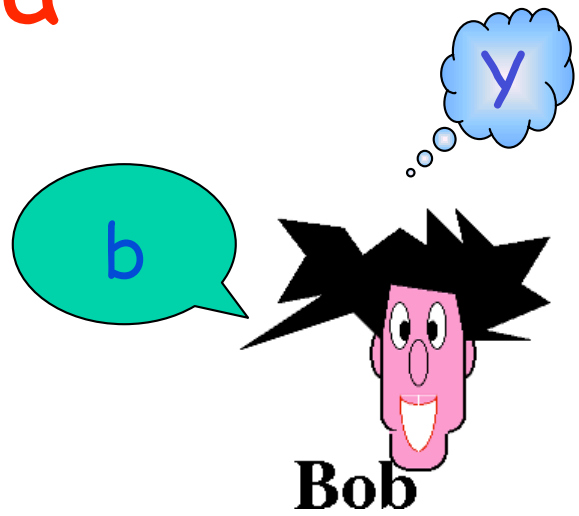
$a = b \iff X = Y$

Condition to make it interesting

a and b must be exponentially shorter than X and Y

Spooky Deutsch-Jozsa





$a = b \iff X = Y$

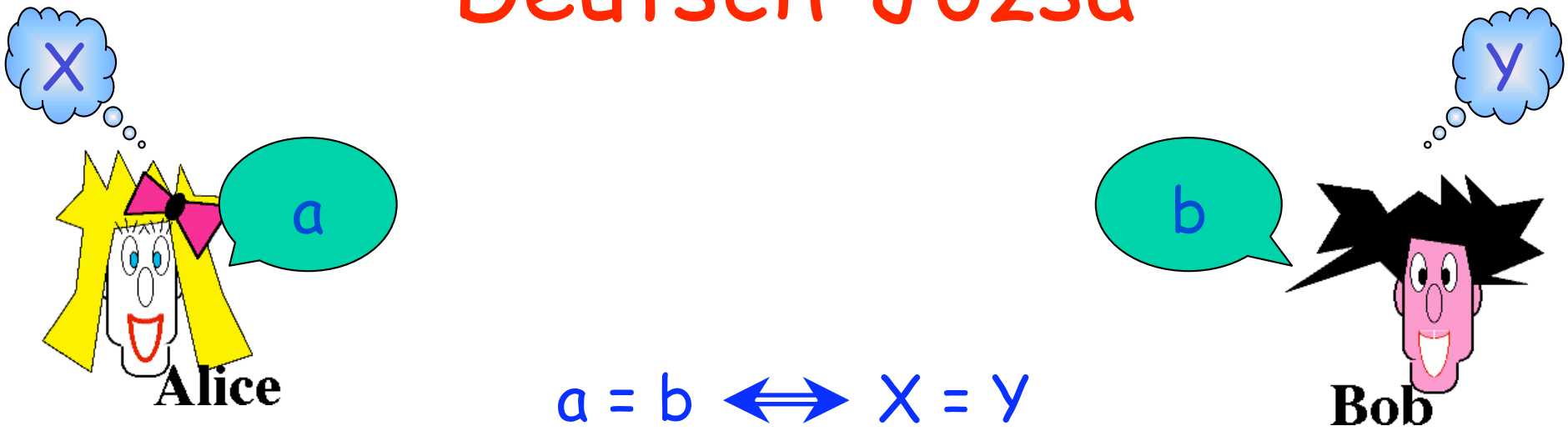
Condition to make it interesting

a and b must be exponentially shorter than X and Y

Example: X and Y are strings of 16 bits

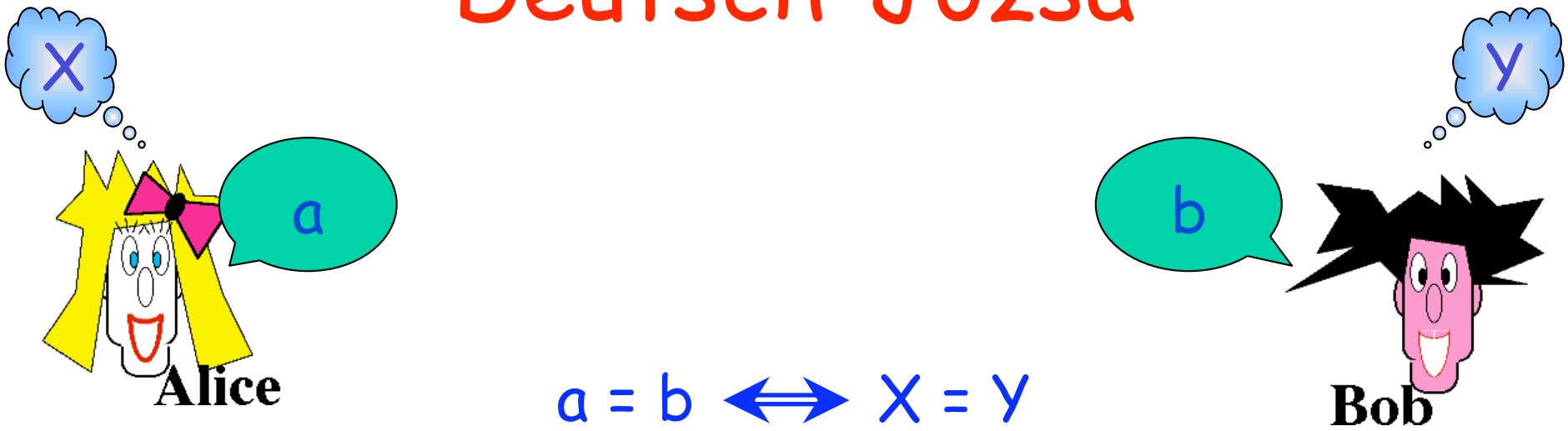
but a and b are strings of only 4 bits

Spooky Deutsch-Jozsa



Good news: this cannot be done classically without communication between Alice and Bob.

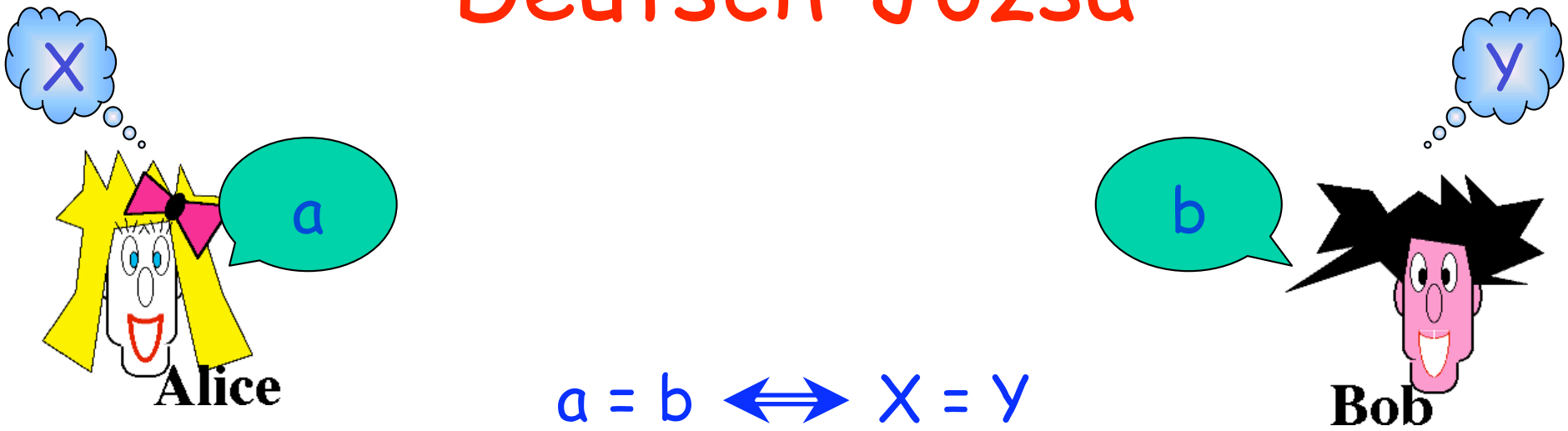
Spooky Deutsch-Jozsa



Good news: this cannot be done classically without communication between Alice and Bob.

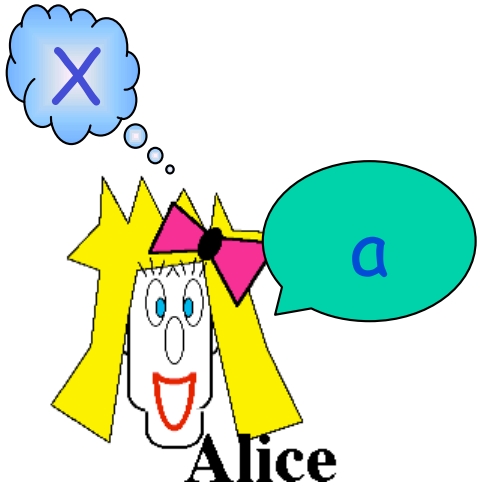
Bad news: this cannot be done without communication even if Alice and Bob are entangled!

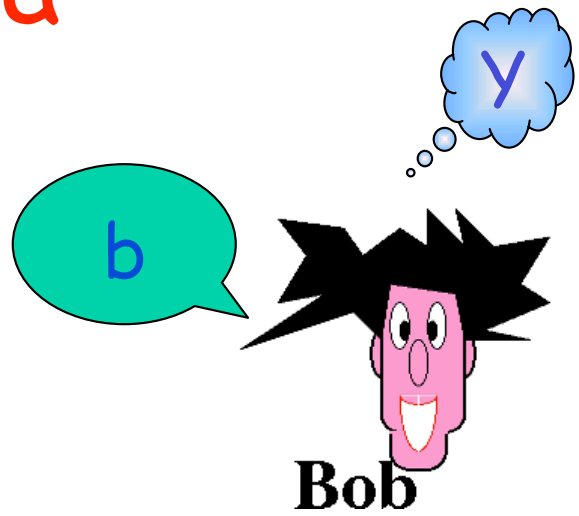
Spooky Deutsch-Jozsa



Promise to get quantum advantage

Spooky Deutsch-Jozsa





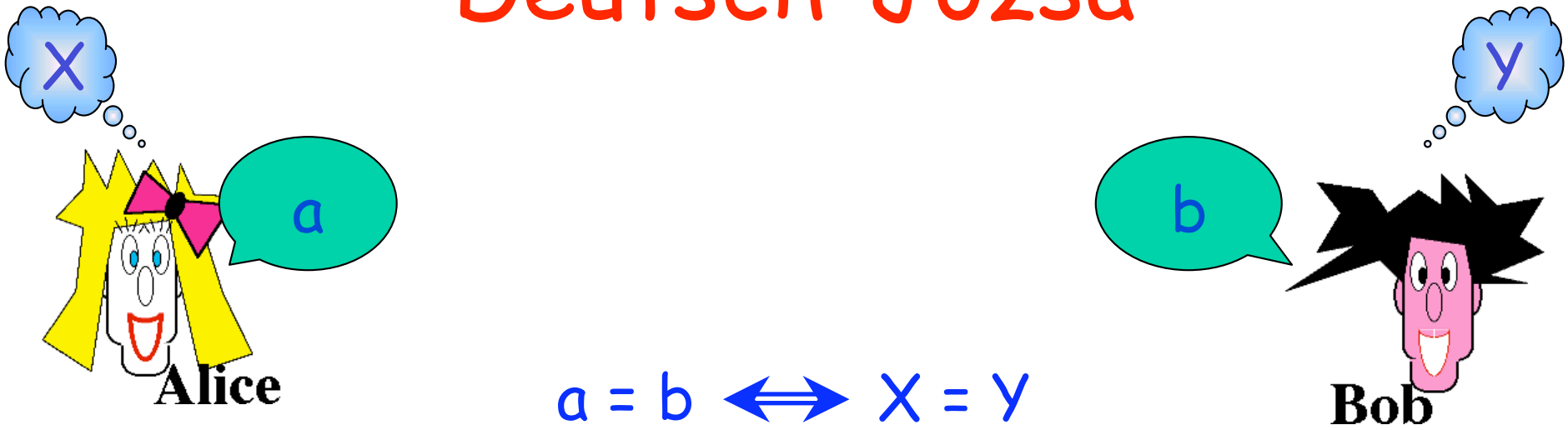
$a = b \iff X = Y$

Promise to get quantum advantage

Either X = Y *or* X and Y differ

in exactly half the bit positions

Spooky Deutsch-Jozsa



Promise to get quantum advantage

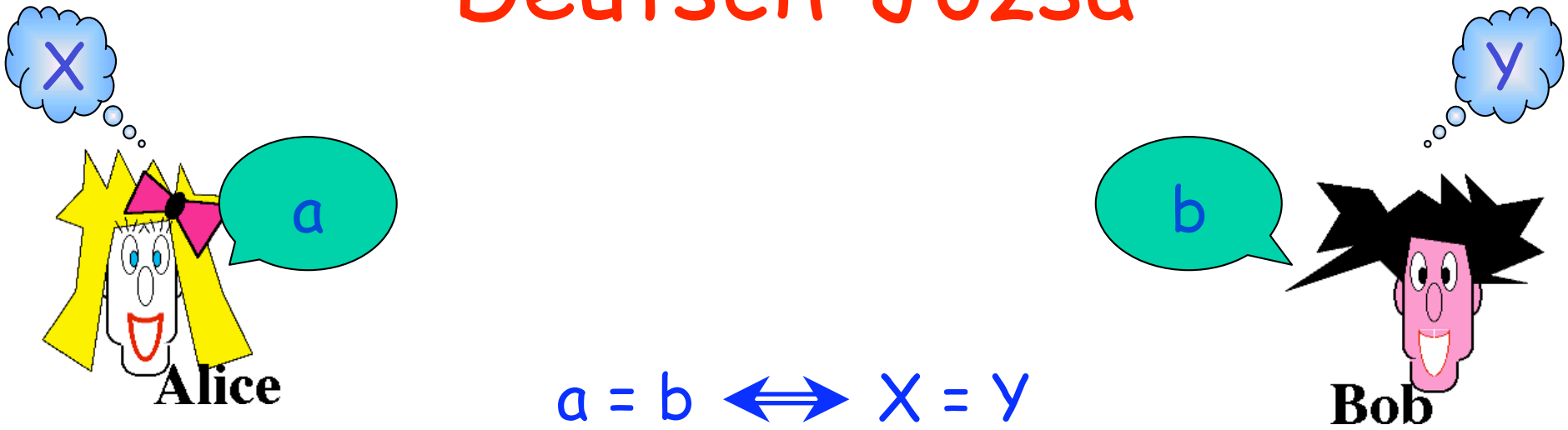
Either X = Y *or* X and Y differ

in exactly half the bit positions

Example: X = 0100110110110100

Y = 0110000010001101

Spooky Deutsch-Jozsa



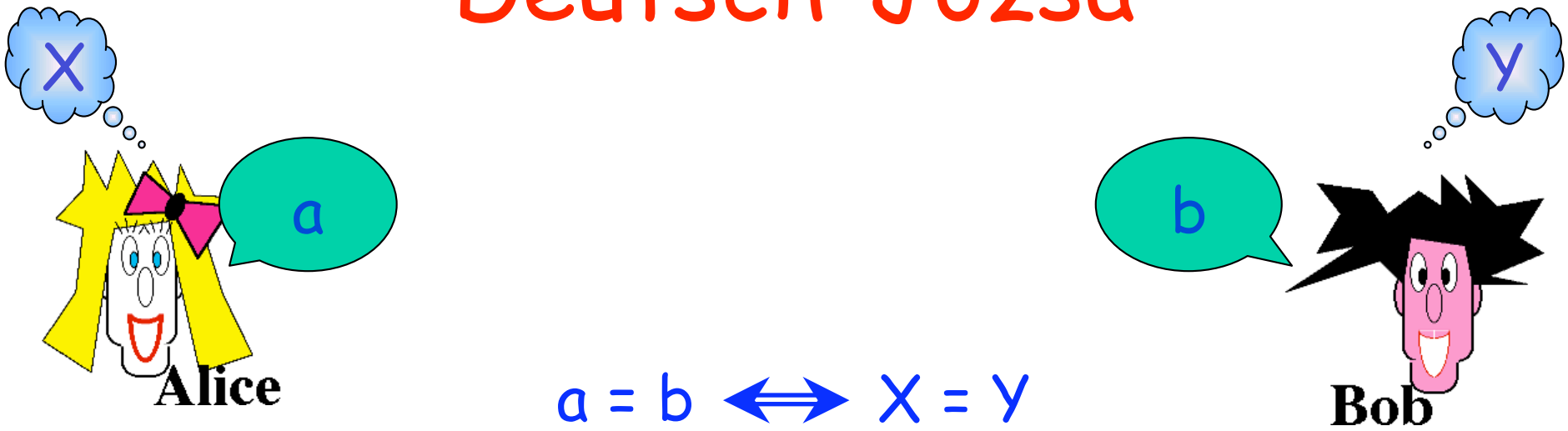
Promise to get quantum advantage

Either X = Y *or* X and Y differ

in exactly half the bit positions

This is still classically impossible

Spooky Deutsch-Jozsa



Promise to get quantum advantage

Either X = Y *or* X and Y differ

in exactly half the bit positions

This is still classically impossible

But entanglement makes it possible!

Deutsch-Josza algorithm

Deutsch-Josza problem:
Given $f : \{0,1\}^n \to \{0,1\}$, decide if f is constant ($\forall x, y, f(x) = f(y)$) or balanced ($|f^{-1}(0)| = |f^{-1}(1)|$).

Deutsch-Josza algorithm(f)

- $|\psi\rangle = H^{\otimes n} F' H^{\otimes n} \ |0\rangle$
- $m =$ Measure($|\psi\rangle$)
- if $m = 0$ answer CONSTANT otherwise BALANCED

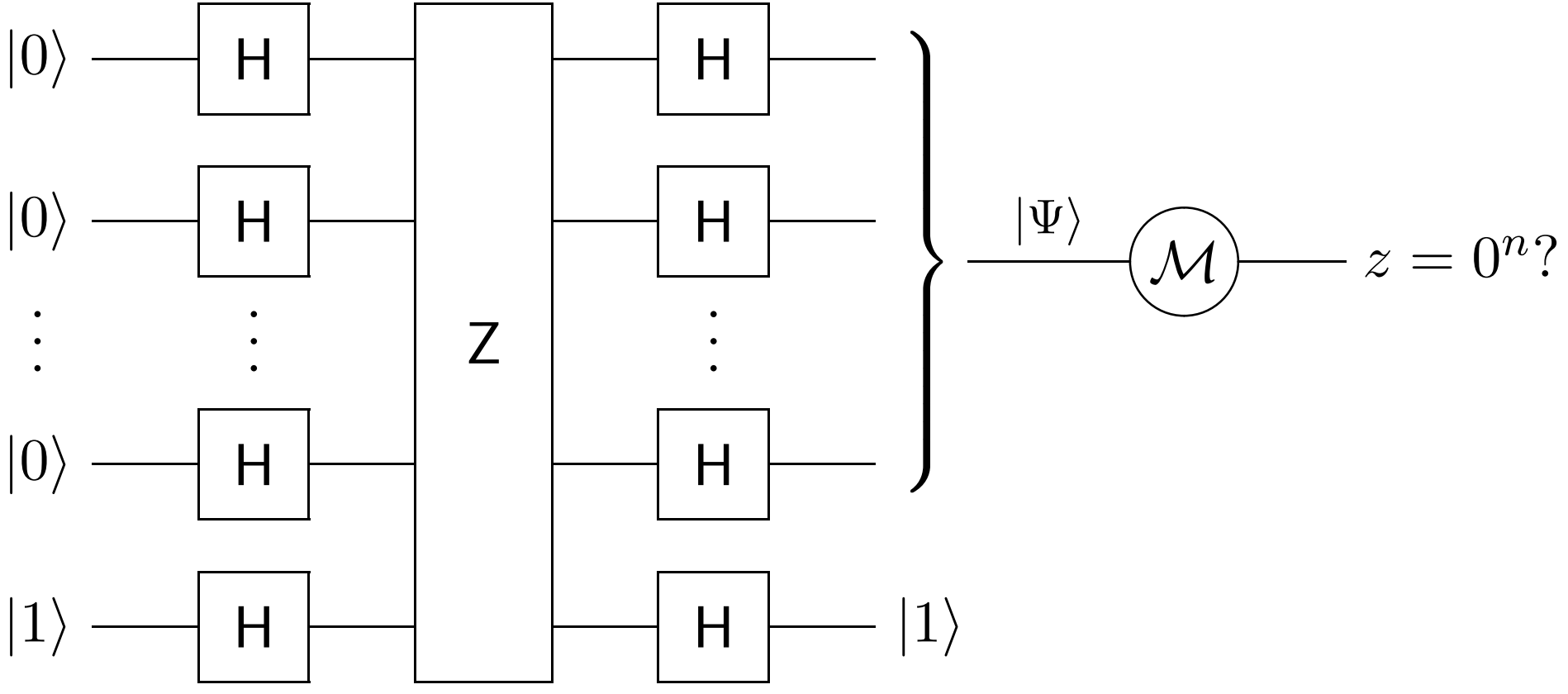
Deterministic classical algorithm: $2^{n-1} + 1$ evaluations of f.

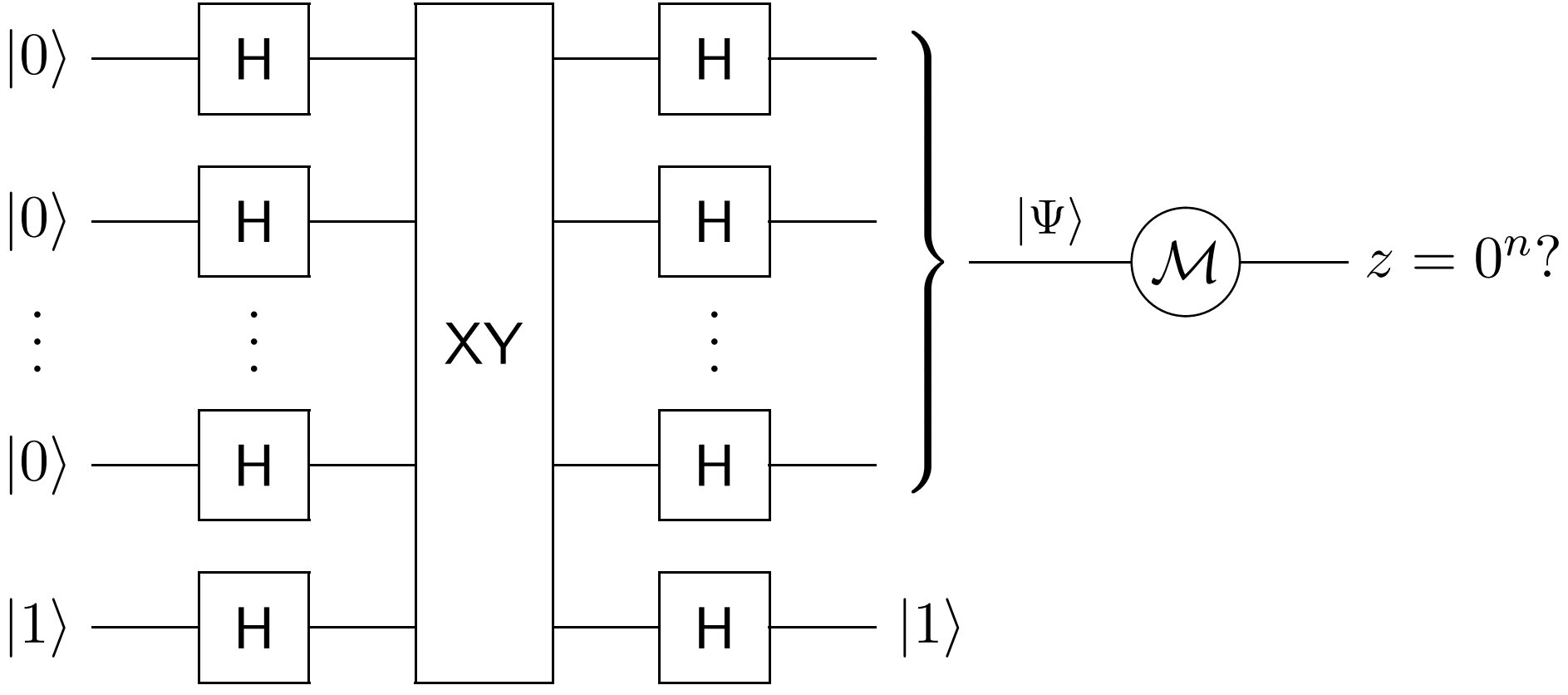
Example: X = 0100110110110100

Y = 0110000010001101

---

z = 0010110100111001


$|0\rangle$
$|0\rangle$
$|0\rangle$
$|1\rangle$
H
H
H
H
Z
H
H
H
H
$|1\rangle$
$|\Psi\rangle$
$\mathcal{M}$
$z = 0^n?$


$|0\rangle$
$|0\rangle$
$|0\rangle$
$|1\rangle$
H
H
H
H
H
H
H
H
XY
$|\Psi\rangle$
$\mathcal{M}$
$z = 0^n?$
$|1\rangle$

Spooky Protocol

- Alice and Bob share n Bell states

$$|\Phi_n^+\rangle = \sum_{z\in\{0,1\}^n} 2^{-n/2}\ |z\rangle|z\rangle\,.$$

  Let $m = 2^n$.

- Alice receives $x \in \{0,1\}^m$
  Bob receives $y \in \{0,1\}^m$.

- Alice performs $U_A : |z\rangle \ \rightarrow\ (-1)^{x_z}\ |z\rangle$
  Bob performs $U_B : |z\rangle \ \rightarrow\ (-1)^{y_z}\ |z\rangle$
  for each $z \in \{0,1\}^n$.

- They both the apply Walsh–Hadamard transform H

$$|0\rangle \overset{\mathsf{H}}{\longmapsto} \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \overset{\mathsf{H}}{\longmapsto} \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle$$

  to each of their n qubits.

$$|z\rangle \overset{\mathsf{H}}{\longmapsto} \sum_{x\in\{0,1\}^n} 2^{-n/2}\ (-1)^{z\cdot x}|x\rangle$$

- They measure their registers:
  Alice obtains a and
  Bob obtains b.

Analysis

- $\sum_{z \in \{0,1\}^n} |z\rangle|z\rangle$ (forget normalization $2^{-n/2}$)

- $\sum_z (-1)^{x_z} \ (-1)^{y_z} \ |z\rangle|z\rangle$

  $= \sum_z (-1)^{x_z \oplus y_z} \ |z\rangle|z\rangle$

- $\sum_z (-1)^{x_z \oplus y_z} \left(\sum_a (-1)^{z \cdot a} |a\rangle \right) \left(\sum_b (-1)^{z \cdot b} |b\rangle \right)$

  $= \sum_{a,b} \left(\sum_z (-1)^{x_z \oplus y_z \oplus \, z \cdot (a \oplus b)} \right) |a\rangle|b\rangle$

Equality Case: $a = b$

- The amplitude α of $|a\rangle|b\rangle$, up to normalization, is

$$\alpha = \sum_{z \in \{0,1\}^n} (-1)^{x_z \oplus y_z \oplus z \cdot (a \oplus b)}$$

$$= \sum_{z \in \{0,1\}^n} (-1)^{z \cdot (a \oplus b)}$$

- This is $\alpha = 0$ when $a \oplus b \neq 0$.
- Thus the probability that $a \neq b$ is 0, and therefore $a = b$ with certainty.

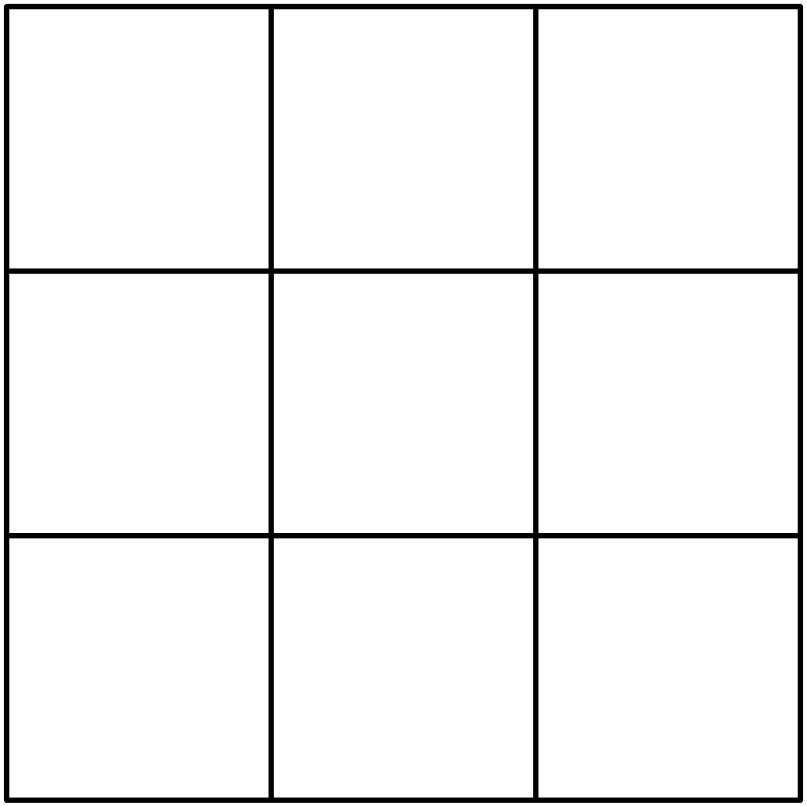
Balanced Case: $d_H(x, y) = m/2$

- The amplitude α of $|a\rangle|b\rangle$, up to normalization, is

$$\begin{aligned}
\alpha &= \sum_{z \in \{0,1\}^n} (-1)^{x_z \oplus y_z \oplus\, z \cdot (a \oplus b)} \\
&= \sum_{z \in \{0,1\}^n} (-1)^{x_z \oplus y_z} \qquad \text{when } a \oplus b = 0 \\
&= 0
\end{aligned}$$

- Thus the probability that $a = b$ is 0,
  and therefore $a \neq b$ with certainty.

Magic Square



Magic Square

0	1	1
0	0	0
1	0	1

Magic Square

0	1	1
0	0	0
1	0	1

even

Magic Square

0	1	1	even
0	0	0	even
1	0	1	

Magic Square

0	1	1	even
0	0	0	even
1	0	1	even

Magic Square

0	1	1	even
0	0	0	even
1	0	1	even
odd			

Magic Square

0	1	1	even
0	0	0	even
1	0	1	even
odd	odd		

Magic Square

0	1	1	even
0	0	0	even
1	0	1	even
odd	odd	odd	

Magic Square

0	1	1	even
0	0	0	even
1	0	1	even
odd	odd	~~odd~~	

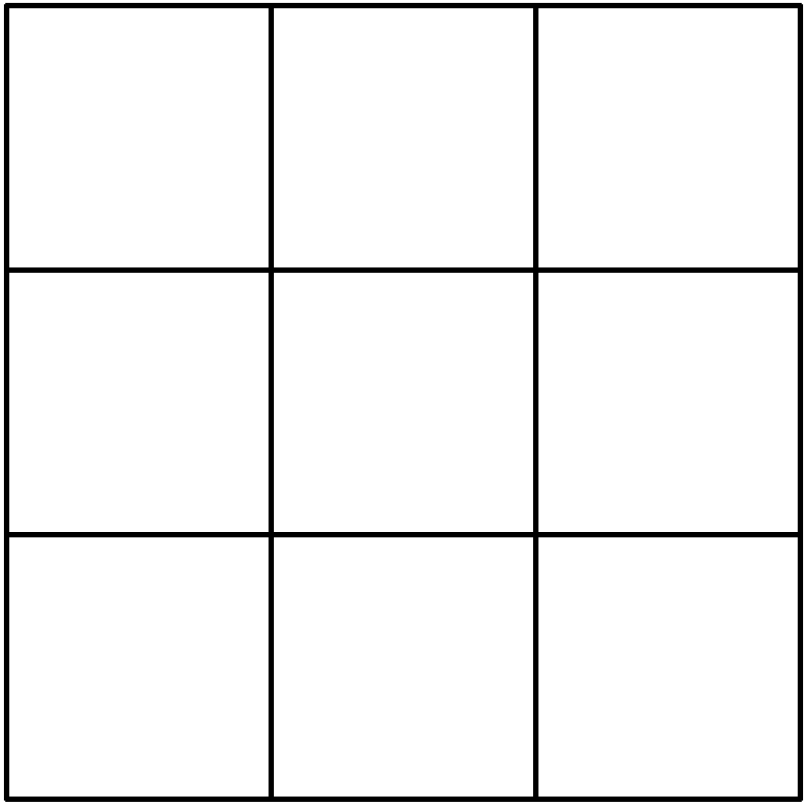
Magic Square

0	1	1	even
0	0	1	even
1	0	1	even
odd	odd	odd	

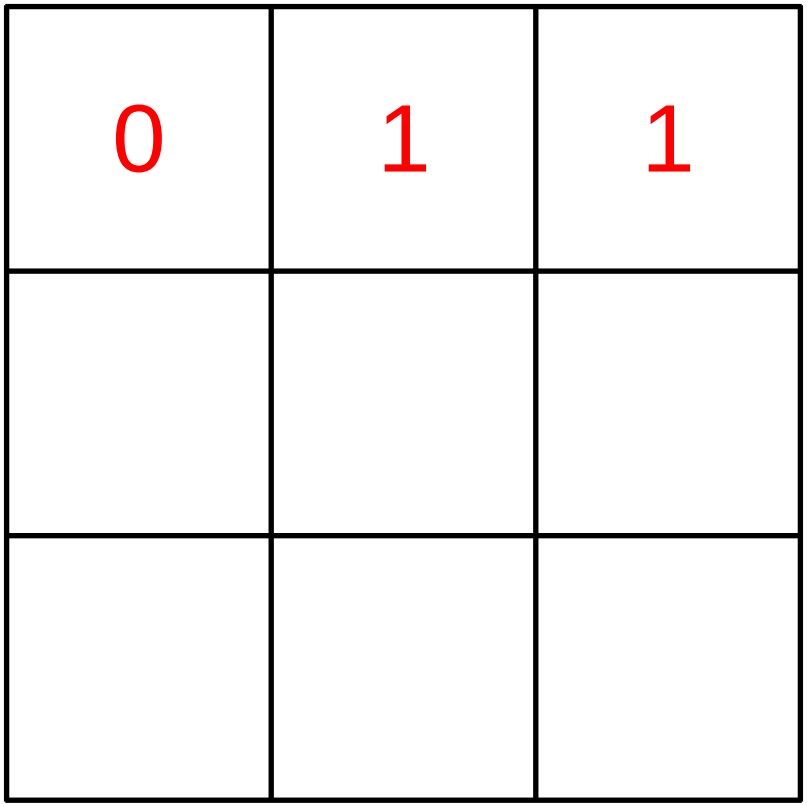
Magic Square

0	1	1	even
0	0	1	~~even~~
1	0	1	even
odd	odd	odd	

Question for Alice: row 1

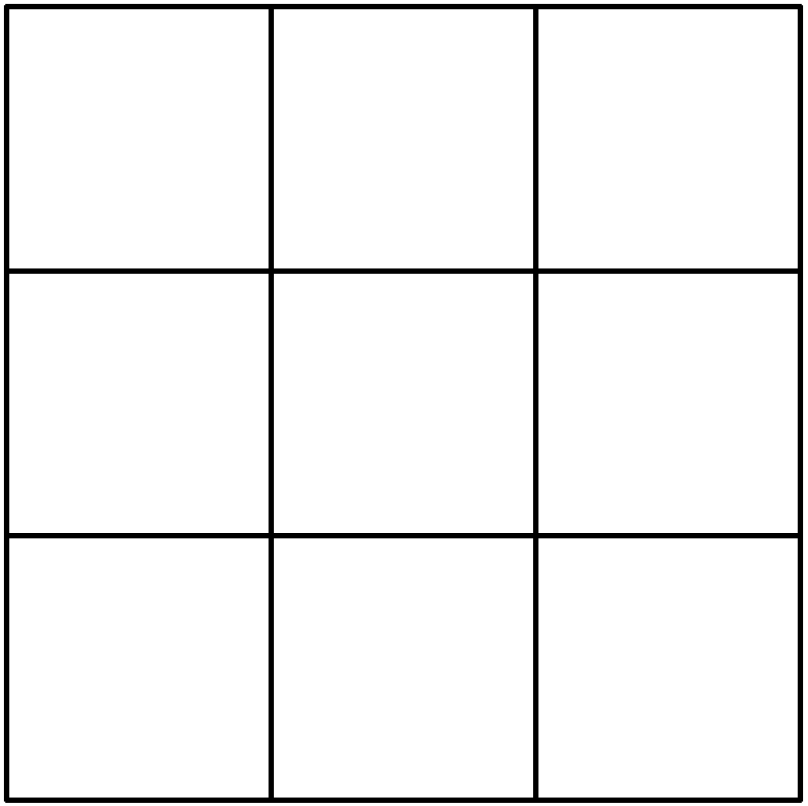


Question for Alice: row 1

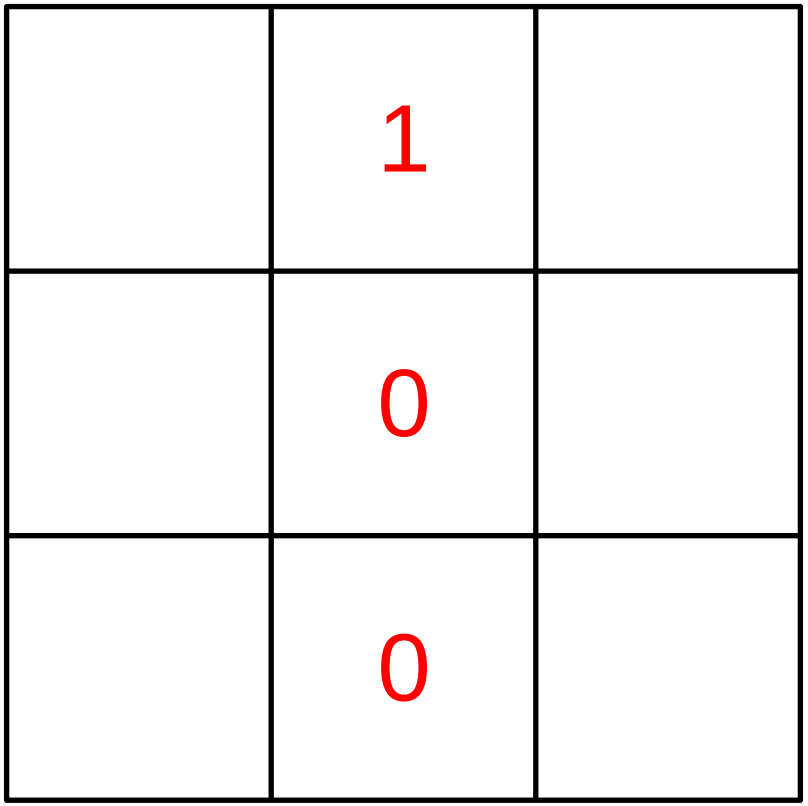


even

Question for Bob: column 2

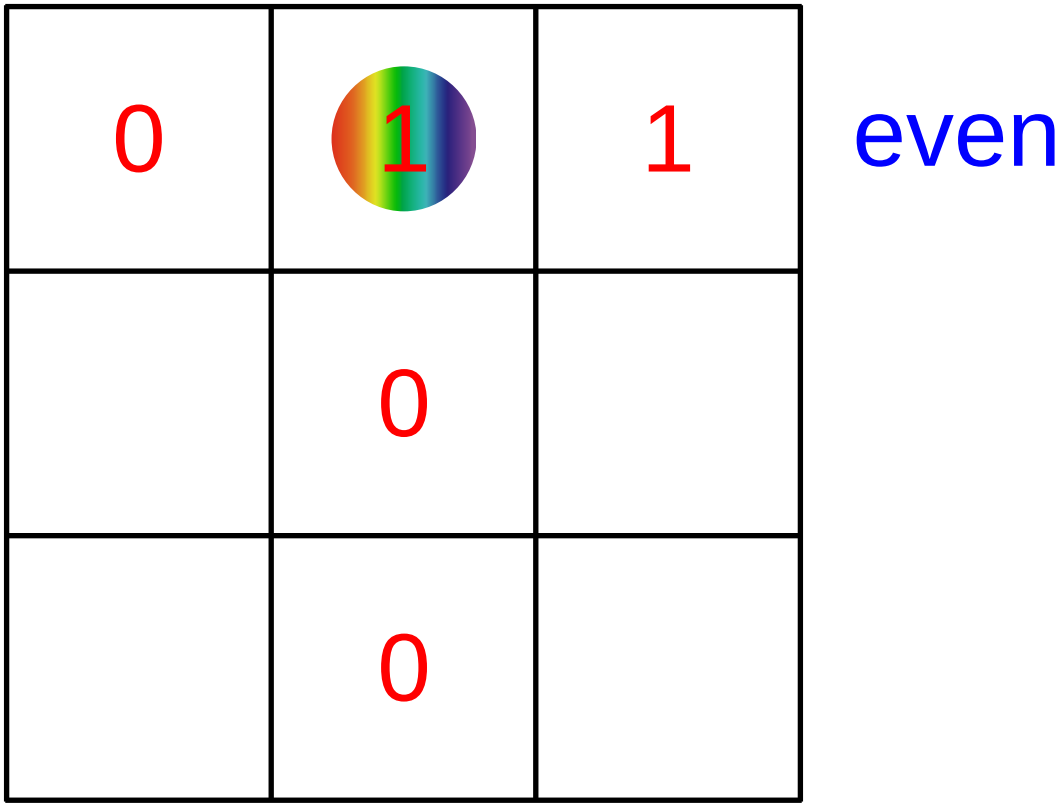


Question for Bob: column 2



odd

Answers must match!



Magic Square

0	1	1	even
0	0		even
1	0	1	even
odd	odd	odd	

Magic Square Cheating

0	1	1	even
0	0	0/1	even
1	0	1	even
odd	odd	odd	

Magic Square

Classically: without communication Alice and Bob cannot succeed with a probability better than 8/9

Magic Square

Classically: without communication Alice and Bob cannot succeed with a probability better than 8/9

If they are entangled, Alice and Bob can succeed every time!

5.2. **Quantum Winning Strategy.** The quantum winning strategy for the magic square game is not as simple as the classical impossibility proof. First, Alice and Bob share the entangled state

$$|\psi\rangle = \tfrac{1}{2}|0011\rangle - \tfrac{1}{2}|0110\rangle - \tfrac{1}{2}|1001\rangle + \tfrac{1}{2}|1100\rangle$$

The first two qubits belong to Alice and the last two to Bob. Upon receiving their inputs x and y, Alice and Bob apply unitary transformations A_x and B_y, respectively, according to the following matrices.

$$A_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} i & 0 & 0 & 1 \\ 0 & -i & 1 & 0 \\ 0 & i & 1 & 0 \\ 1 & 0 & 0 & i \end{bmatrix},\ A_2 = \frac{1}{2}\begin{bmatrix} i & 1 & 1 & i \\ -i & 1 & -1 & i \\ i & 1 & -1 & -i \\ -i & 1 & 1 & -i \end{bmatrix},\ A_3 = \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}$$

$$B_1 = \frac{1}{2}\begin{bmatrix} i & -i & 1 & 1 \\ -i & -i & 1 & -1 \\ 1 & 1 & -i & i \\ -i & i & 1 & 1 \end{bmatrix},\ B_2 = \frac{1}{2}\begin{bmatrix} -1 & i & 1 & i \\ 1 & i & 1 & -i \\ 1 & -i & 1 & i \\ -1 & -i & 1 & -i \end{bmatrix},\ B_3 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix}$$

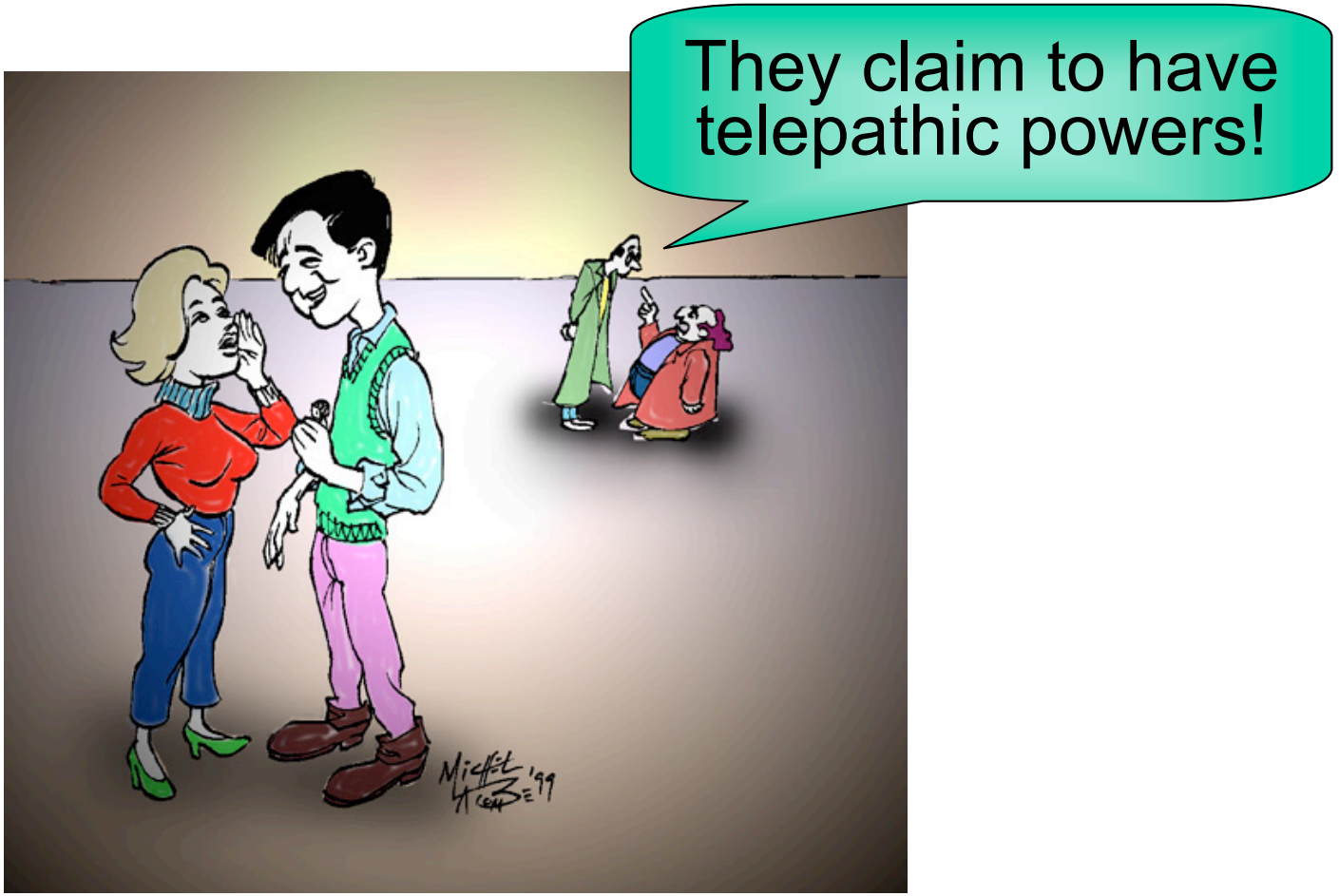
Consider for example inputs $x = 2$ and $y = 3$. After Alice and Bob apply A_2 and B_3, respectively, the state evolves to

$$(A_2 \otimes B_3)|\psi\rangle = \tfrac{1}{2\sqrt{2}}\big[|0000\rangle - |0010\rangle - |0101\rangle + |0111\rangle \\ +|1001\rangle + |1011\rangle - |1100\rangle - |1110\rangle\big]$$

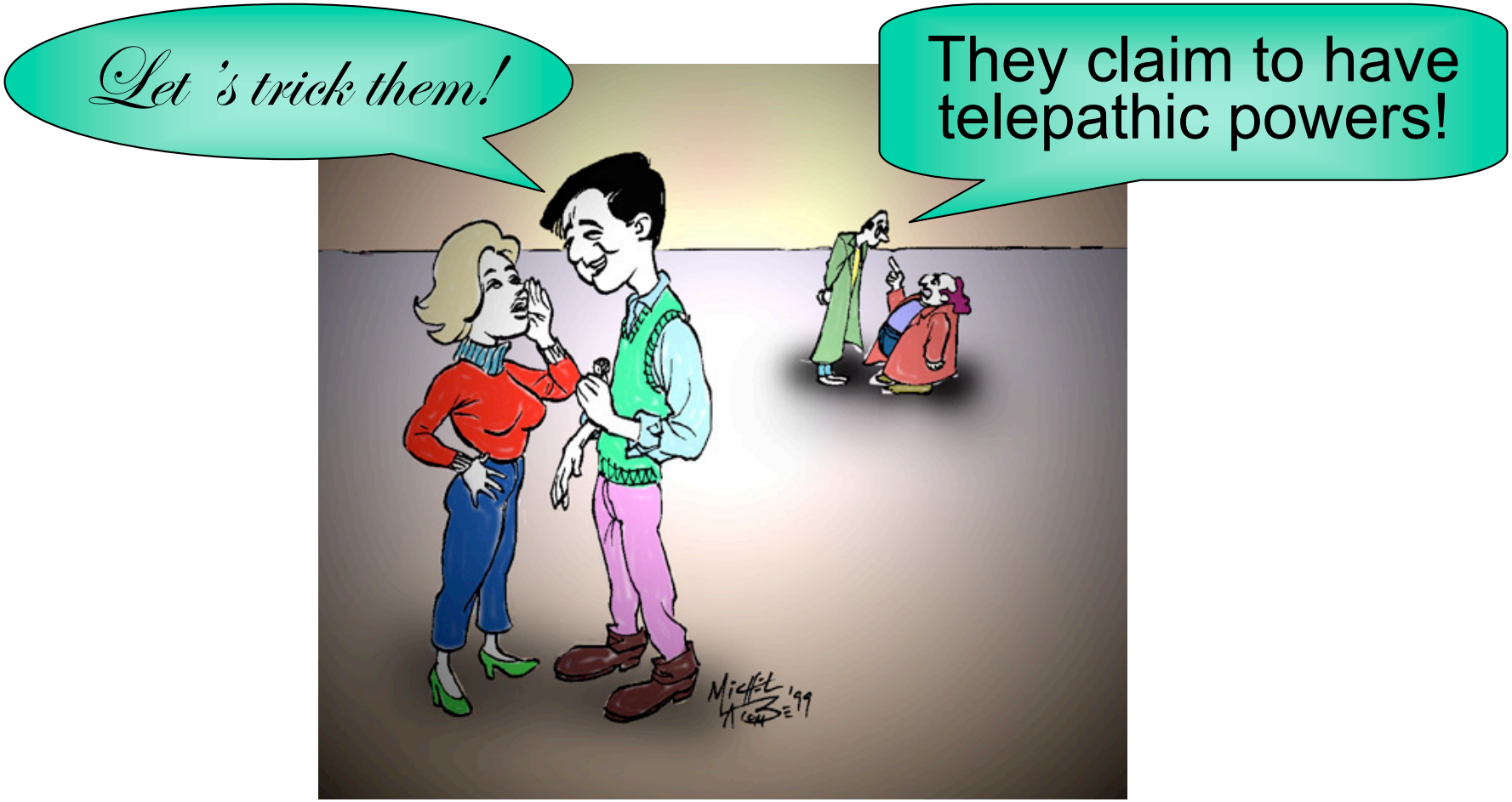
After measurement, Alice and Bob could obtain 10 and 01, for instance. In that case, Alice would complete with bit 1 so that her output $a = 101$ has even parity and Bob would complete with bit 0 so that his output $b = 010$ has odd parity. Xavier and Yolande will be satisfied with the answer since both Alice and Bob agree that the third entry of the second row is indeed the same as the second entry of the third column: $a_3 = b_2 = 1$. It is easy to check that the seven other possible answers that Alice and Bob could have given on this example are all appropriate. The verification that this quantum strategy wins also on the other eight possible questions is tedious but straightforward.

Pseudo Telepathy

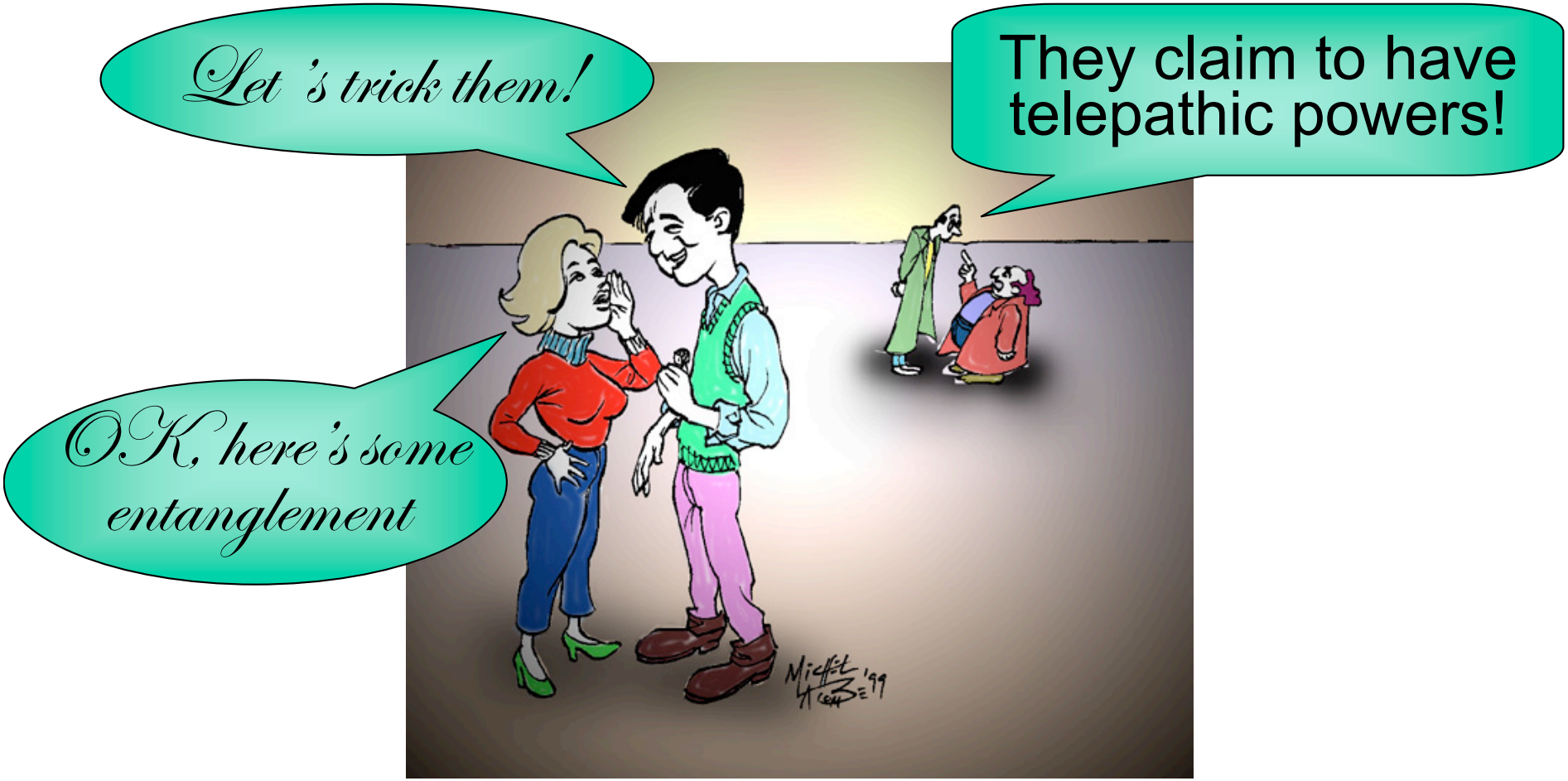
Pseudo Telepathy



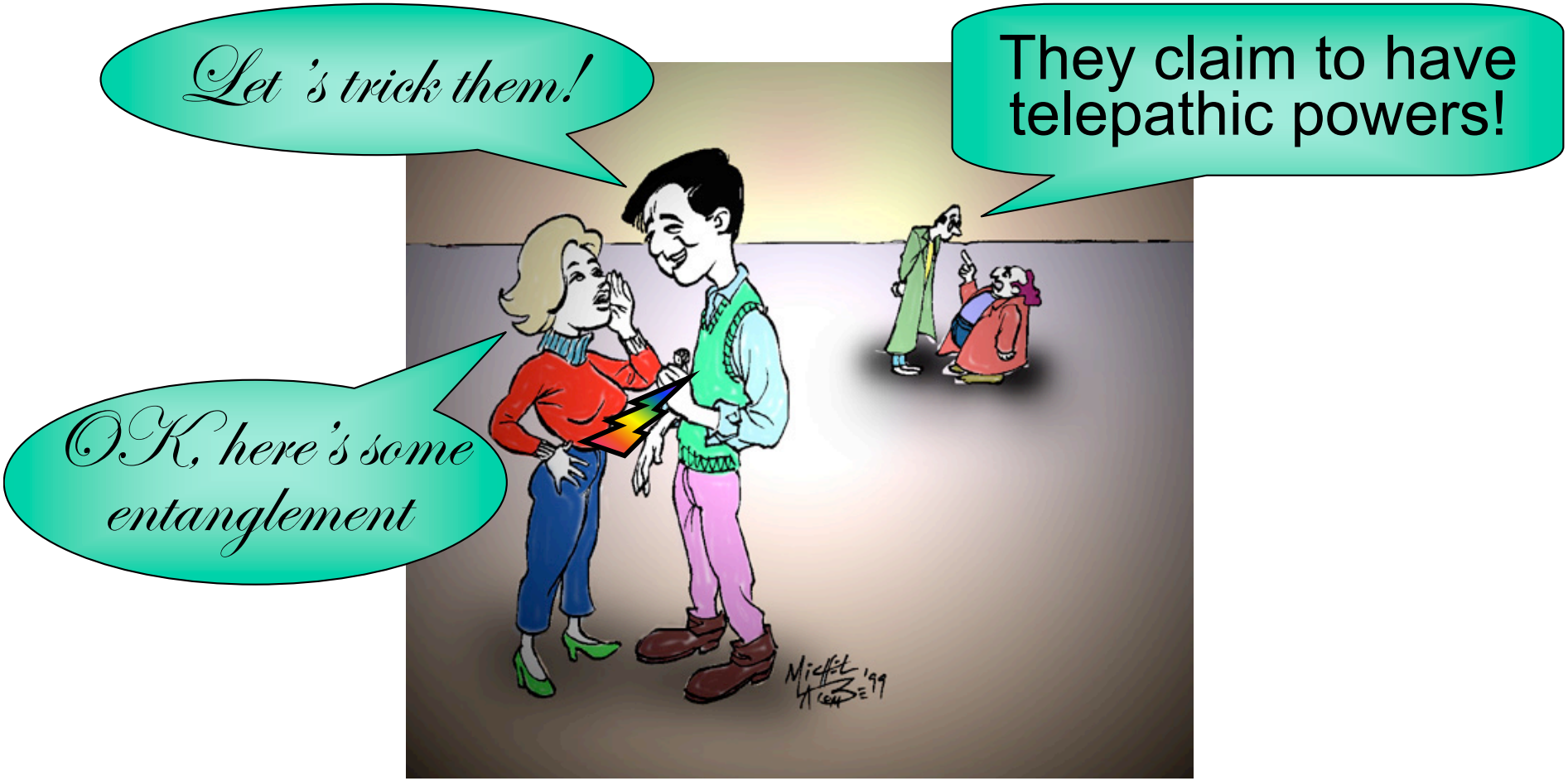
Pseudo Telepathy



Pseudo Telepathy



Pseudo Telepathy



Pseudo Telepathy

Pseudo Telepathy

Pseudo Telepathy

Pseudo Telepathy

For Further Reading

Quantum Pseudo Telepathy

Foundations of Physics **35**(11)
November 2005

(Preliminary: quant–ph/0407221)