Fun and games with quantum entanglement

Stephanie Wehner

What to expect

- Quantum Bits
  - What makes them different?
- Entanglement
  - Action at a distance…
  - Why is this so special?
  - Playing games with entanglement
- Applications
  - Why bother?

Quantum Bits

Classical Bits: 0 or 1

Quantum Bits: 0 or 1 at the same time!

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Quantum Bits

Classical Bits: 0 or 1

Quantum Bits: 0 or 1 at the same time! Cannot be copied.

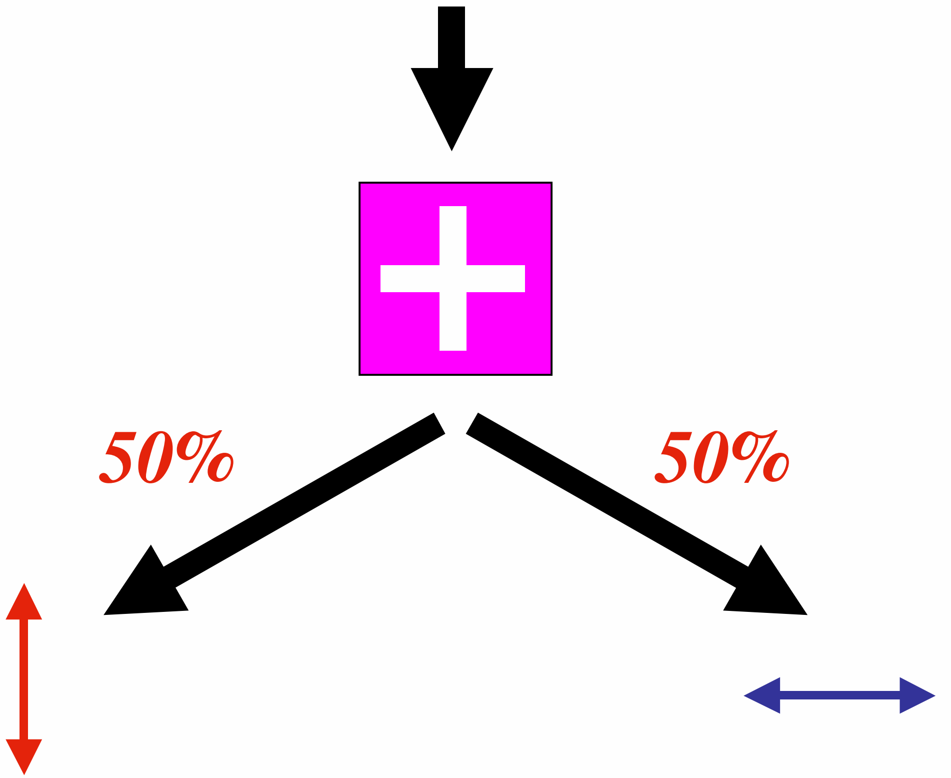
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\Vert$$

$$\frac{1}{\sqrt{2}} \updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow$$

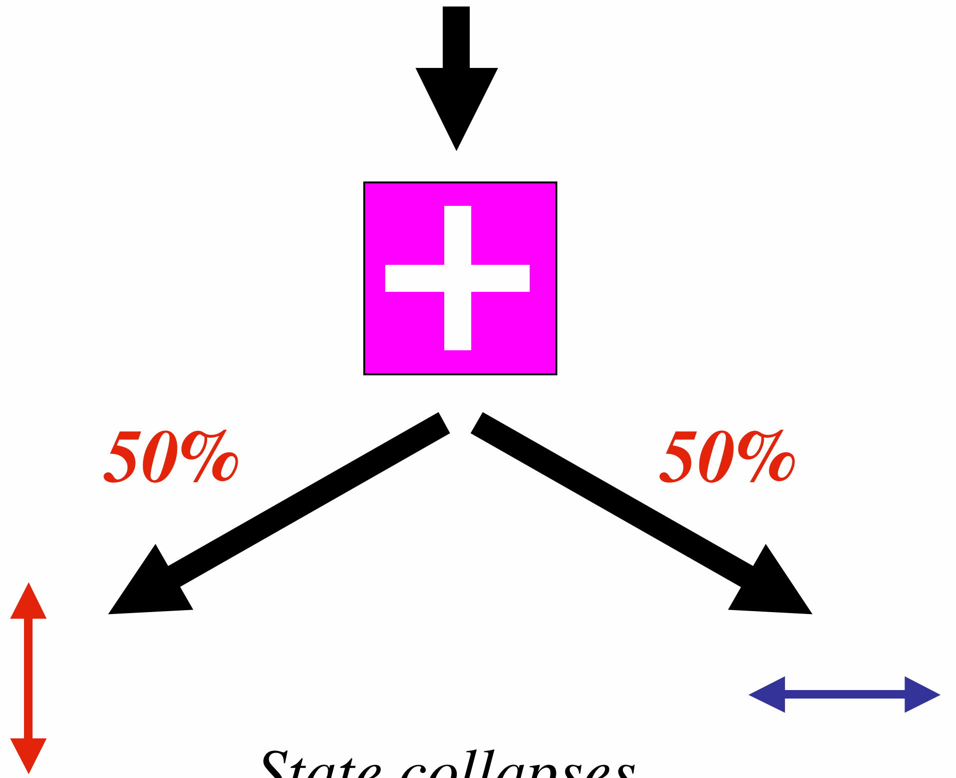
Measurements

$$\frac{1}{\sqrt{2}}\updownarrow \quad + \quad \frac{1}{\sqrt{2}}\leftrightarrow$$



Measurements

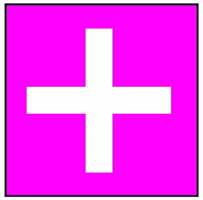
$$\frac{1}{\sqrt{2}} \updownarrow \quad + \quad \frac{1}{\sqrt{2}} \leftrightarrow$$



State collapses

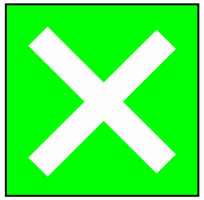
Different basis...

Basis 1: Vertical and Horizontal

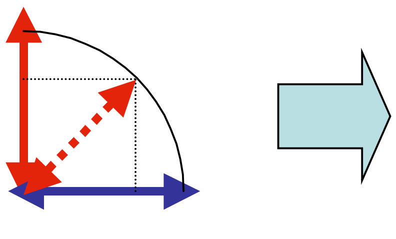


0 $\updownarrow$ 1 $\leftrightarrow$

Basis 2: Diagonal

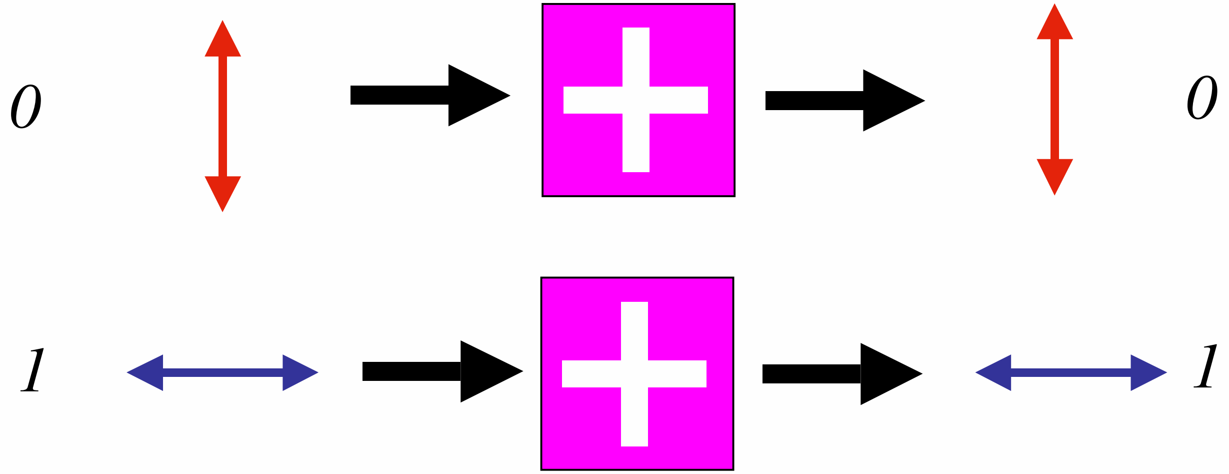


0 $\nearrow\!\!\!\!\swarrow$ 1 $\nwarrow\!\!\!\!\searrow$

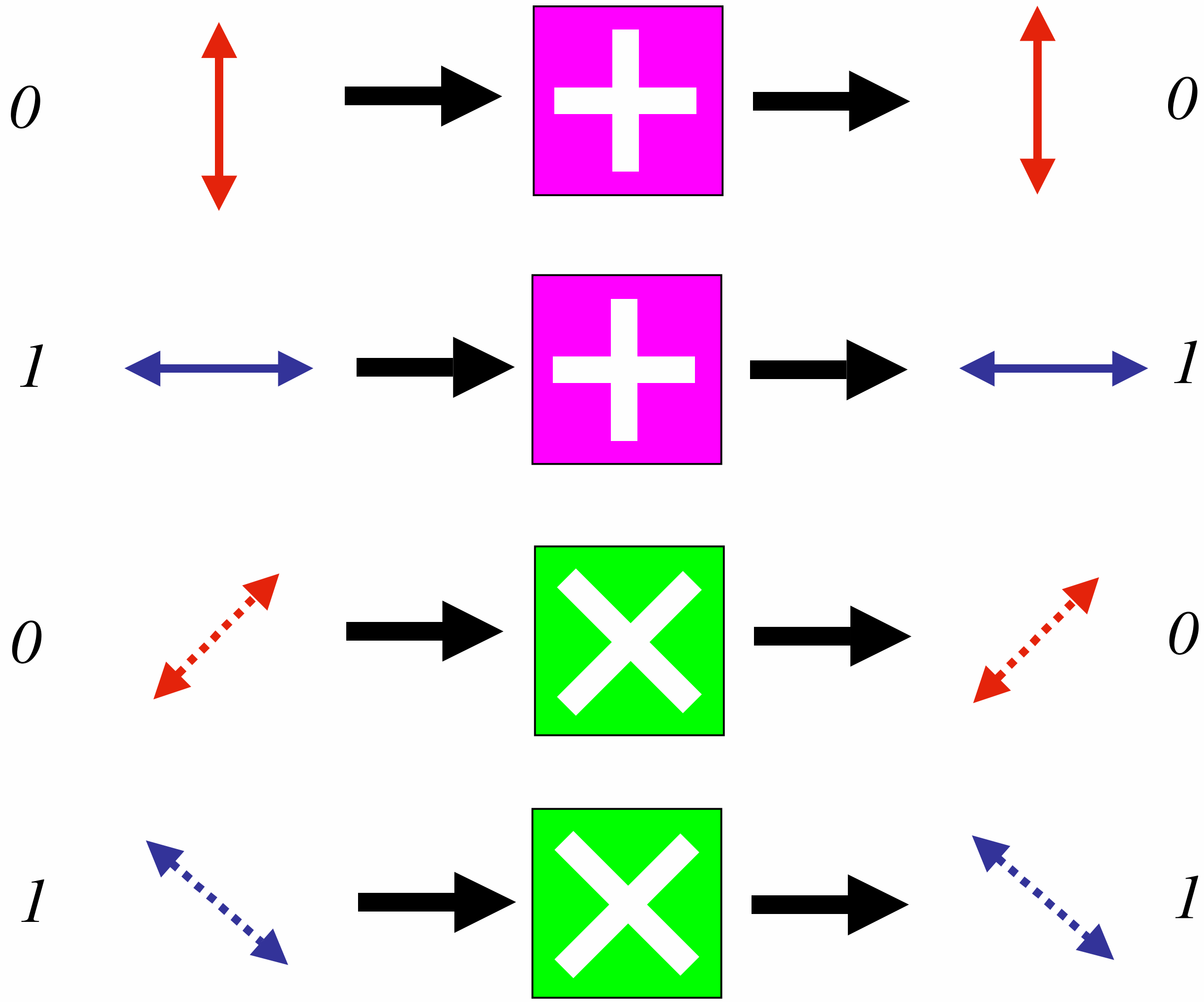


$$\nearrow\!\!\!\!\swarrow \; = \frac{1}{\sqrt{2}} \updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow$$

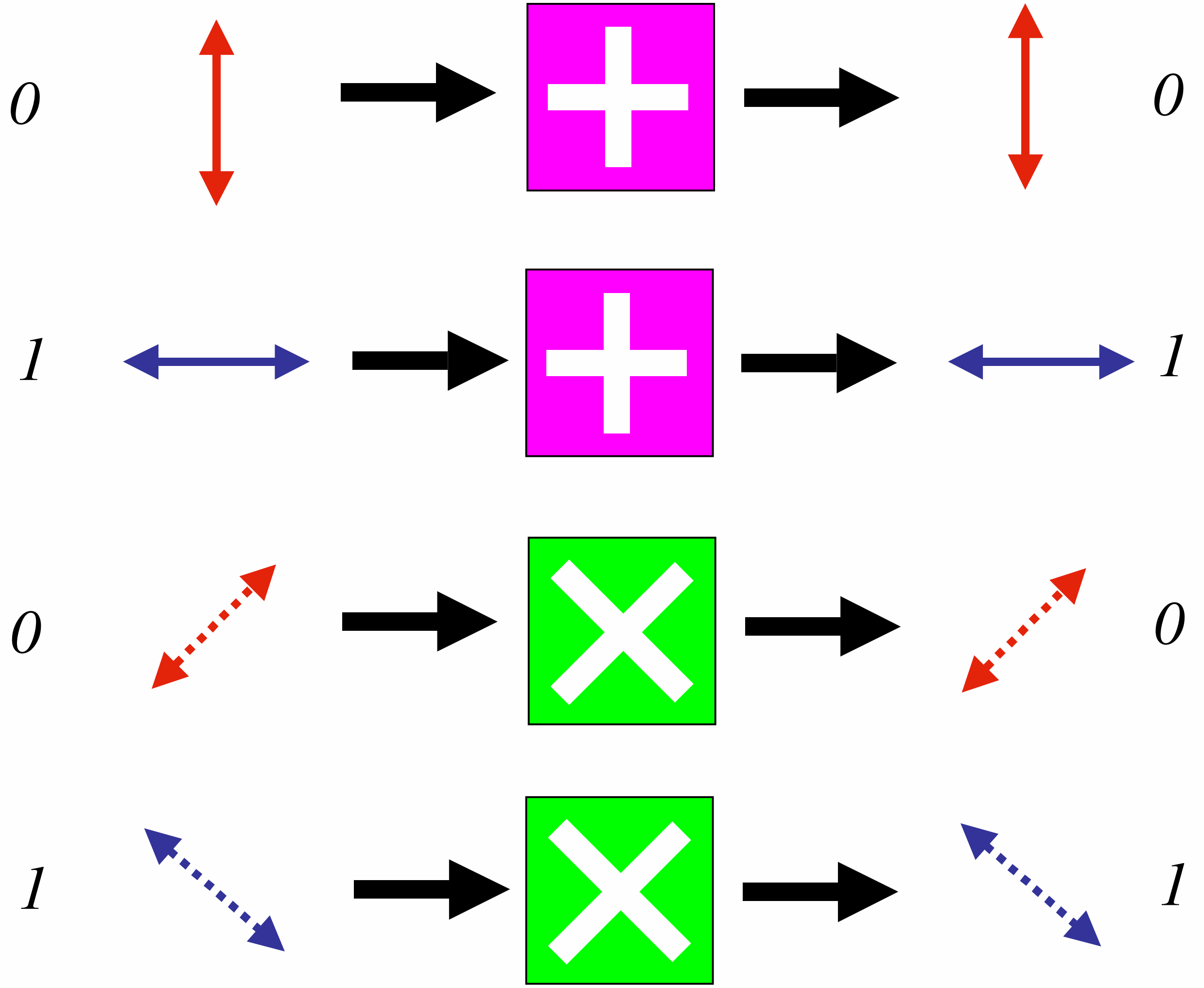
Measurement in the same basis



Measurement in the same basis

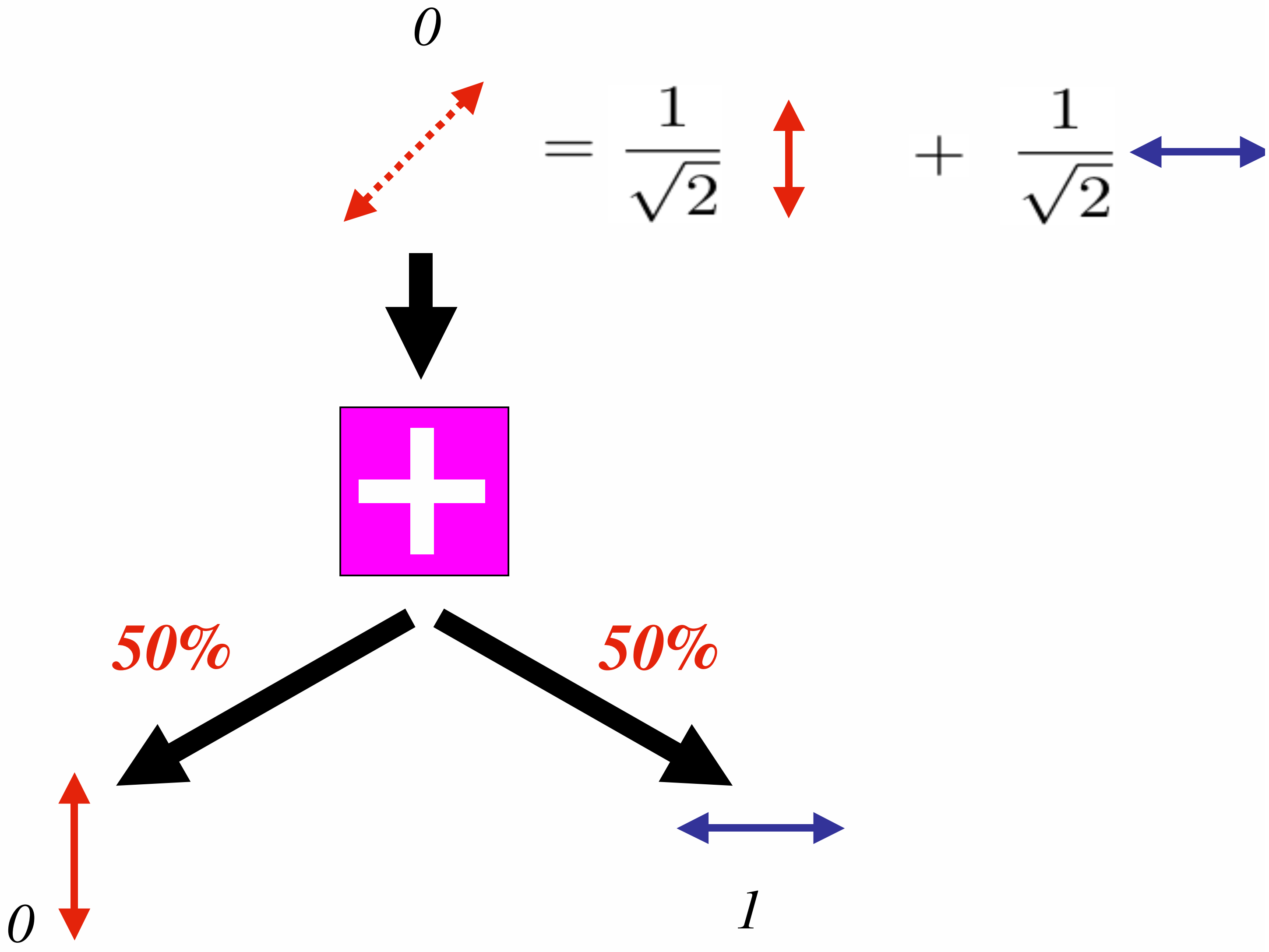


Measurement in the same basis

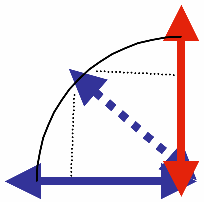


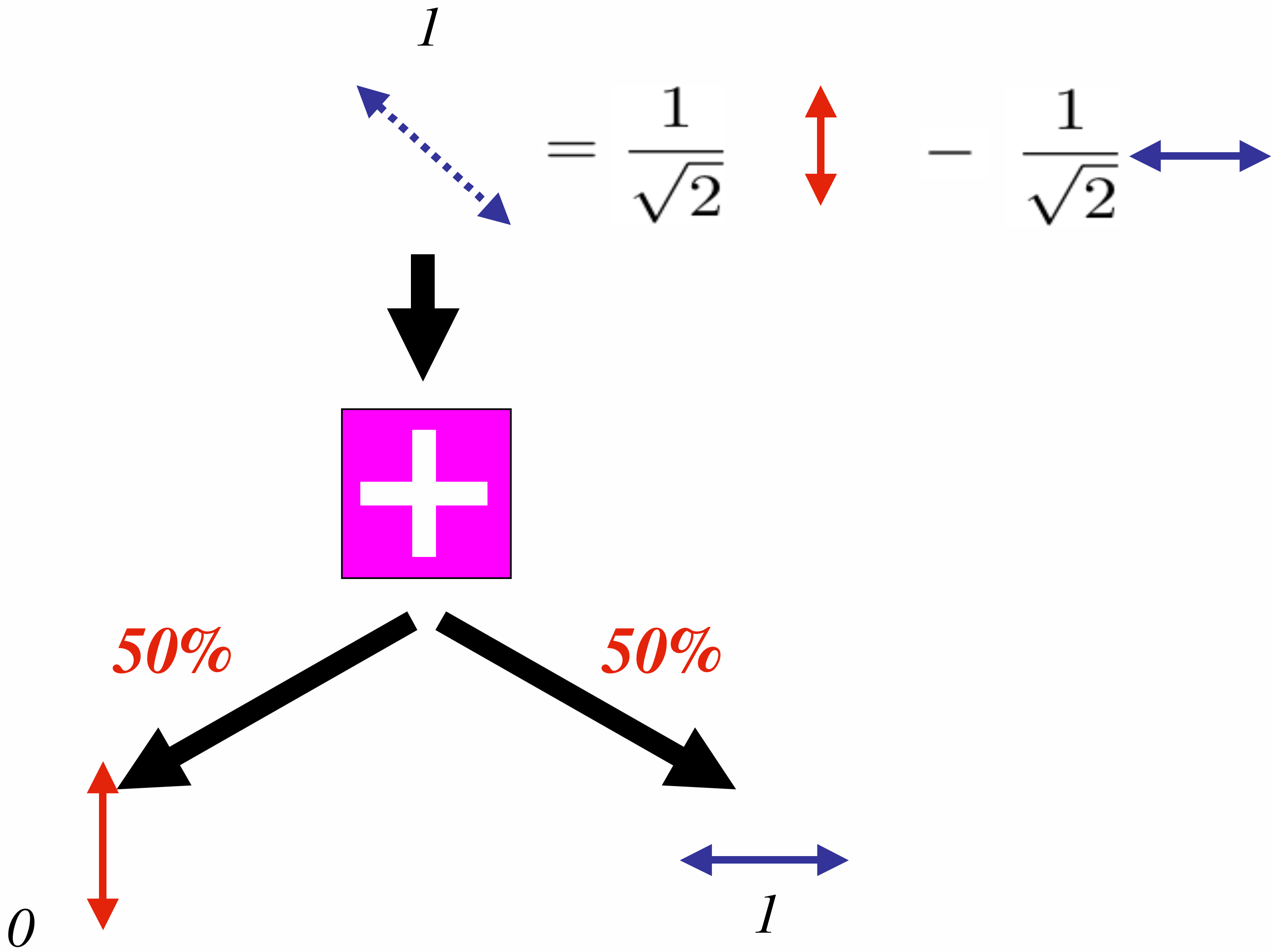
Measurement in the same basis ***does not change*** *the state.*

Measurement in a different basis....

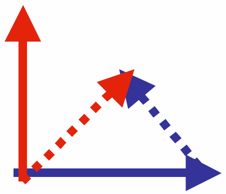


Measurement in a different basis....



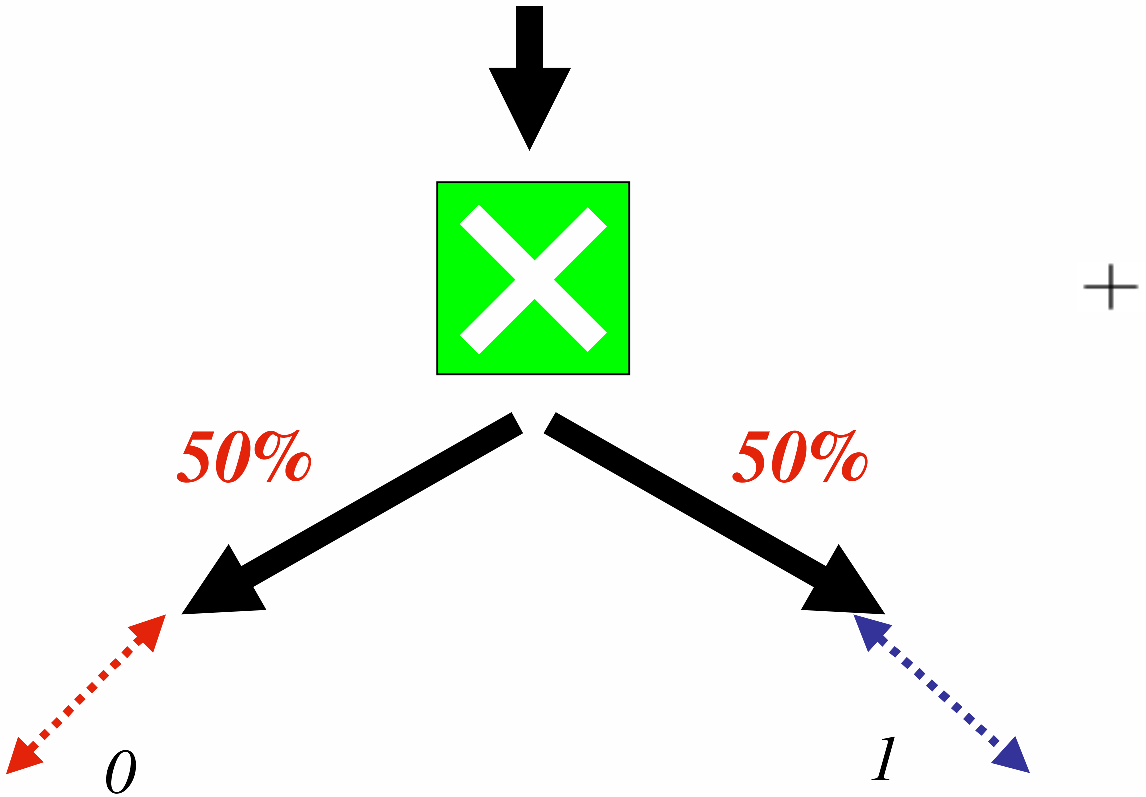


Measurement in a different basis....

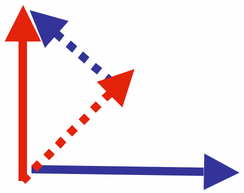


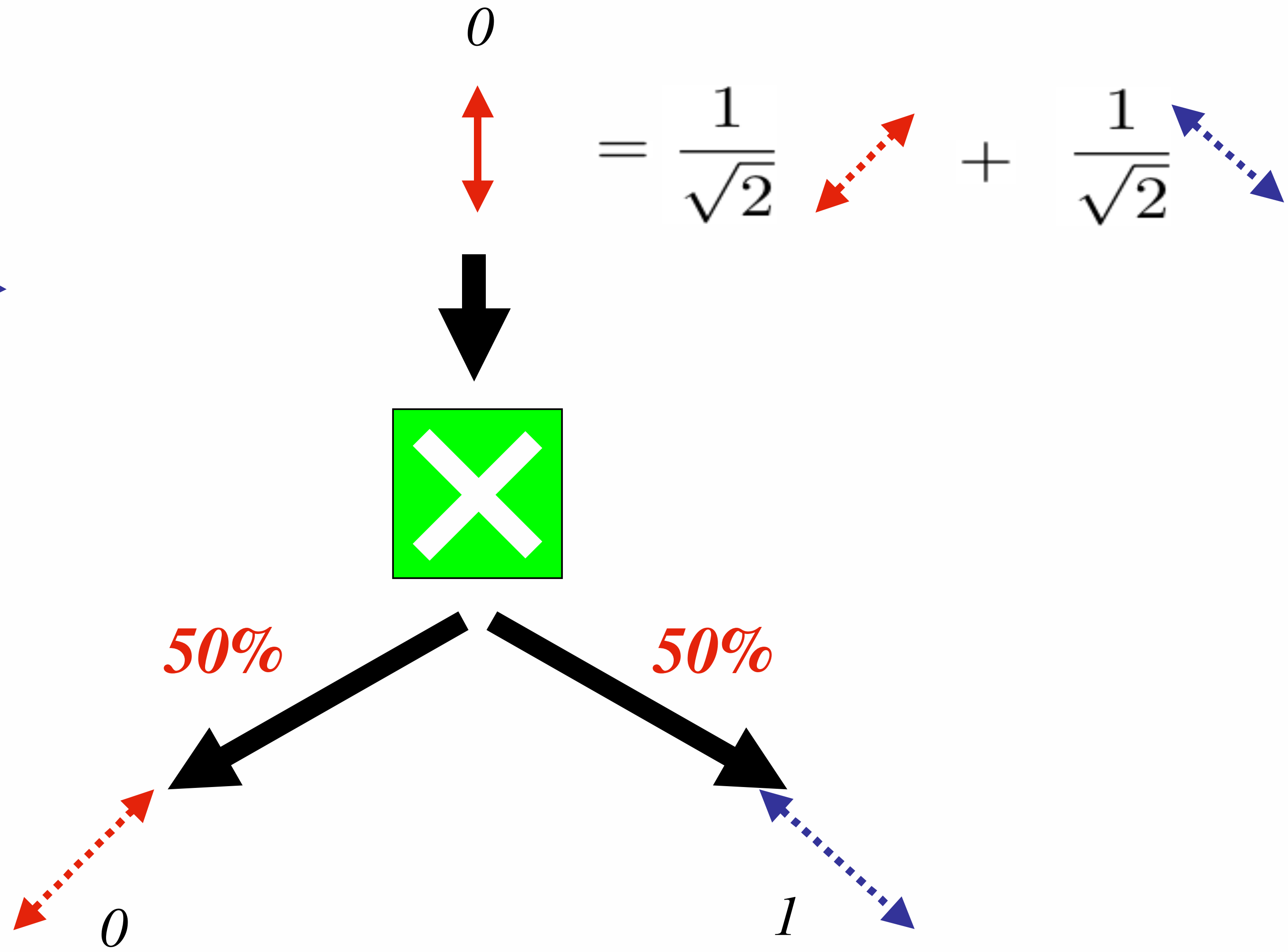
1

$$\leftrightarrow \;=\; \frac{1}{\sqrt{2}} \swarrow\!\!\!\nearrow \;-\; \frac{1}{\sqrt{2}} \nwarrow\!\!\!\searrow$$



Measurement in a different basis....





Two funny quantum effects

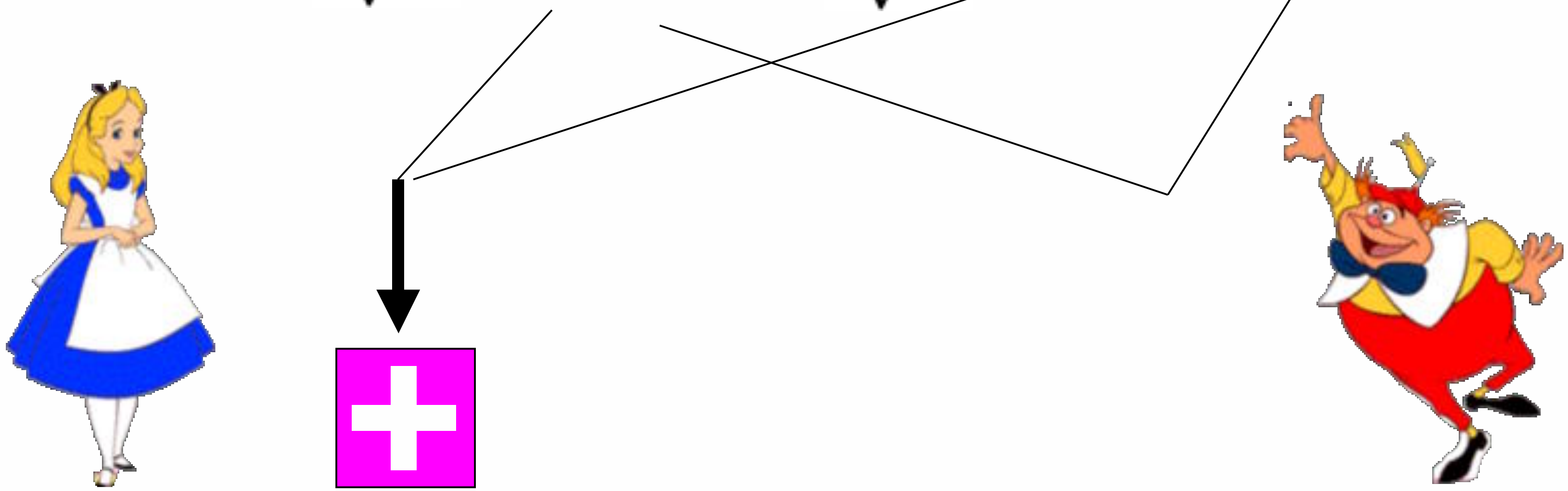
- Interference (see WTH ‘05)
- Entanglement

Entanglement

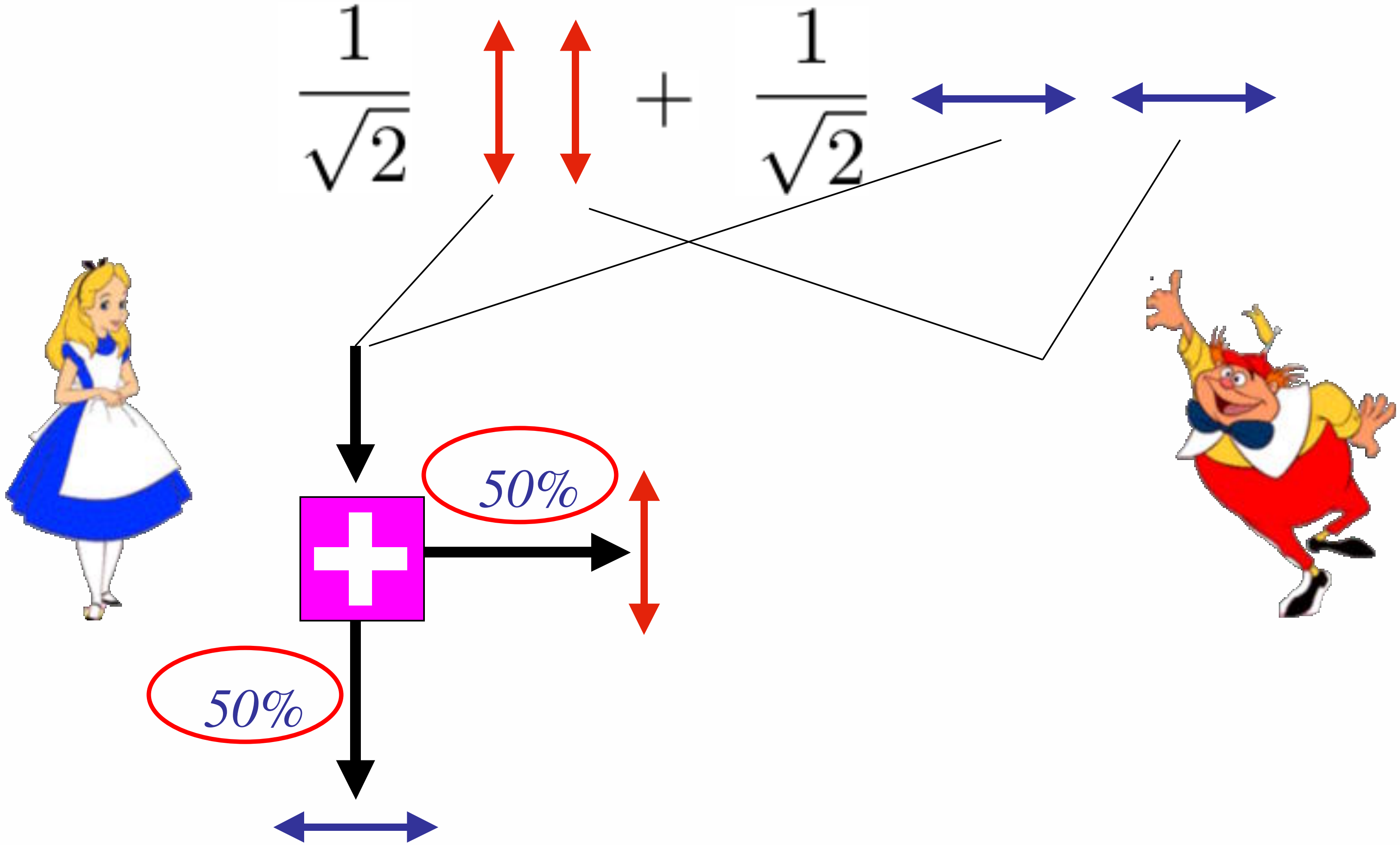
$$\frac{1}{\sqrt{2}} \updownarrow\updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow\leftrightarrow$$

Entanglement

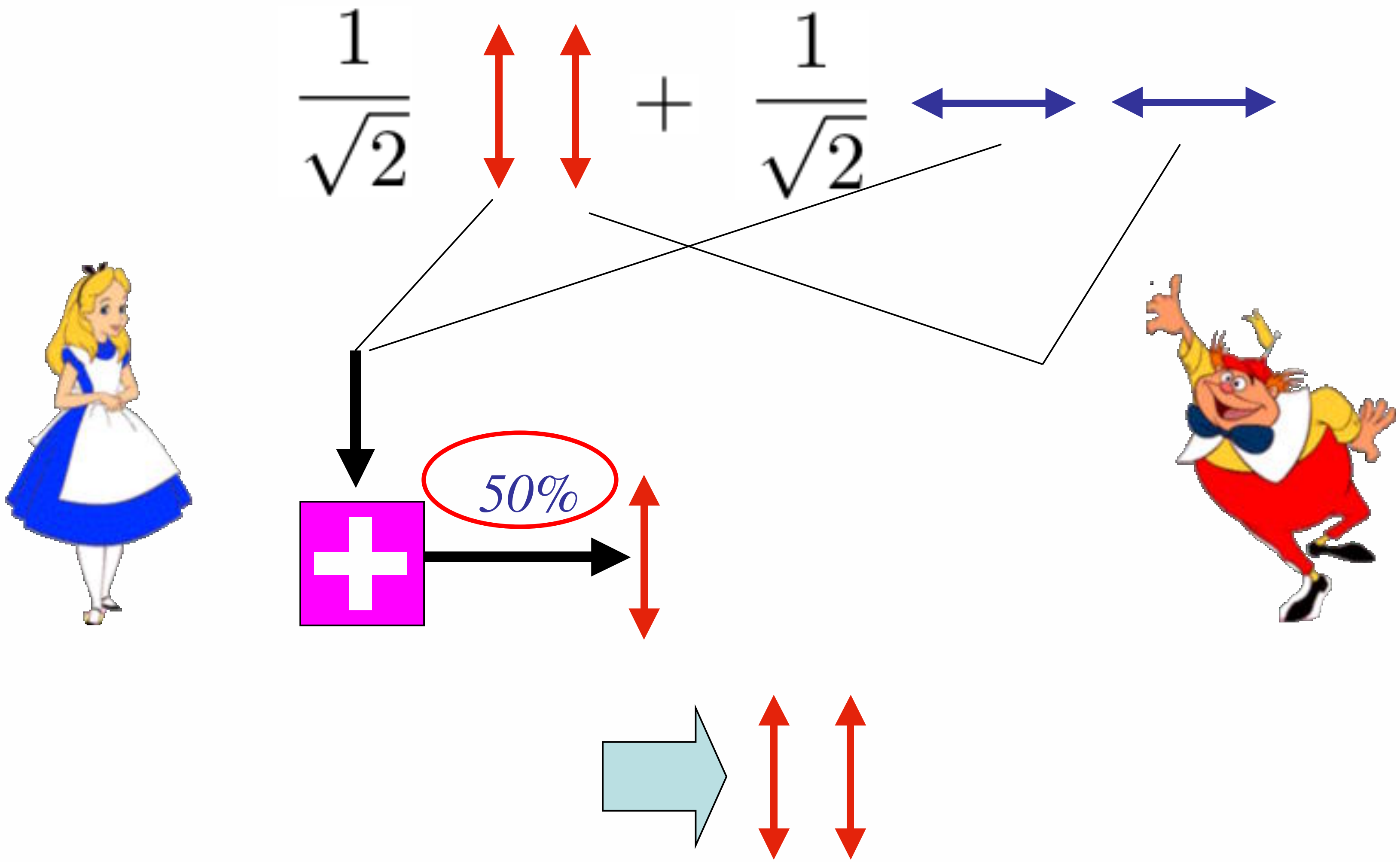
$$\frac{1}{\sqrt{2}} \updownarrow \updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow \leftrightarrow$$



Entanglement

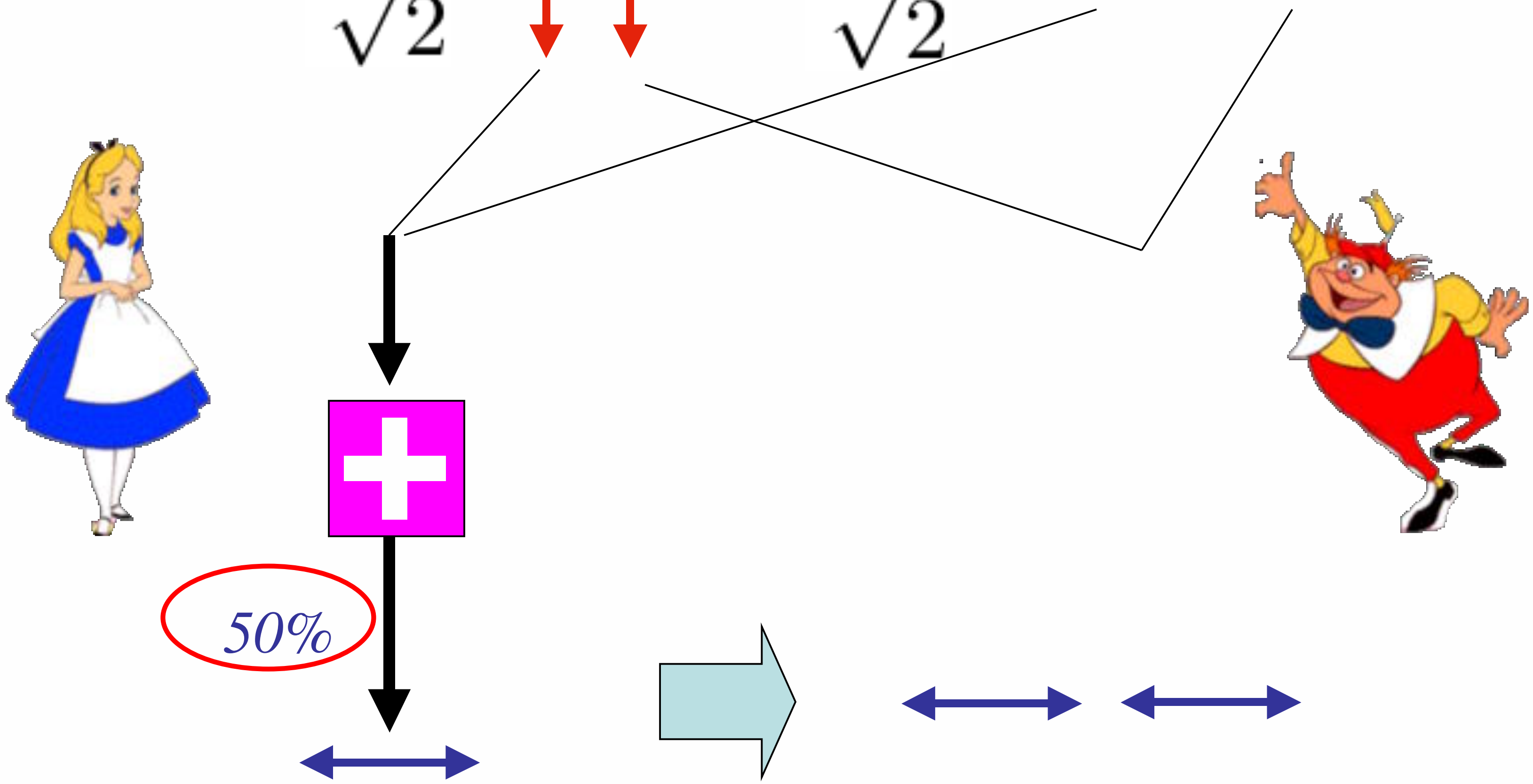


 Entanglement

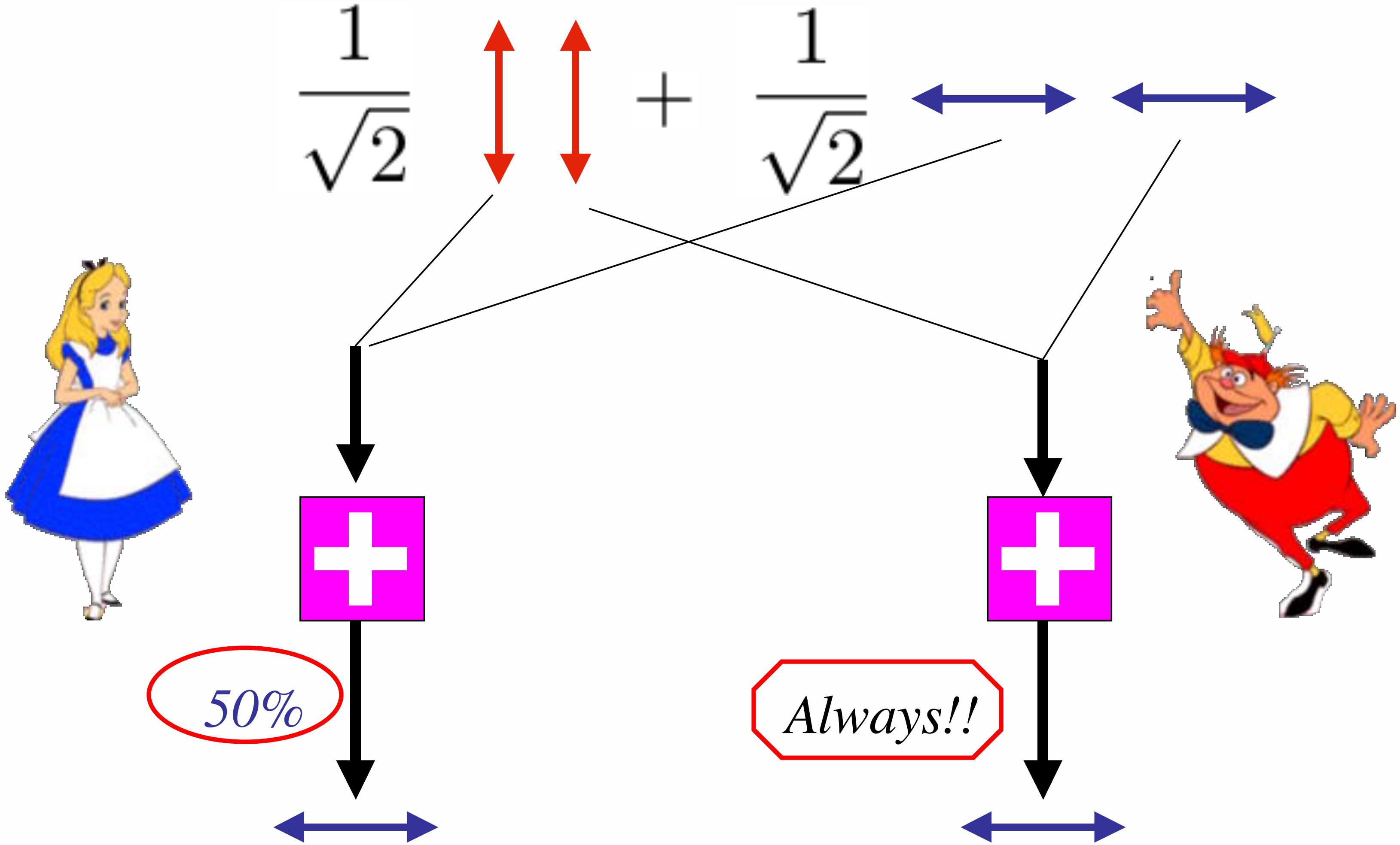


Entanglement

$$\frac{1}{\sqrt{2}} \updownarrow \updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow \leftrightarrow$$

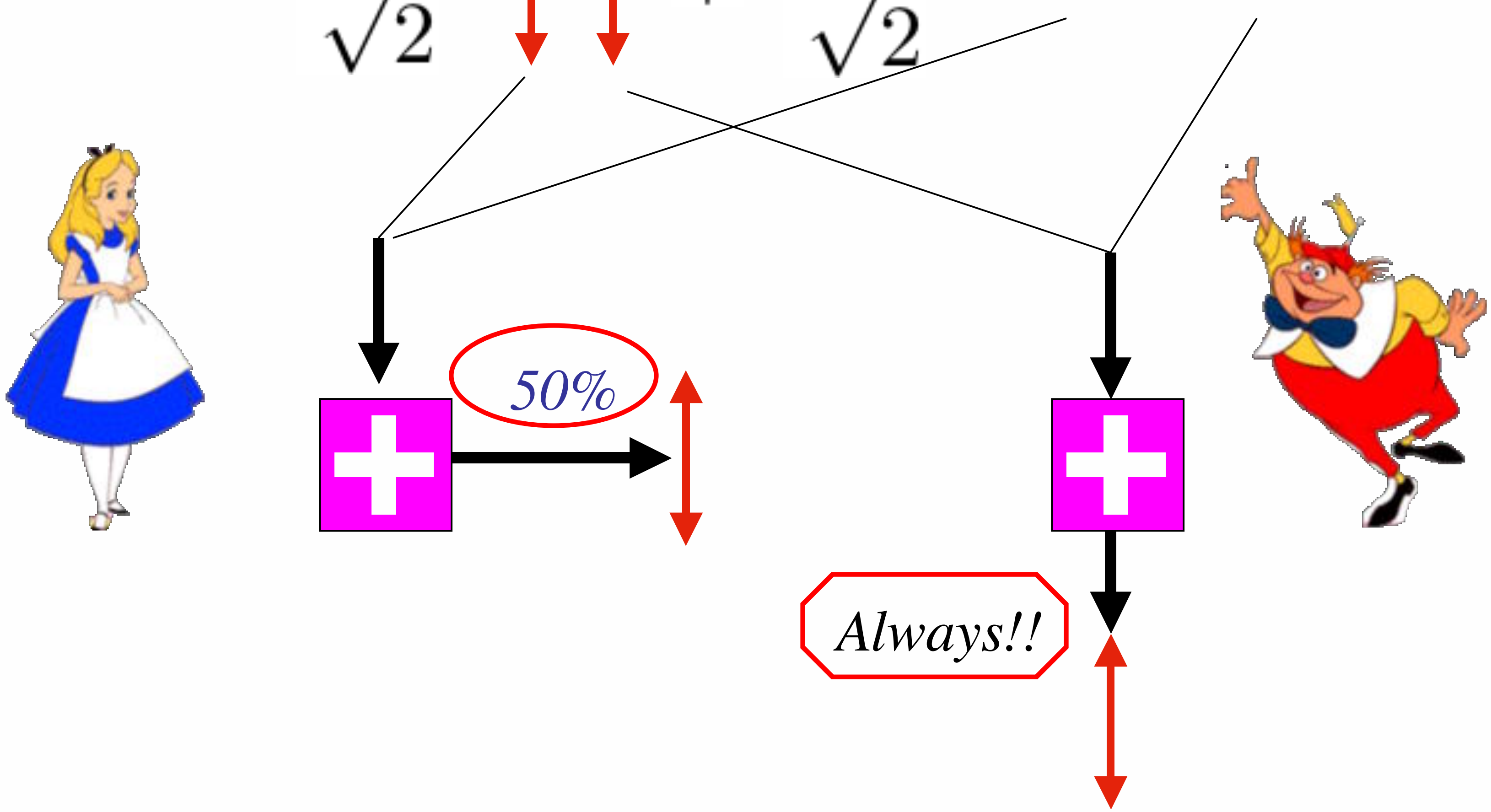


Perfect correlations



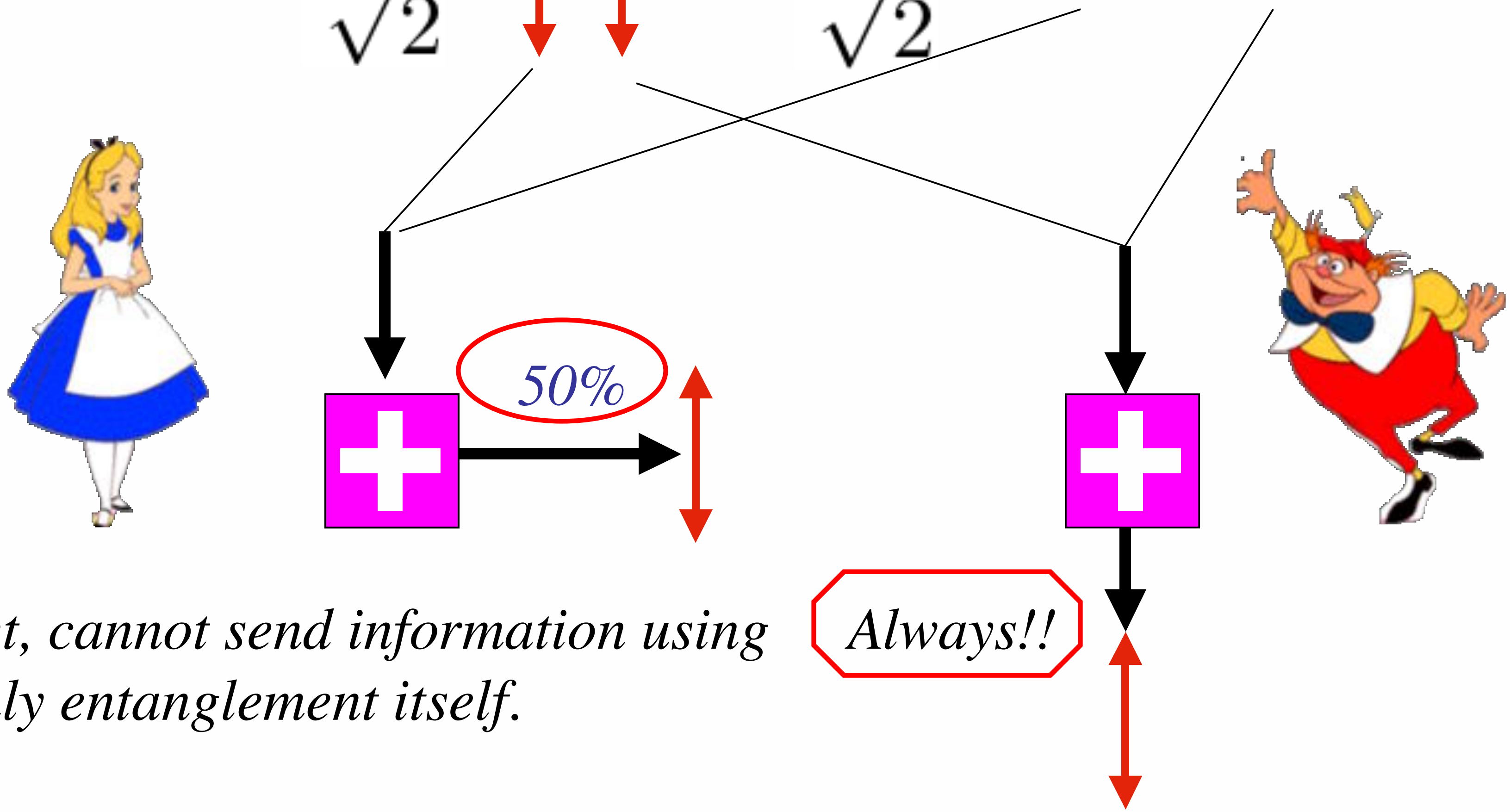
Perfect correlations

$$\frac{1}{\sqrt{2}}\,\updownarrow\,\updownarrow\;+\;\frac{1}{\sqrt{2}}\,\leftrightarrow\,\leftrightarrow$$



Perfect correlations

$$\frac{1}{\sqrt{2}} \updownarrow \updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow \leftrightarrow$$



Yet, cannot send information using only entanglement itself.

Let’s be more sceptical…
Perhaps there’s communication?

- Cannot communicate faster than light
- Measure immediately, no chance to communicate

Earth

Mars

Let's be more sceptical…
Perhaps there's communication?

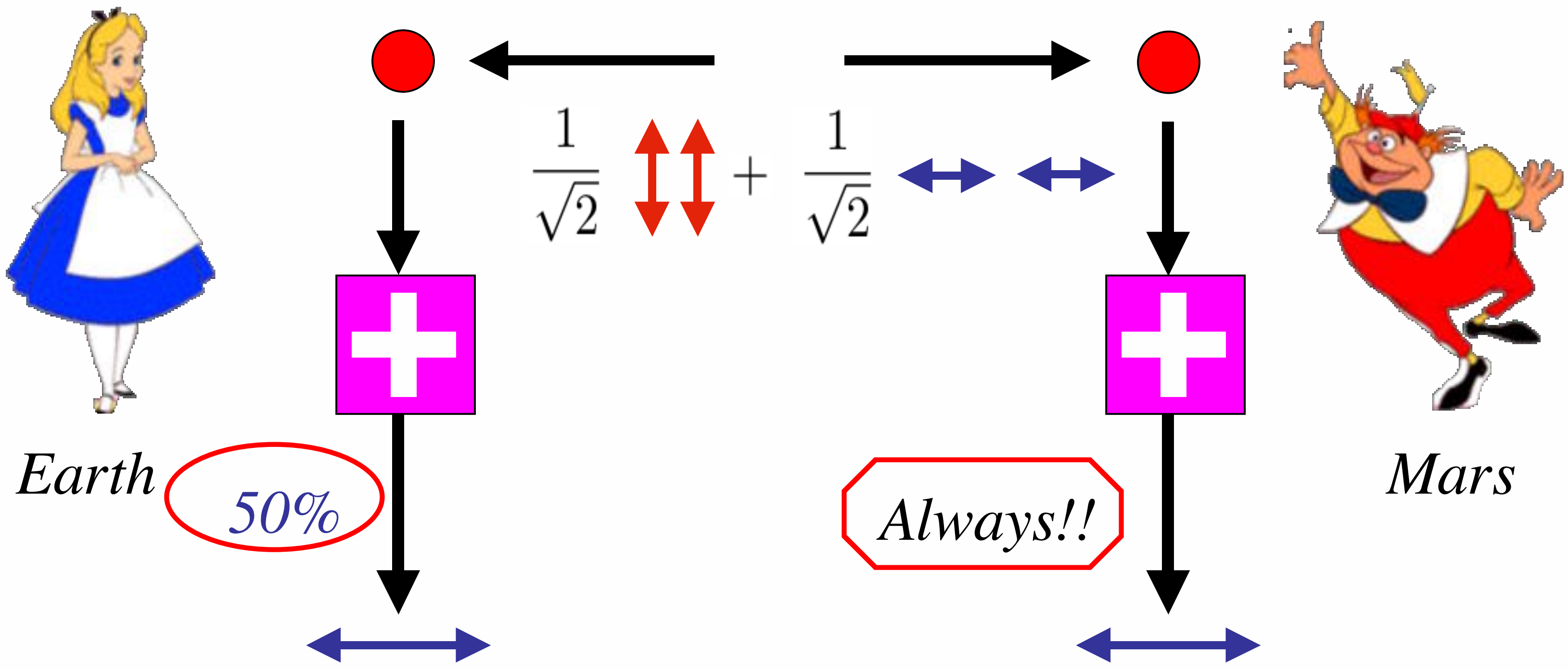
- Cannot communicate faster than light
- Measure immediately, no chance to communicate

$$\frac{1}{\sqrt{2}} \updownarrow\updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow\leftrightarrow$$

Earth *Mars*

Let's be more sceptical…
Perhaps there's communication?

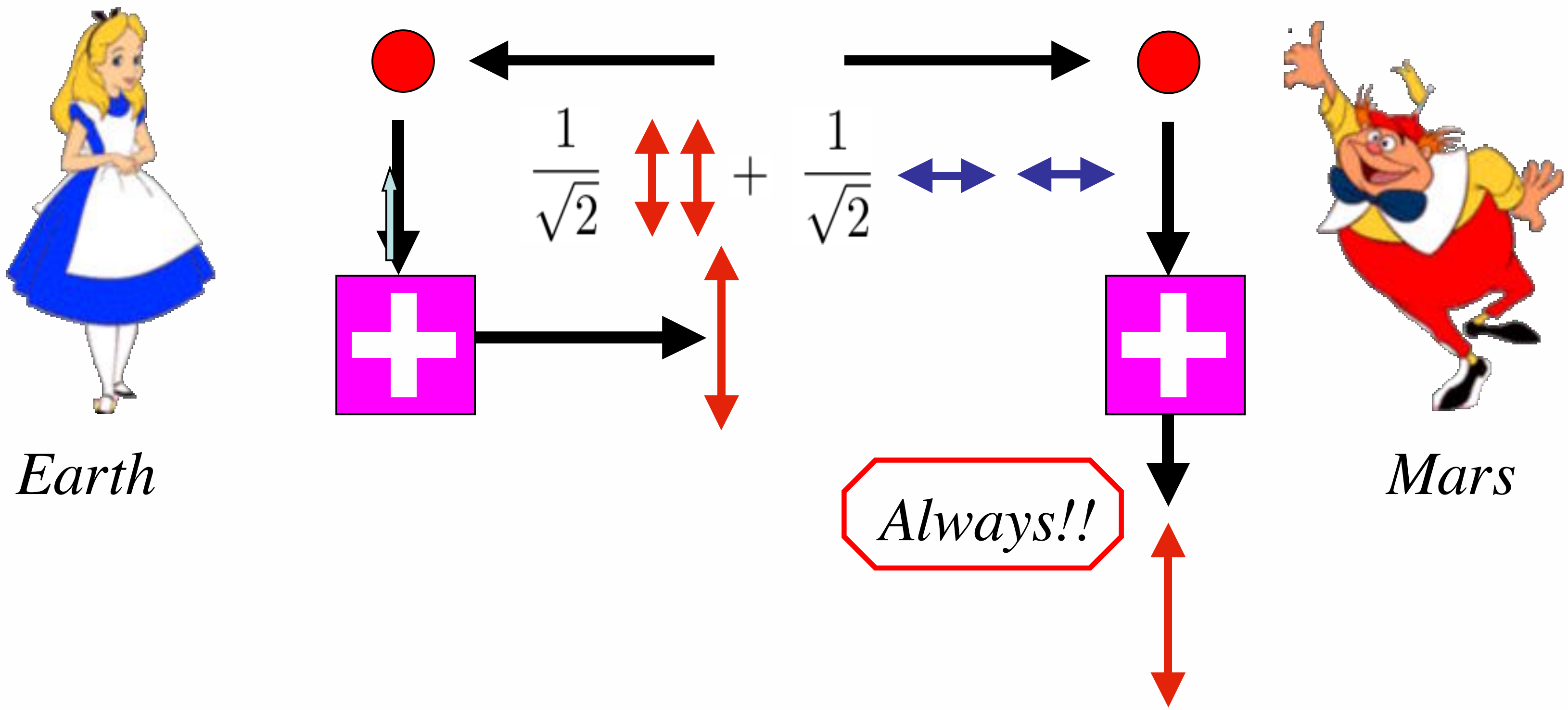
- Cannot communicate faster than light
- Measure immediately, no chance to communicate



Let’s be more sceptical…

Works even without communication

- Cannot communicate faster than light
- Measure immediately, no chance to communicate



Let’s be more sceptical…

What does that mean, “there’s a 50% chance of obtaining an outcome?”

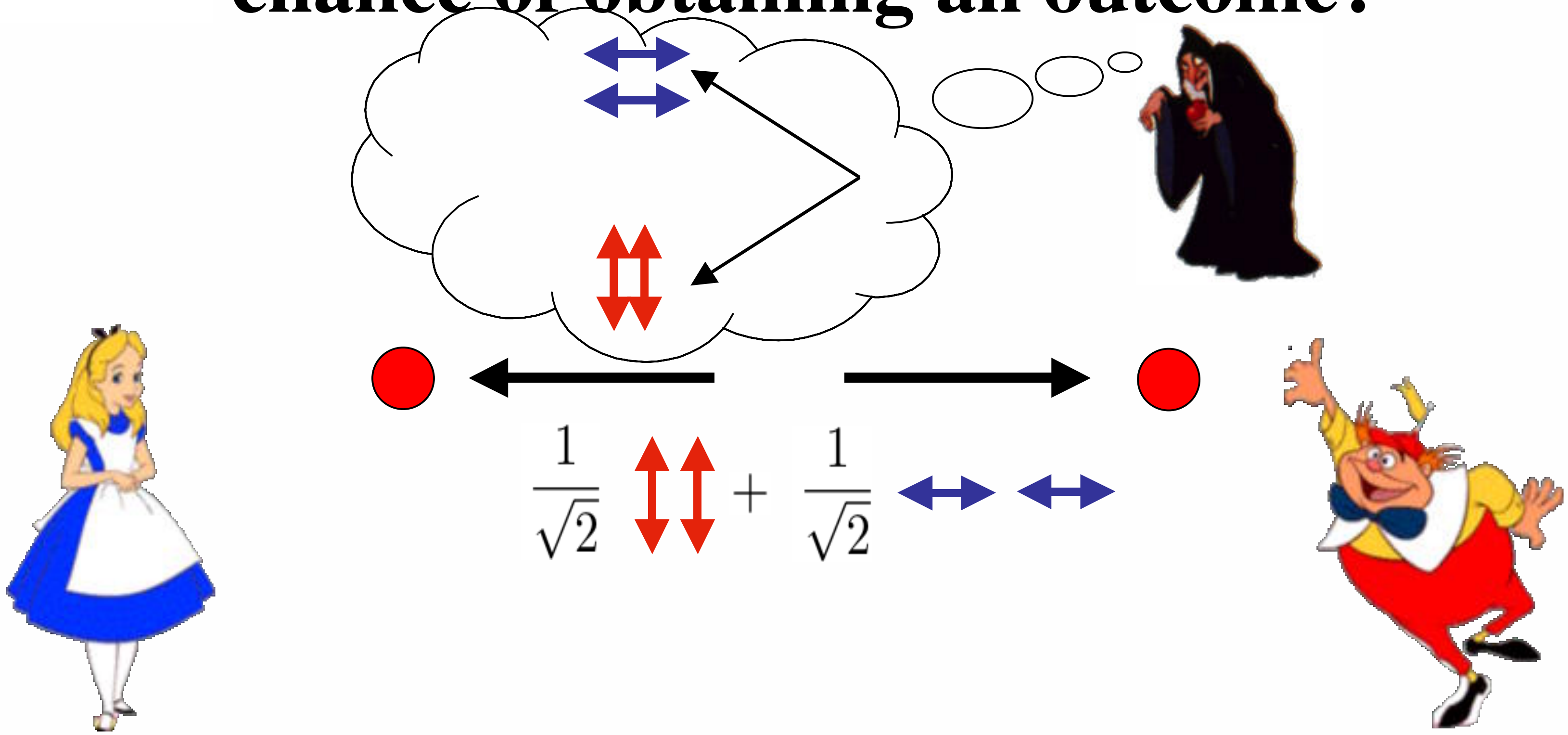
$$\frac{1}{\sqrt{2}} \updownarrow\updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow\leftrightarrow$$

??

Earth *Mars*

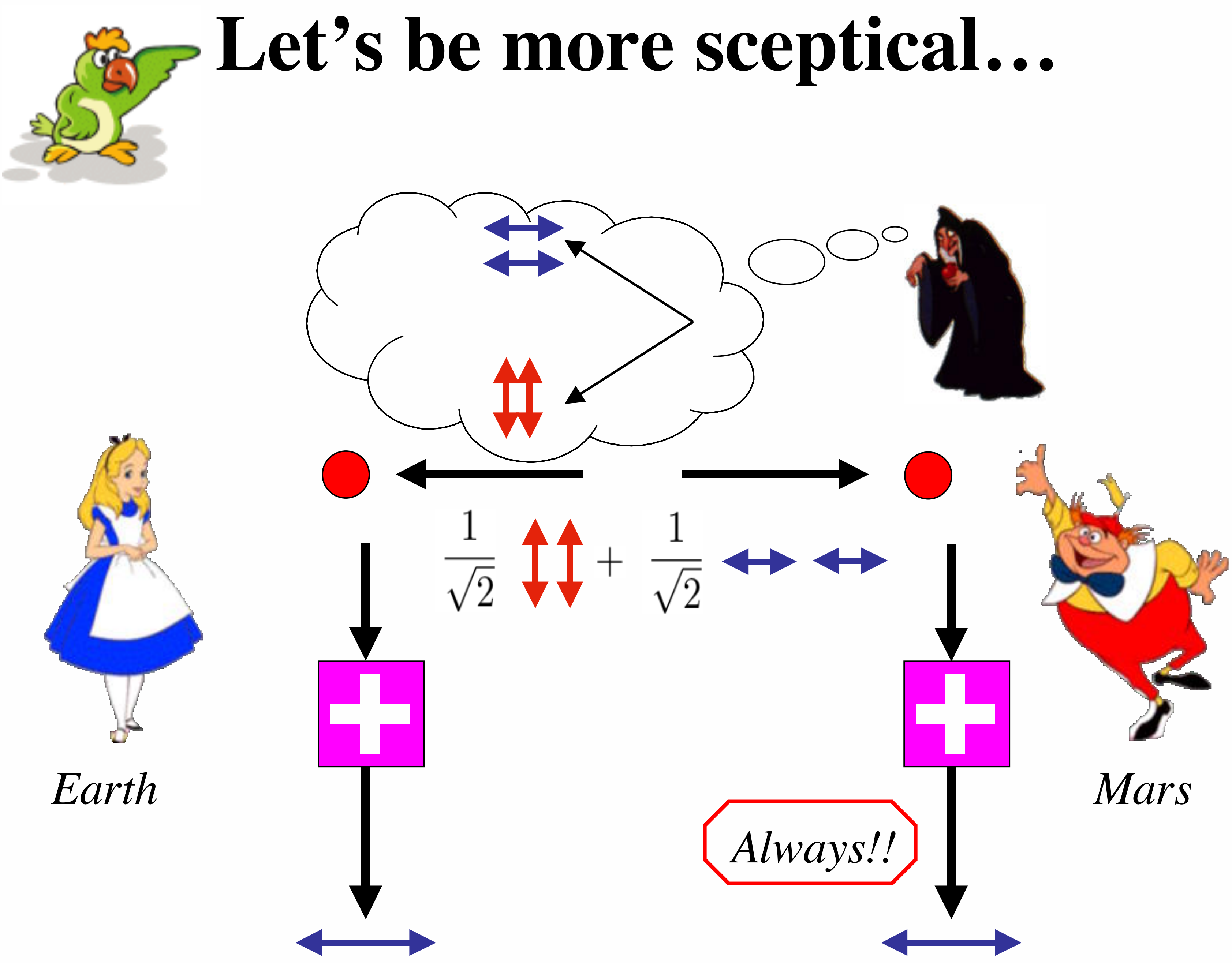
Let's be more sceptical…

What does that mean, "there's a 50% chance of obtaining an outcome?"

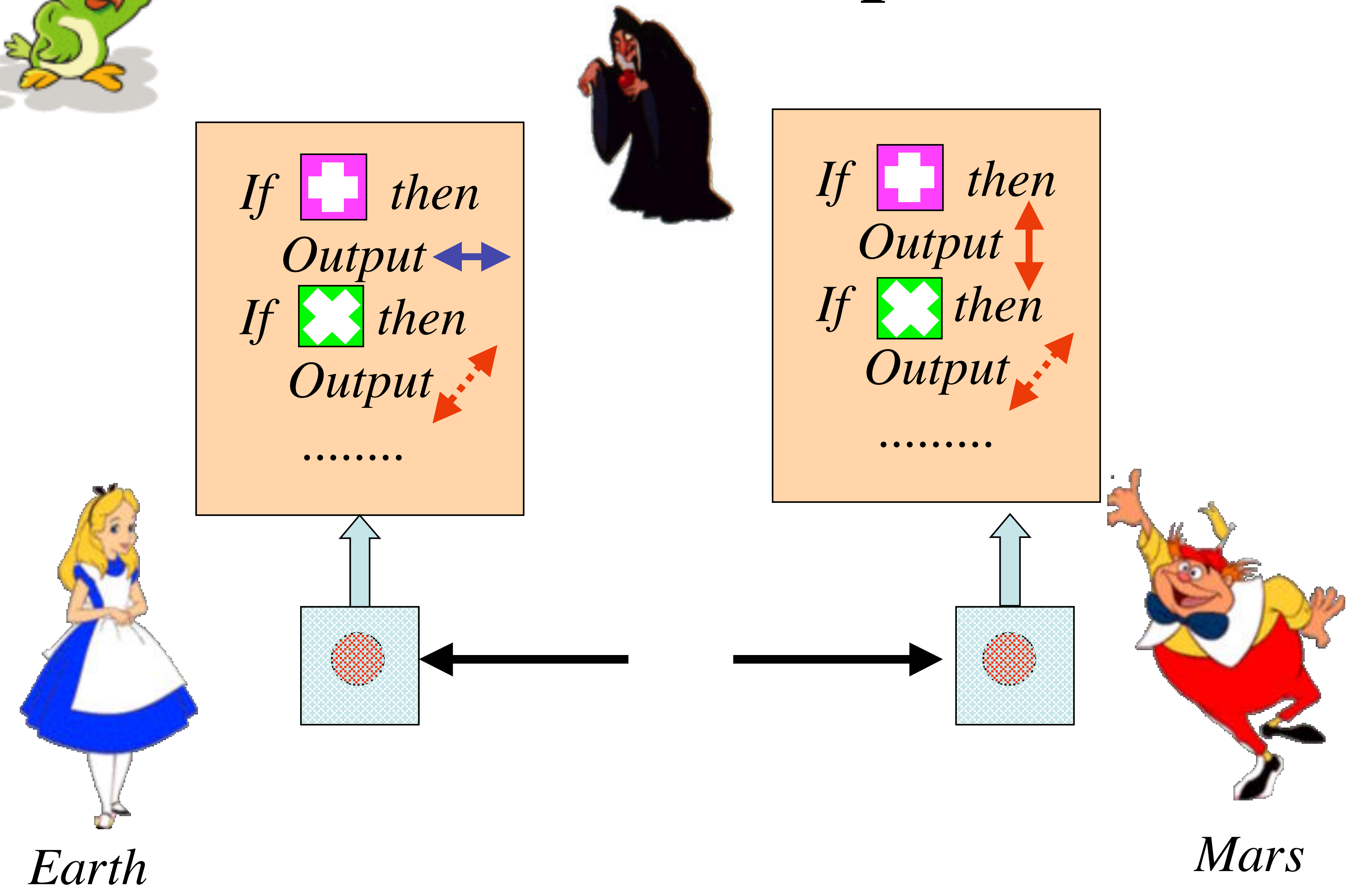


Earth *Mars*

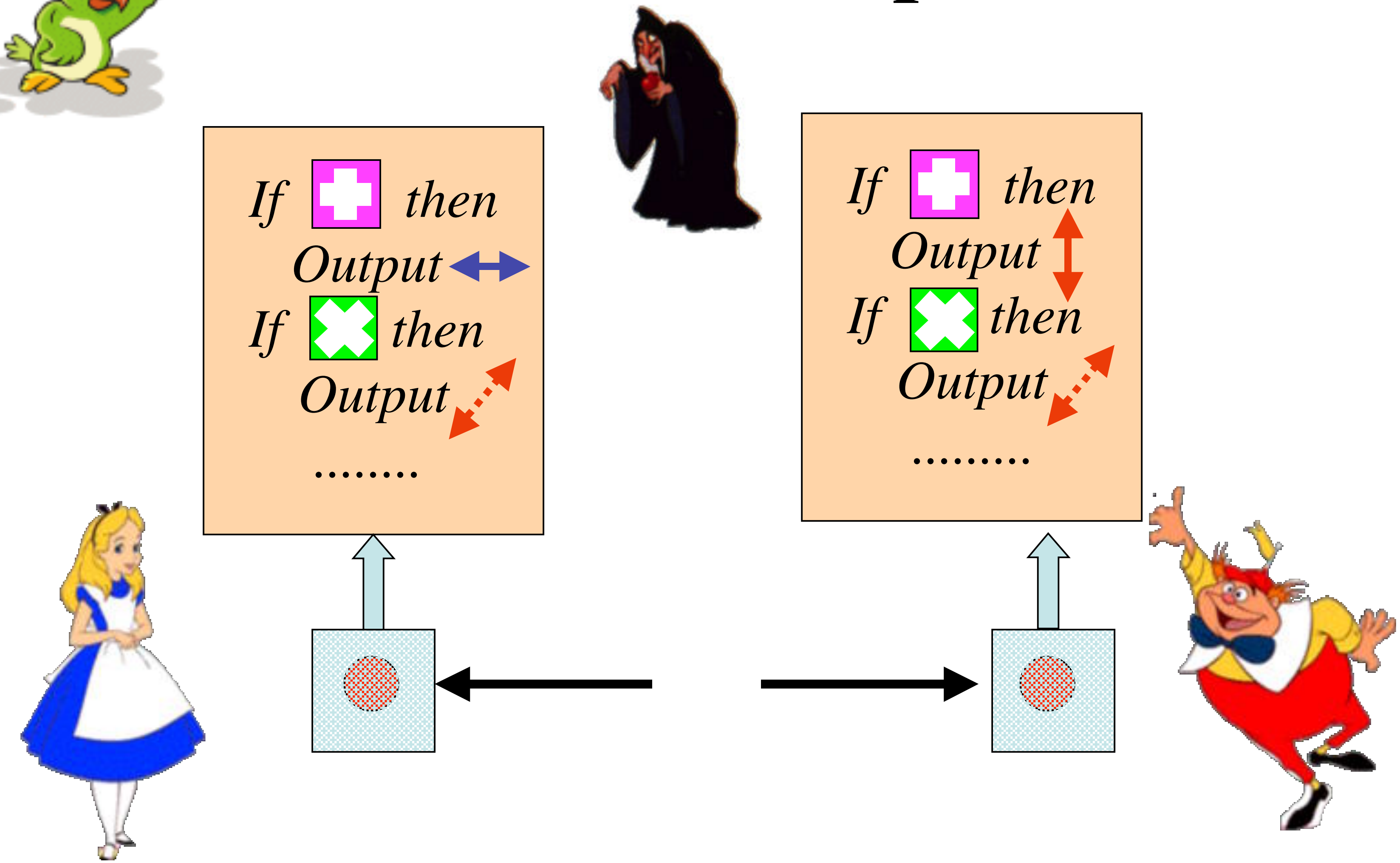
Let's be more sceptical…



Let’s be more sceptical…



Let’s be more sceptical…



Not a big deal then…. But how can we be sure this is how it works?

Let’s play a game of Q & A

- *Measurement settings are the questions:*

  0

  1

- *Outcomes are the answers:*

  0

  1

- *Instructions are the strategies of a player:*

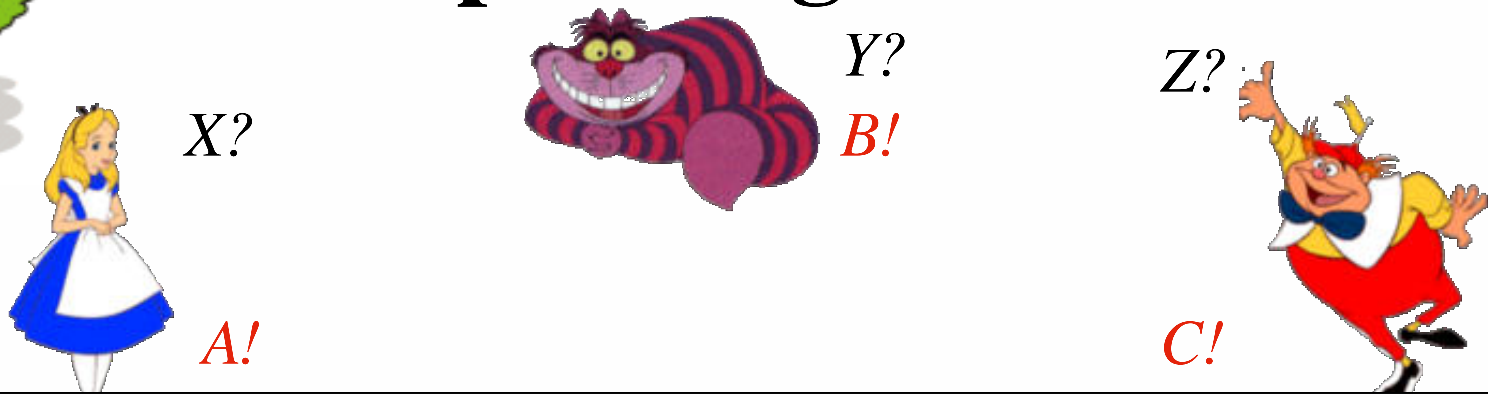
If then
Output
If then
Output

If then
Output
If then
Output

Let’s play a game of Q & A

- Some rules:
  - We tell the players clearly what game we wish to play.
  - Before we start the game, players can communicate and decide on a strategy. This determines their “cheat sheet”.
  - Once the game has started, they are no longer allowed to communicate.

A three person game



- *Questions: X Y and Z. Always X + Y + Z mod 2 = 0.*

- *GHZ game (Greenberger, Horne, Zeilinger)*

A three person game

$X?$

$A!$

$Y?$

$B!$

$Z?$

$C!$

- *Questions: X Y and Z. Always $X + Y + Z \bmod 2 = 0$.*
- *Players win iff X or Y or $Z = A + B + C \bmod 2$*
- *GHZ game (Greenberger, Horne, Zeilinger)*

A three person game

X?

A!

Y?

B!

Z?

C!

- *Questions: X Y and Z. Always* $X + Y + Z \bmod 2 = 0$.
- *Players win iff X or Y or Z* $= A + B + C \bmod 2$

- *If communication is possible, players can easily win.*

- *GHZ game (Greenberger, Horne, Zeilinger)*

A three person game

Y?

B!

Z?

X?

A!

C!

- *Questions: X Y and Z. Always X + Y + Z mod 2 = 0.*
- *Players win iff X or Y or Z = A + B + C mod 2*

- *If communication is possible, players can easily win.*
- *Put players in far away places again, so they have "no time to communicate before we expect answers.*

- *GHZ game (Greenberger, Horne, Zeilinger)*

A three person game

X?

A!

Y?

B!

Z?

C!

- *Questions: X Y and Z. Always X + Y + Z mod 2 = 0.*
- *Players win iff X or Y or Z = A + B + C mod 2*

X Y Z	A + B + C mod 2	
000	0: 000,011,101,110	
011	1: 001,010,100,111	
101	1:	
110	1:	

- *GHZ game (Greenberger, Horne, Zeilinger)*

A three person game

X?

A = X !

Y?

B = not Y!

Z?

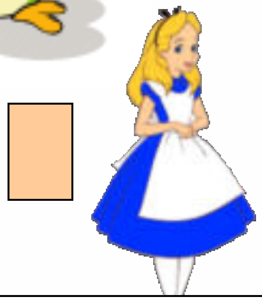
C = 1!

- *Questions: X Y and Z. Always X + Y + Z mod 2 = 0.*
- *Players win iff X or Y or Z = A + B + C mod 2*

X Y Z	A + B + C mod 2	One strategy:
000	0: 000,011,101,110	011 - Win!
011	1: 001,010,100,111	001 - Win!
101	1:	111 - Win!
110	1:	101 - Loose...

- *GHZ game (Greenberger, Horne, Zeilinger)*

Suppose qubits were like boxes



X?

A !

Y?

B !

Z?

C!

- *Questions: X Y and Z. Always* $X + Y + Z \bmod 2 = 0$.
- *Players win iff* X *or* Y *or* $Z = A + B + C \bmod 2$

- *It's impossible to win all the time with a classical strategy:*

$$A(0) + B(0) + C(0) = 0$$
$$A(0) + B(1) + C(1) = 1$$
$$A(1) + B(0) + C(1) = 1$$
$$A(1) + B(1) + C(0) = 1$$

sum all four mod 2: $0 = 1!$

- *GHZ game (Greenberger, Horne, Zeilinger)*

Quantumly, things are a little different….

X?

A !

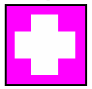
Y?

B !

Z?

C!

- *Questions: X Y and Z. Always X + Y + Z mod 2 = 0.*
- *Players win iff X or Y or Z = A + B + C mod 2*

- *But with quantum entanglement, the players can win all the time!*
    - *Start out with entangled state*
    - *Just measure with*  *for 0 and*  *for 1*
    - *Take measurement outcome as answer.*

- *GHZ game (Greenberger, Horne, Zeilinger)*

But if quantum entanglement allows the player to win always

- Qubits are not like boxes with a predetermined instruction sheet (aka hidden variables).
  - Communication was not possible.
  - Neither does entanglement allow us to transfer information by itself.
  - Yet, the players can always win...

Other “games”

- Bell/CHSH ‘game’
- Mermin’s Magic Square (described in an easy way by Aravind)
- ……

Great, so why bother?

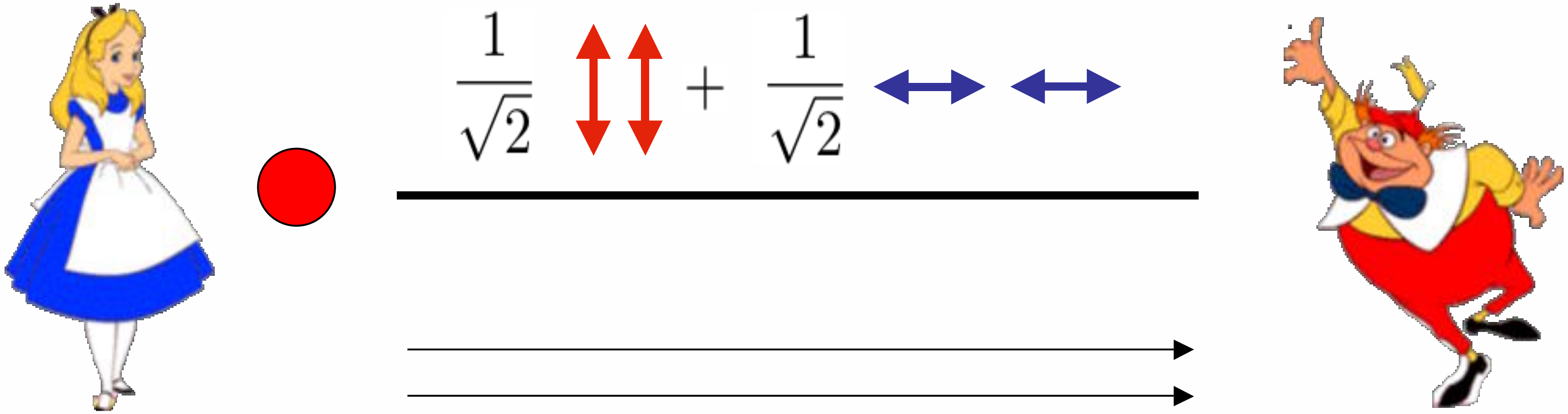
- Quantum entanglement can make things possible which are classically only possible with communication. (such as playing the GHZ game)
- Plays an important role in quantum algorithms:
  - Speedup such as in factoring depends crucially on entanglement! (Linden, Josza)
- Quantum Teleportation
- Plays an important role in quantum cryptography.

Quantum Teleportation

$$\frac{1}{\sqrt{2}}\updownarrow\updownarrow + \frac{1}{\sqrt{2}}\leftrightarrow\leftrightarrow$$

- *Send an arbitrary quantum bit using*
  - *One EPR pair*
  - *2 bits of classical communication*

Quantum Teleportation



$$\frac{1}{\sqrt{2}} \updownarrow\updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow\leftrightarrow$$

- *Send an arbitrary quantum bit using*
  - *One EPR pair*
  - *2 bits of classical communication*

Quantum Teleportation

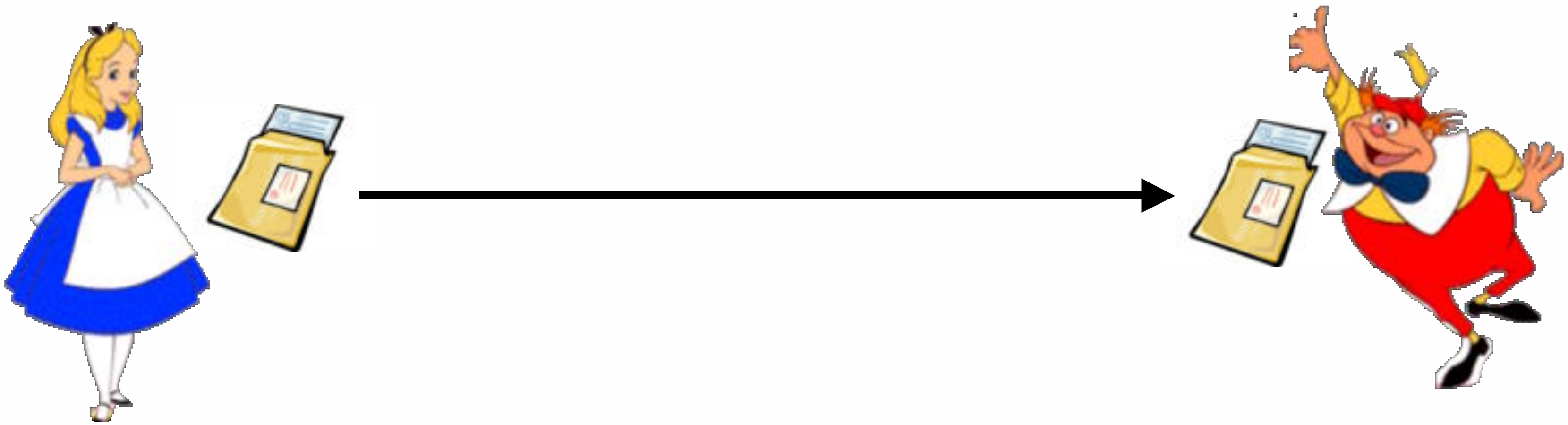
- *Send an arbitrary quantum bit using*
  - *One EPR pair*
  - *2 bits of classical communication*

Applications to cryptography

- Negative: If the security of a protocol depends on the fact that certain parties cannot communicate, the protocol may be compromised if the parties can share entanglement (e.g. In interactive proof systems)
- Positive: quantum key exchange
  - An entanglement view on quantum key exchange

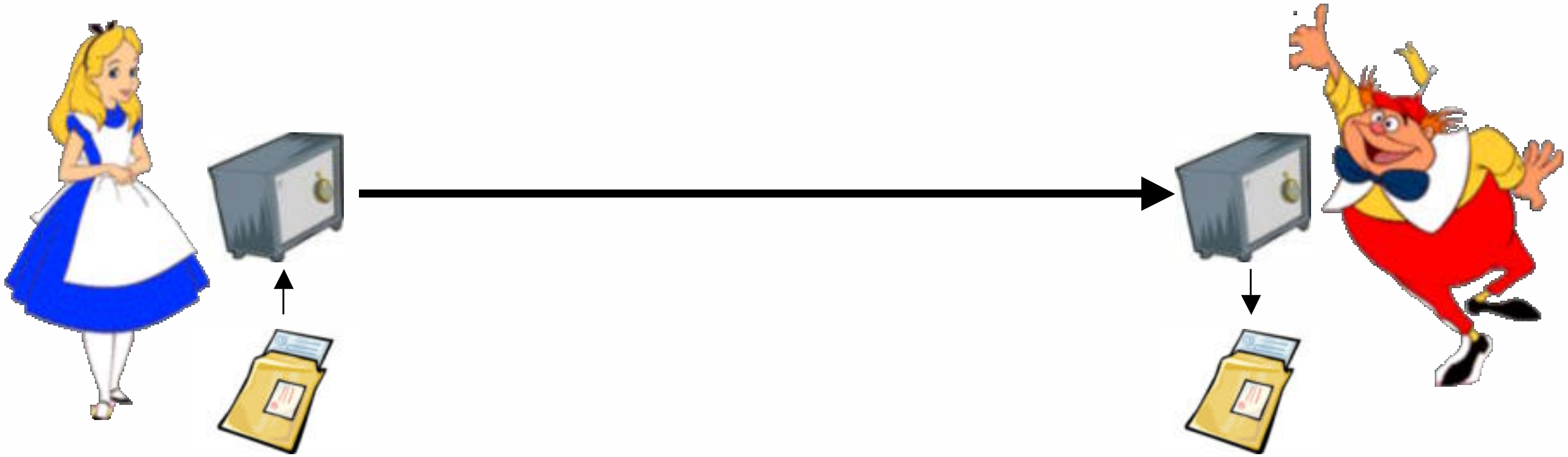
The Problem

The Problem



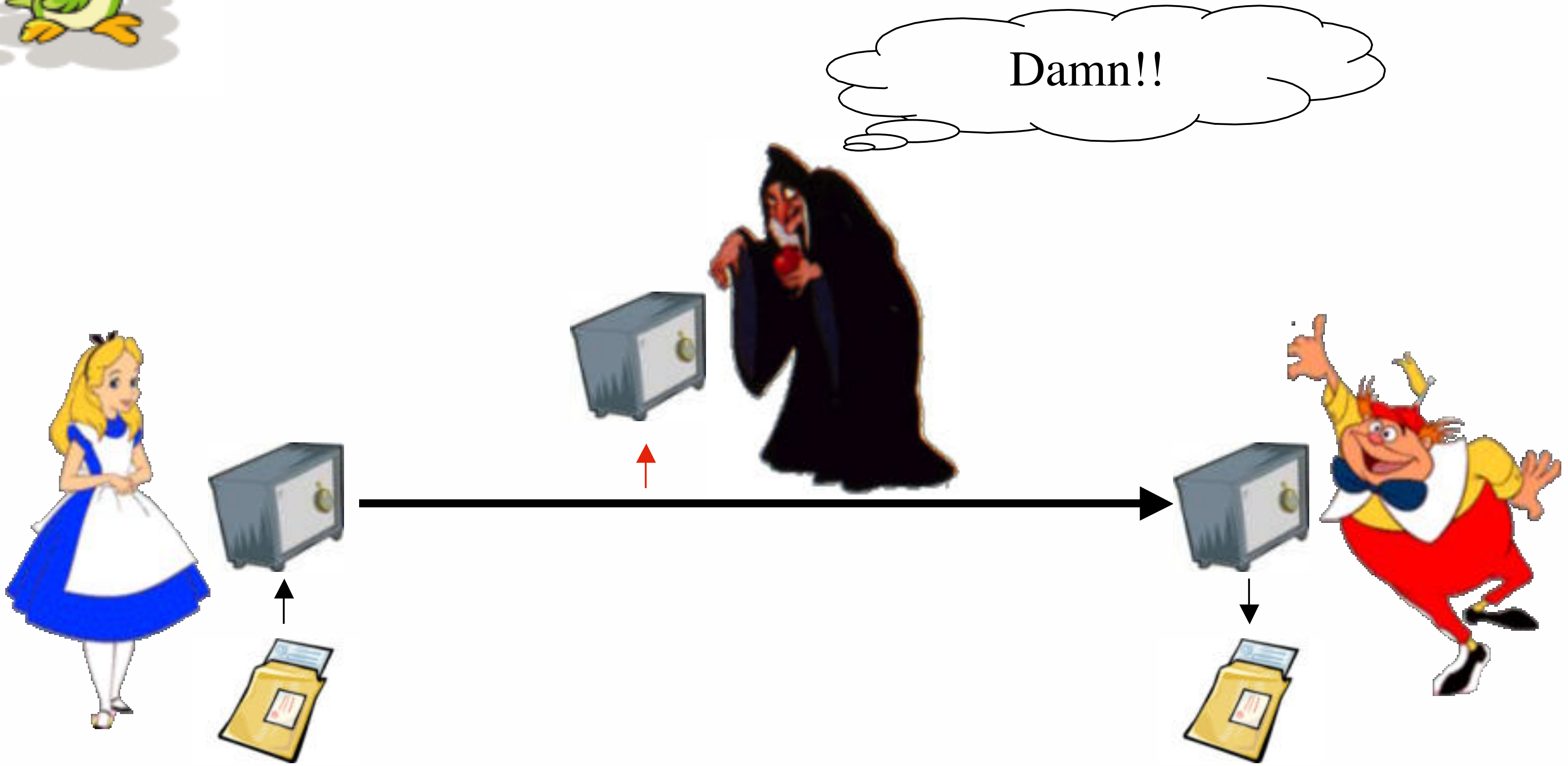
The Problem

Secure Communication



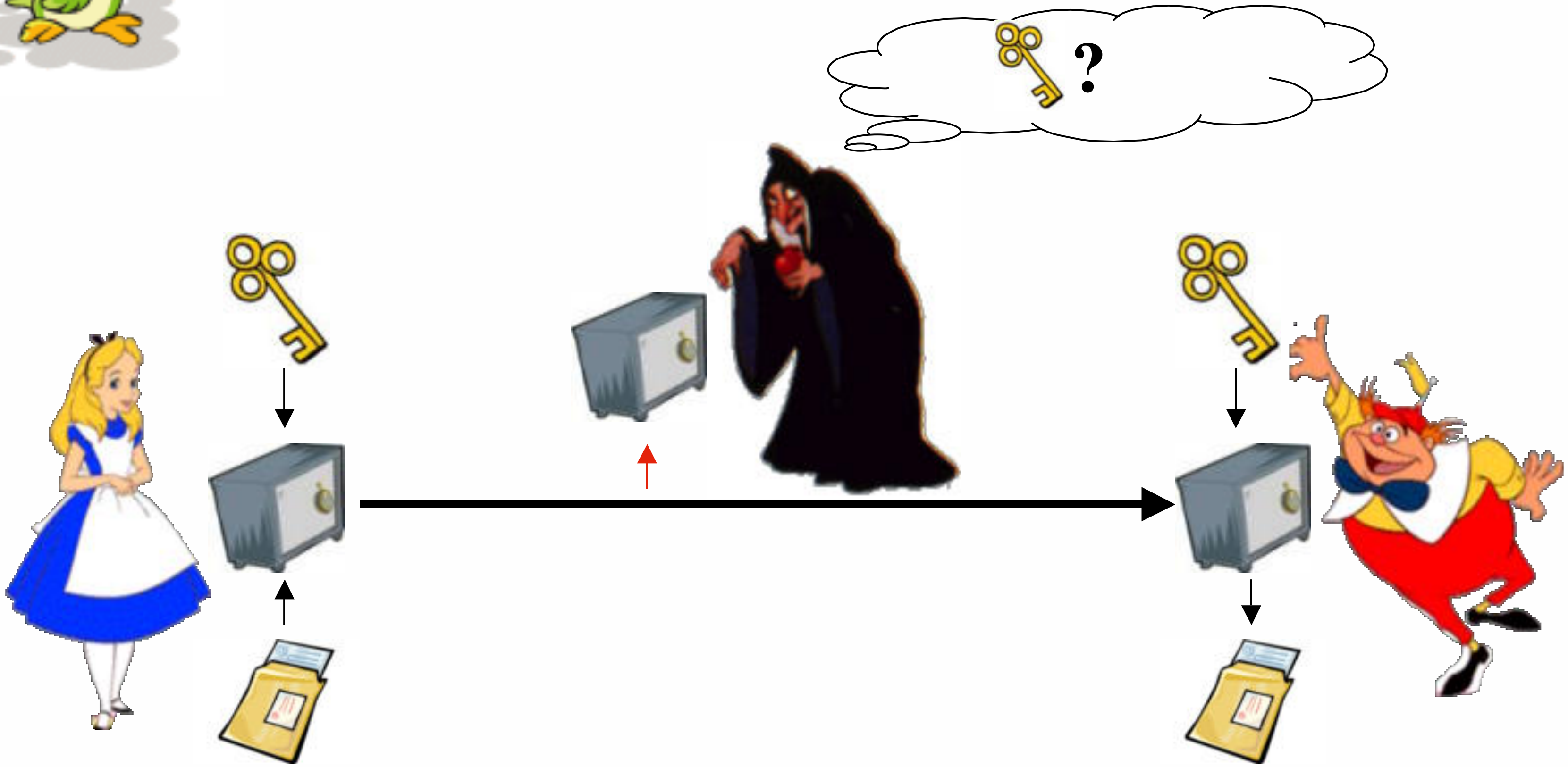
Goal: Hide the message contents from eavesdroppers!

Secure Communication



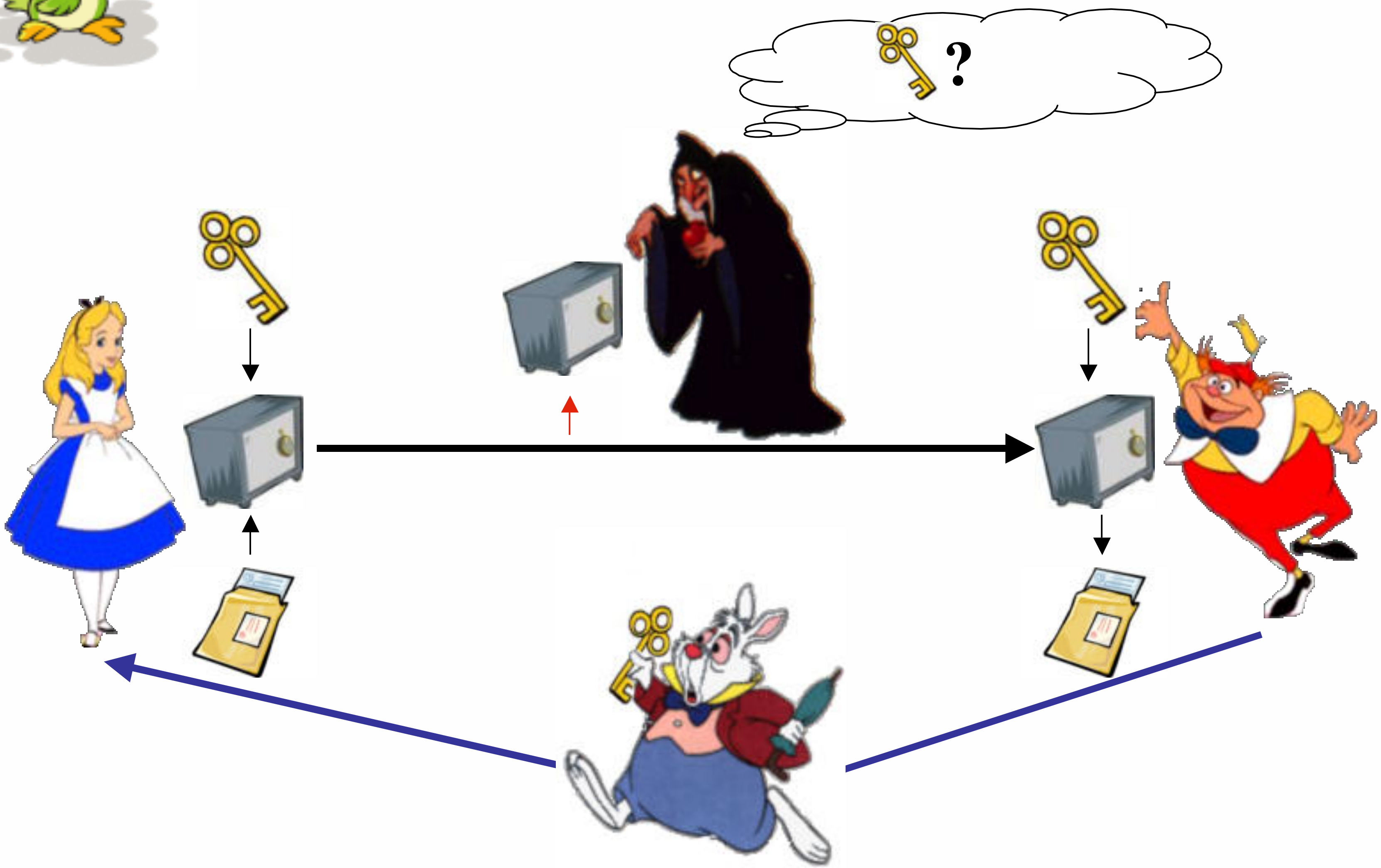
Goal: Hide the message contents from eavesdroppers!

Secret Key Cryptography



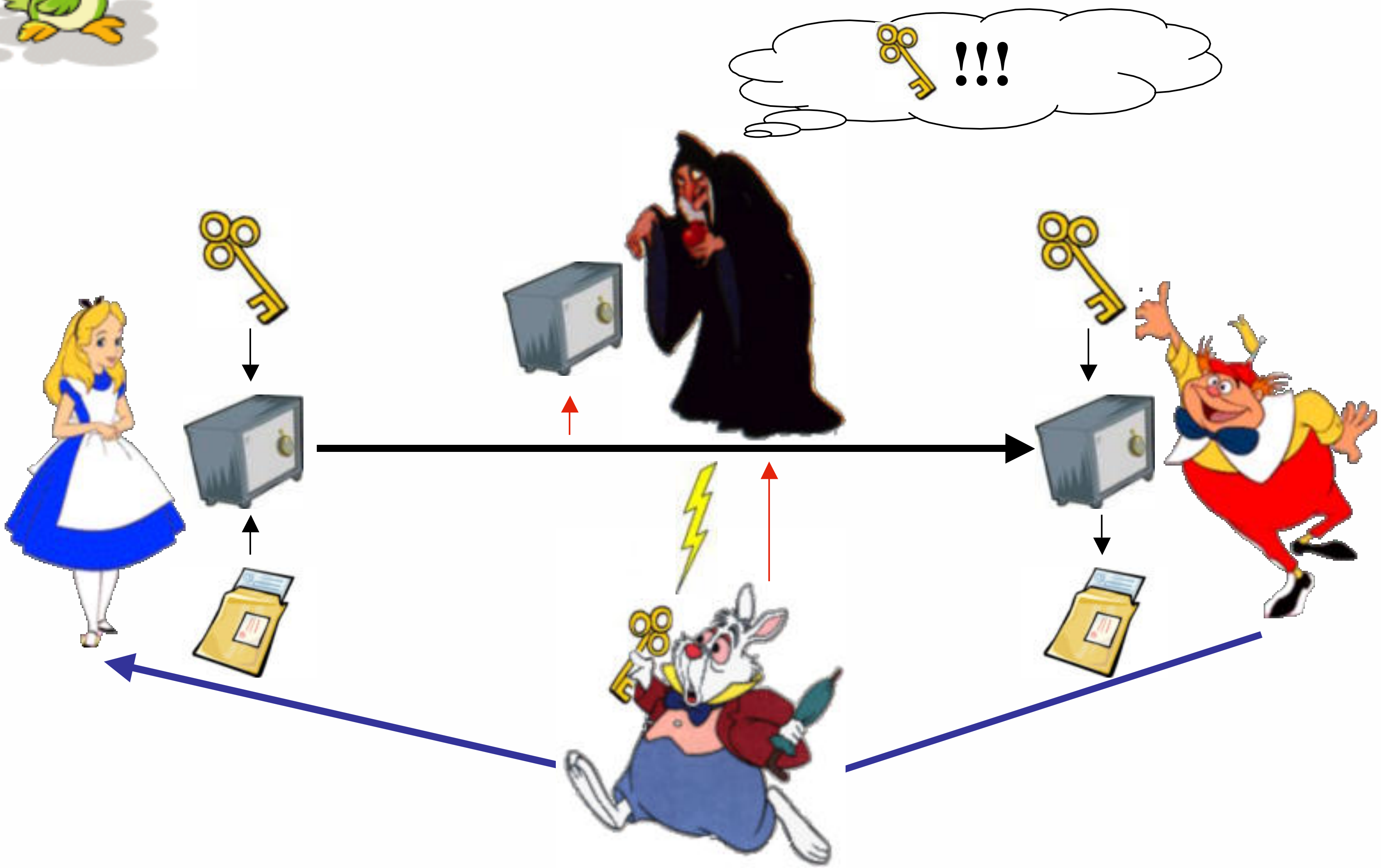
Only Alice and Bob know the key.

Secret Key Cryptography



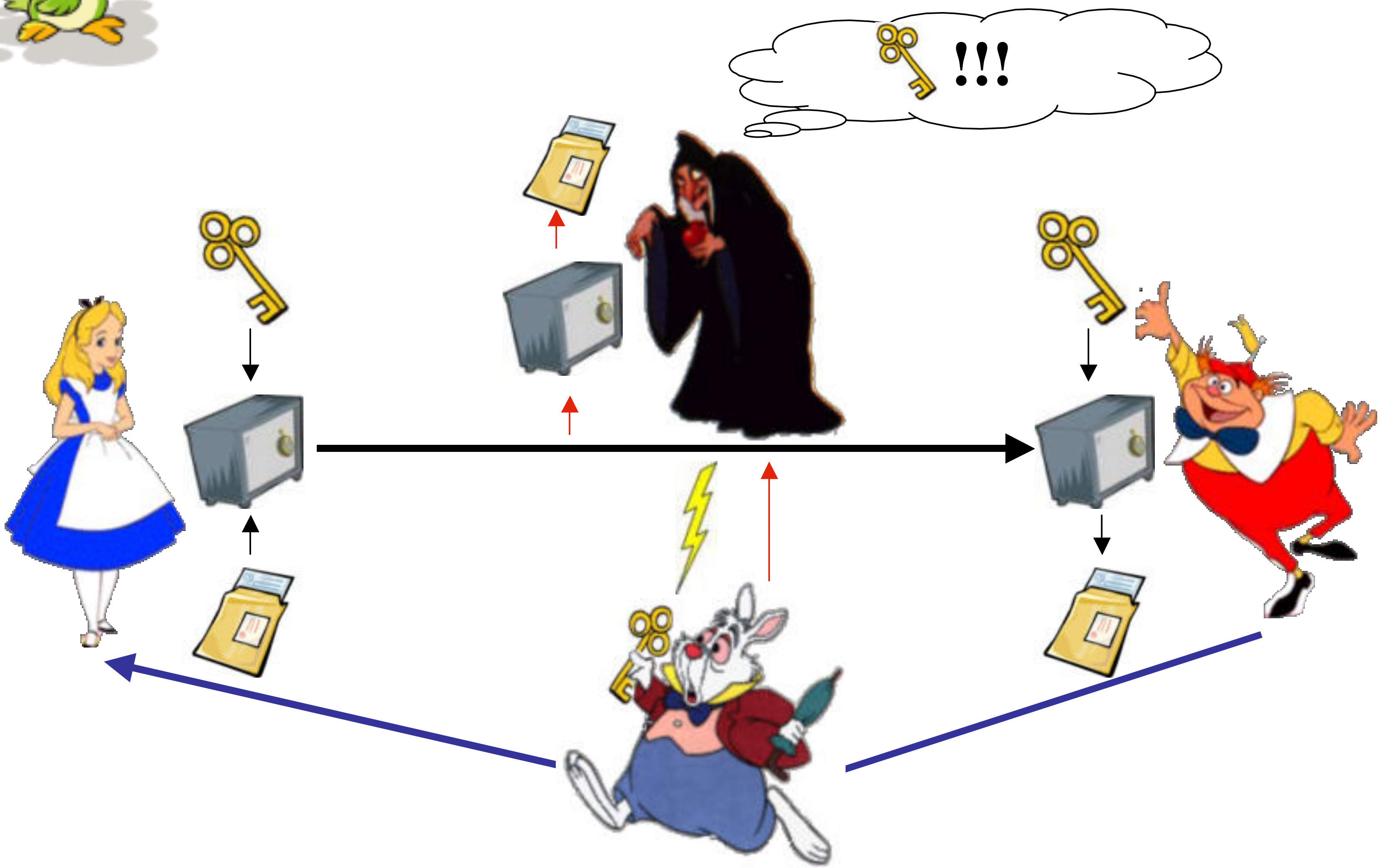
Problem: Need to communicate the key!

Secret Key Cryptography



Problem: Need to communicate the key!

Secret Key Cryptography

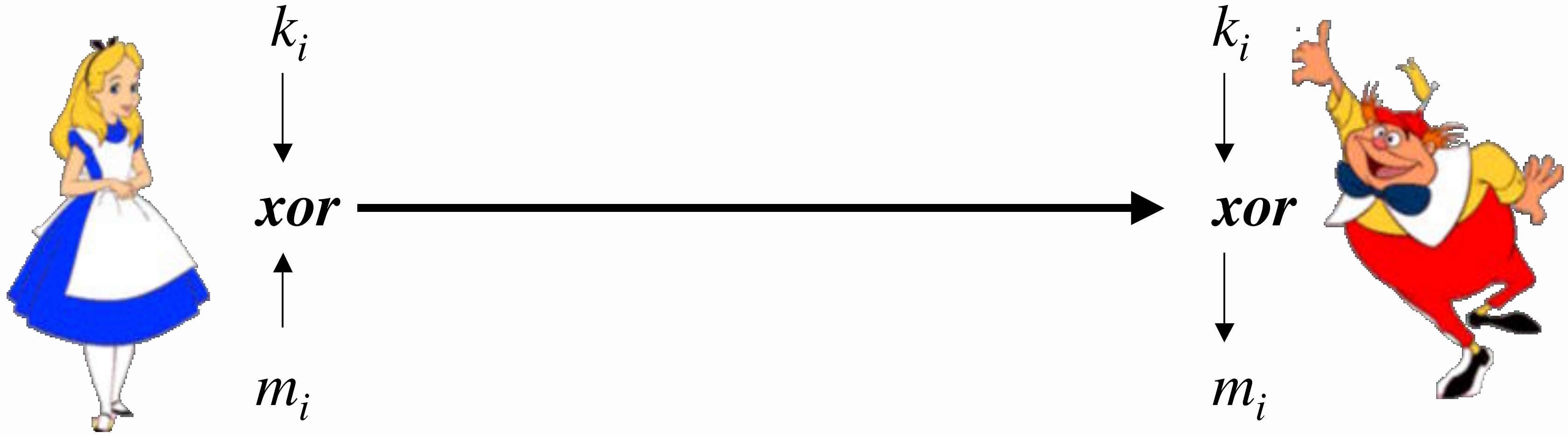


Problem: Need to communicate the key!

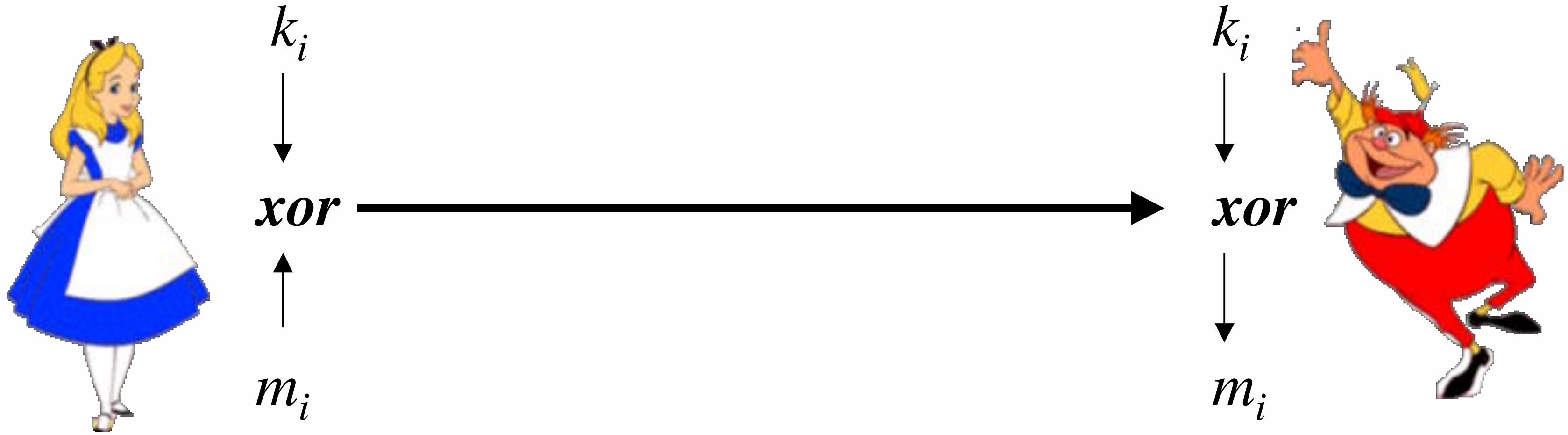
Examples:
Secret Key Cryptography

- Algorithms: DES, IDEA, AES (Rijndael),…
  - Advantage: Short keys
- One-time pad (Vernam cipher)
  - Disadvantage: Key as a long as the message itself
  - This is the **only** system which is secure without imposing any restrictions on the eavesdropper

One time pad



One time pad



Message: 0 1 0 0 1 1 0 0

Key: 0 0 1 0 1 0 0 1

One time pad

k_i

$\downarrow$

xor $\longrightarrow$ ***xor***

$\uparrow$ $\downarrow$

m_i m_i

Message:		0 1 0 0 1 1 0 0
Key:	***xor***	0 0 1 0 1 0 0 1
Encryption:		0 1 1 0 0 1 0 1

One time pad

$$m_i \rightarrow \mathbf{xor} \leftarrow k_i \quad \longrightarrow \quad k_i \rightarrow \mathbf{xor} \rightarrow m_i$$

Message:		0 1 0 0 1 1 0 0
Key:	***xor***	0 0 1 0 1 0 0 1
Encryption:		0 1 1 0 0 1 0 1

Encryption (message ***xor*** key) and decryption (encryption ***xor*** key):

Message 0 1 0 0 1 1 0 0 ***xor*** Key 0 0 1 0 1 0 0 1 → Encryption 0 1 1 0 0 1 0 1

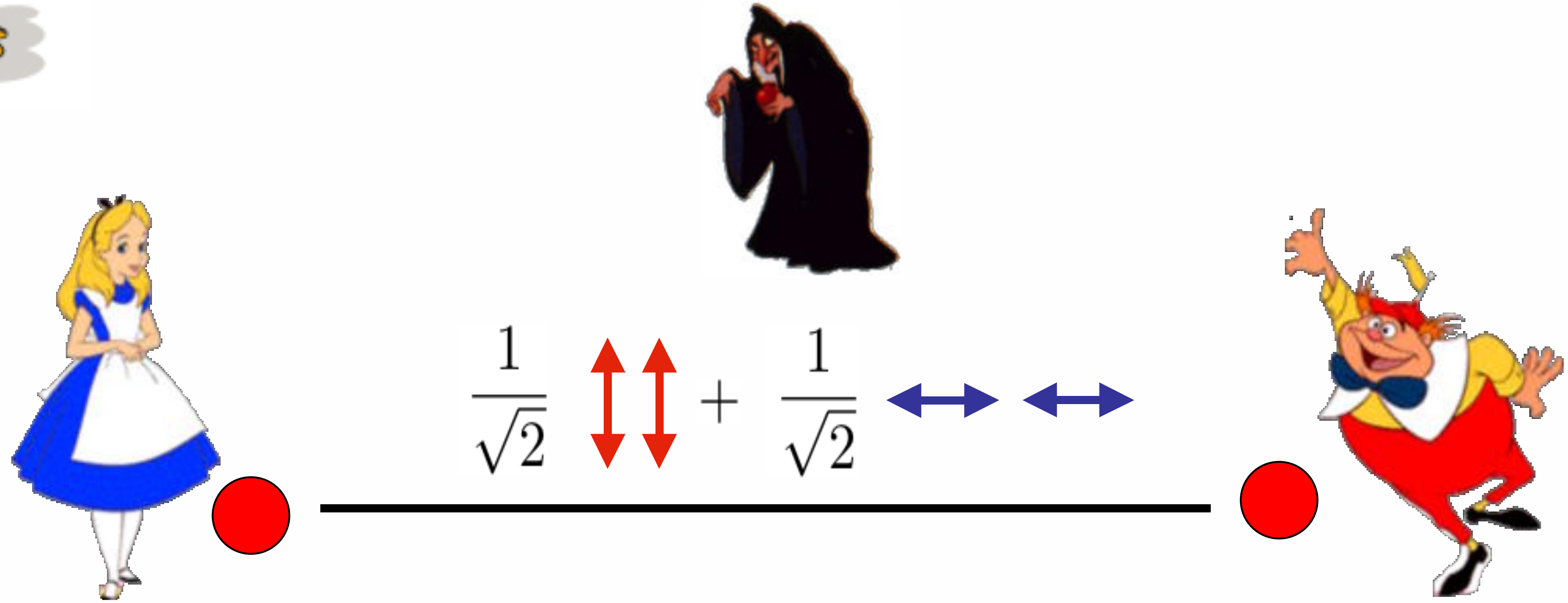
Encryption 0 1 1 0 0 1 0 1 ***xor*** Key 0 0 1 0 1 0 0 1 → Message 0 1 0 0 1 1 0 0

So….

- Secret Key Cryptography
  - Needs a secure channel to distribute the key
  - If the key is shorter then the message, security is based on **non-proven** algorithms (DES, …)
- Public Key Cryptography
  - Security based on **non-proven** assumptions (e.g. factoring is hard)
  - Can be broken with a quantum computer (also retroactively!)

Want: Perfect security from a one time pad, without the need for a secure channel…

Just suppose….



$$\frac{1}{\sqrt{2}}\,\updownarrow\updownarrow + \frac{1}{\sqrt{2}}\,\leftrightarrow\leftrightarrow$$

- *Suppose Alice and Bob shared an EPR pair….*

Just suppose….

$$\frac{1}{\sqrt{2}} \updownarrow\updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow\leftrightarrow$$

- *Suppose Alice and Bob shared an EPR pair….*
- *Then they could measure to obtain a random bit, of which Eve knows absolutely nothing.*
- *Use this bit as a key.*

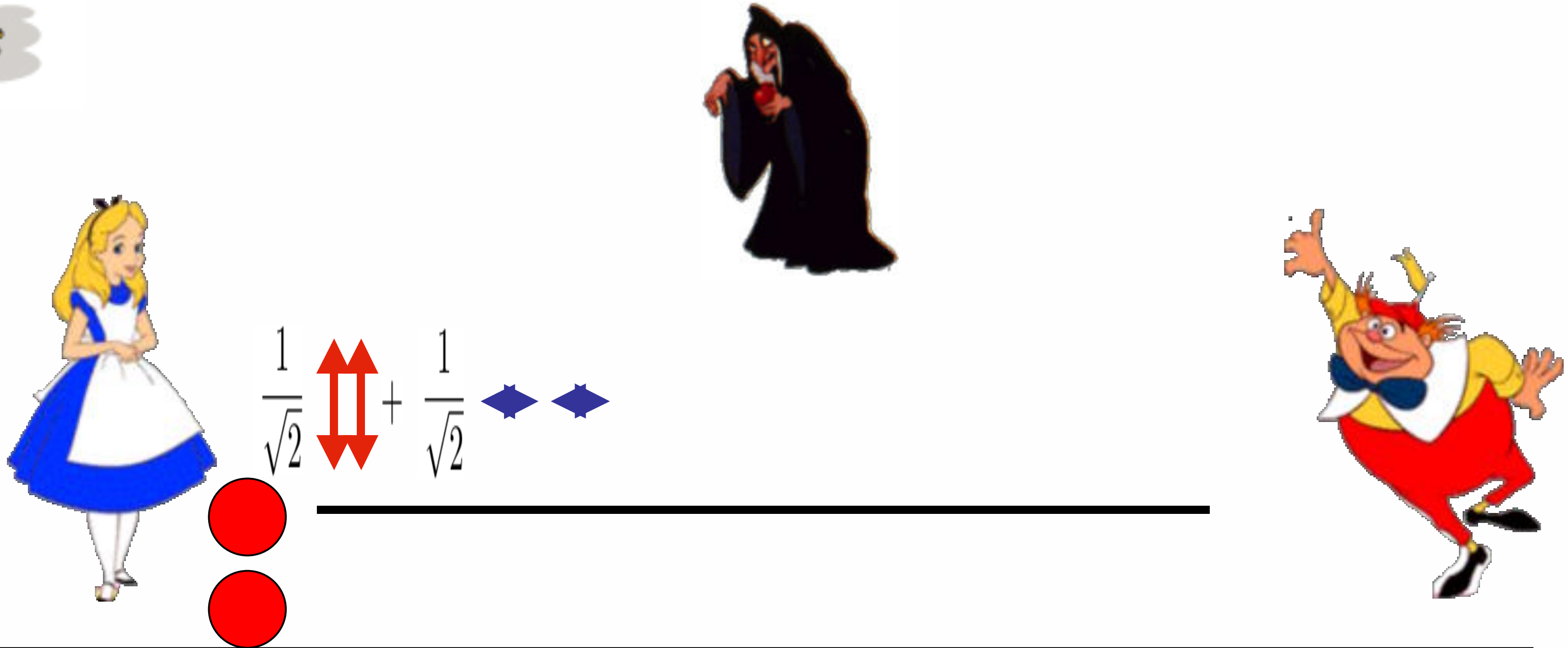
Just suppose….

$$\frac{1}{\sqrt{2}} \updownarrow\updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow\leftrightarrow$$

- *Suppose Alice and Bob shared an EPR pair….*
- *Then they could measure to obtain a random bit, of which Eve knows absolutely nothing.*
- *Use this bit as a key.*

- *But how to get such an EPR pair without Eve interfering ??*

Let's try…



- *Alice creates the entire EPR pair, and sends one half to Bob.*
-

Let’s try…

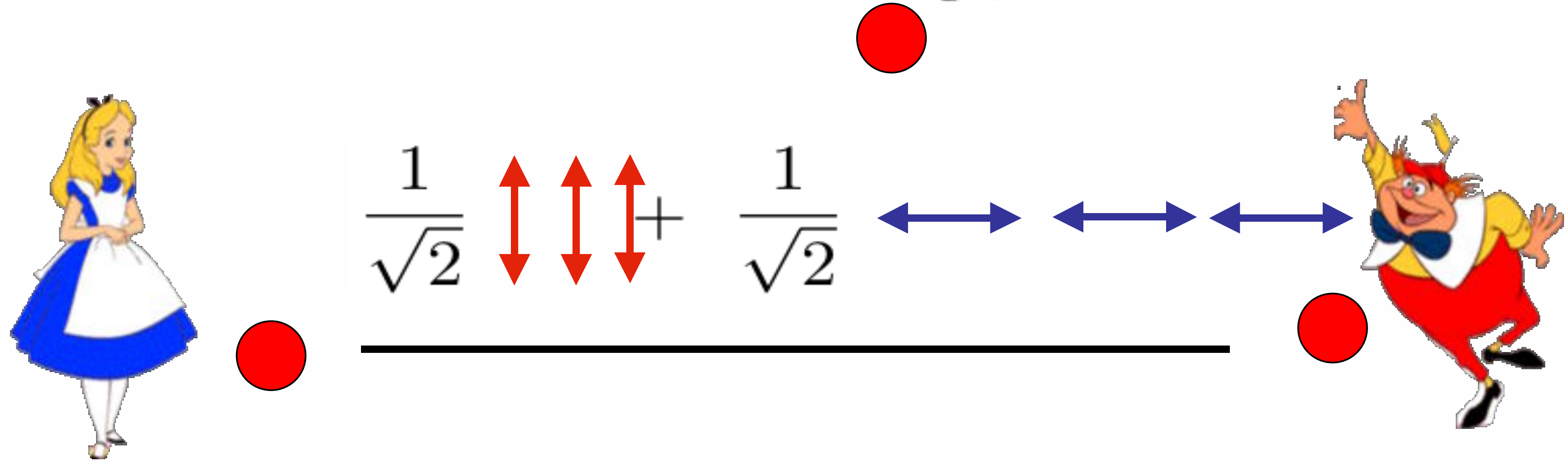
- *Alice creates the entire EPR pair, and sends one half to Bob.*
-

Let's try…

$$\frac{1}{\sqrt{2}} \updownarrow\updownarrow + \frac{1}{\sqrt{2}} \leftrightarrow\leftrightarrow$$

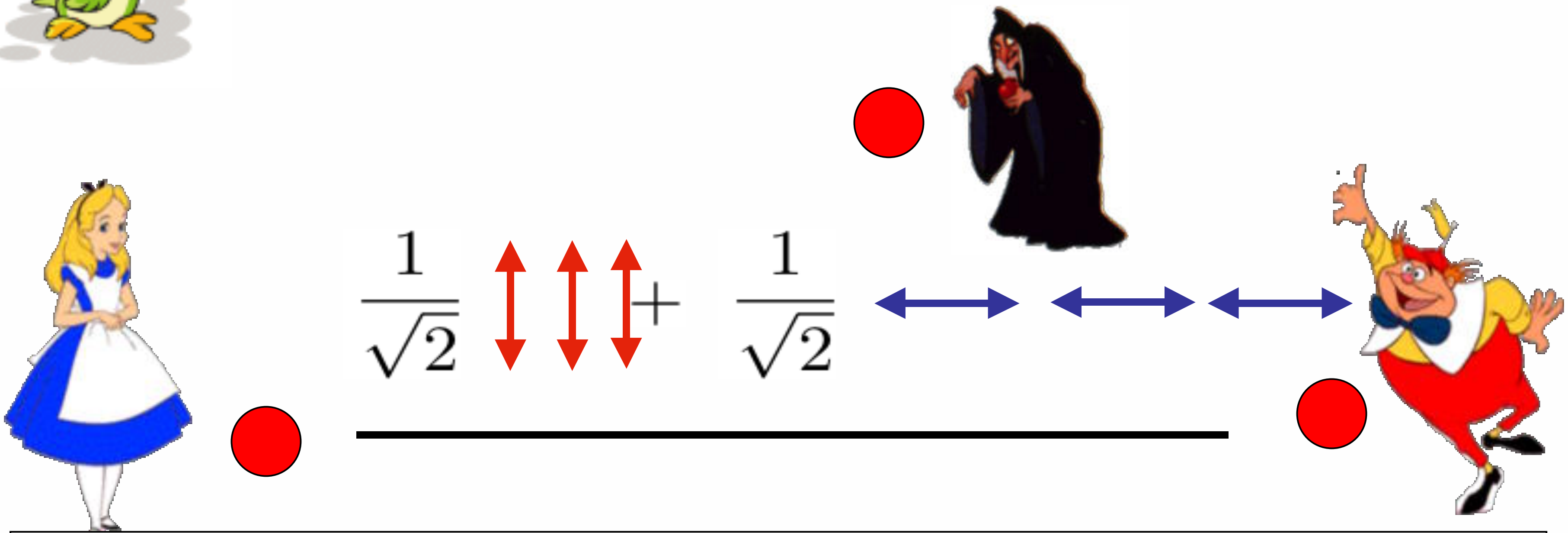
- *Alice creates the entire EPR pair, and sends one half to Bob.*
- *But how can they be sure Eve didn't interfere?*
  - *Perhaps Eve captured Alice's transmission?*

Let’s try…



- *Alice creates the entire EPR pair, and sends one half to Bob.*
- *But how can they be sure Eve didn’t interfere?*
  - *Perhaps Eve captured Alice’s transmission?*
  - *Perhaps Eve is now entangled with both Alice and Bob herself?*

Alice and Bob play a game..



- *But how can they be sure Eve didn't interfere?*
  - *Perhaps Eve is now entangled with both Alice and Bob herself?*
- *Alice and Bob play a two person game, similar to the GHZ game using a random subset of possible EPR pairs.*
- *They check all runs of the game: Eve's presence means they can play it 'less well': the win less rounds than they would expect.*
- *If they detect Eve's presence, they abort. Otherwise, they measure.*

Summary

- Quantum Computing differs dramatically from classical computing
- Entanglement is fundementally different from classical correlations.
- Entanglement plays a central role in quantum computing and cryptography.
- Still many things remain open..