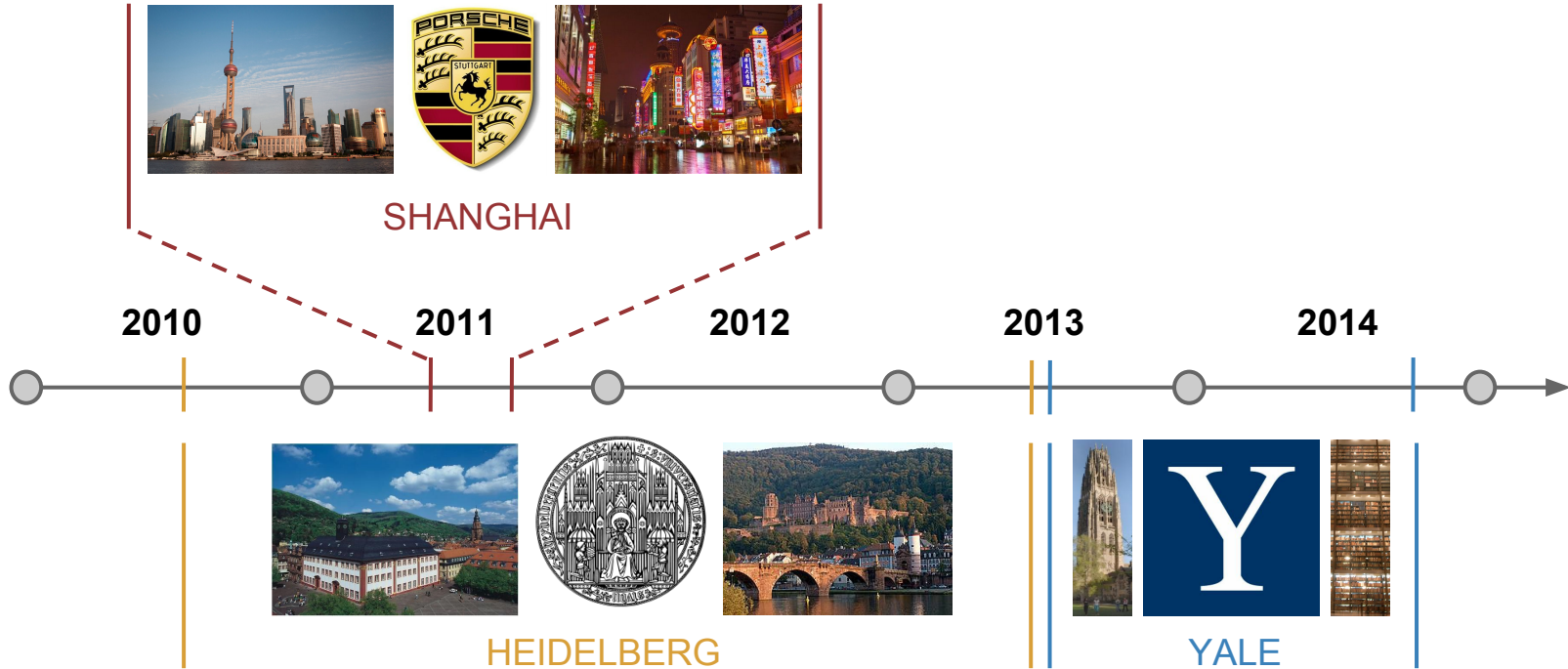


Quantum Cryptography

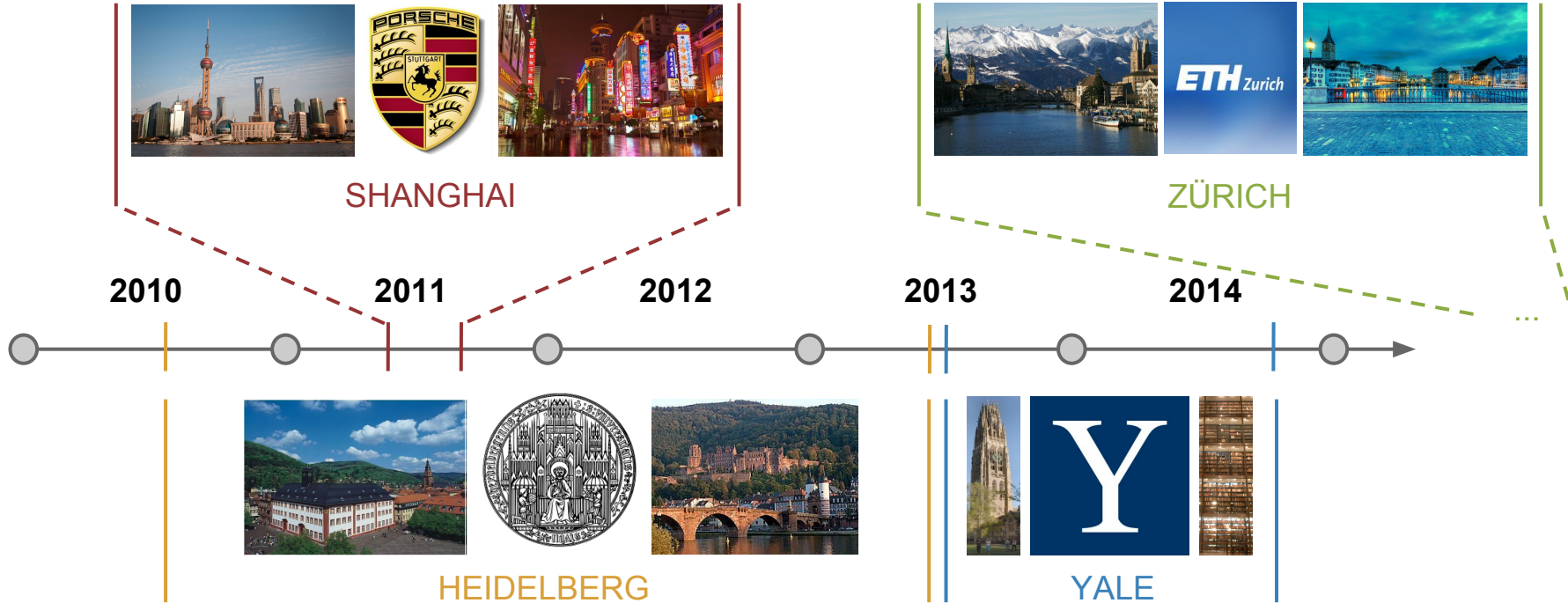
Christian Klumpp

christian.klumpp@yale.edu

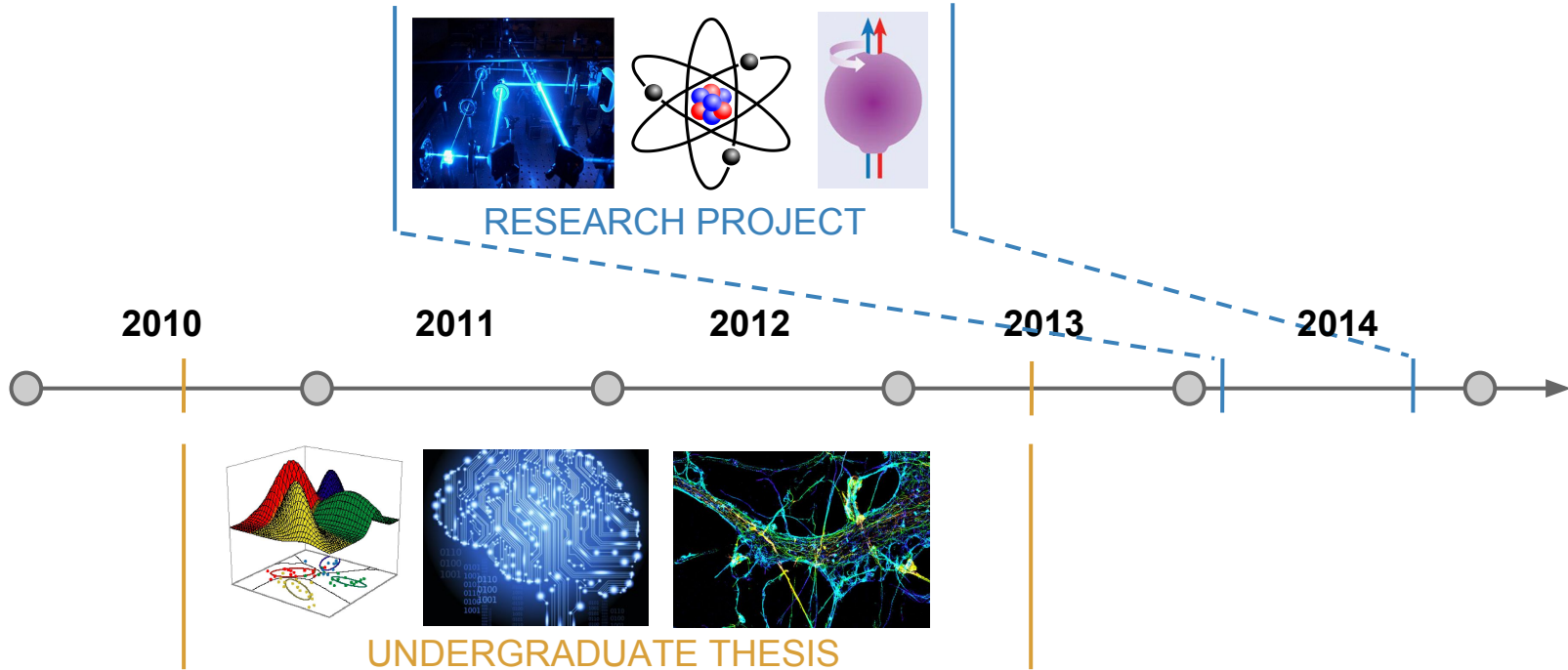
Mostly Germany, some USA and a little bit of China...



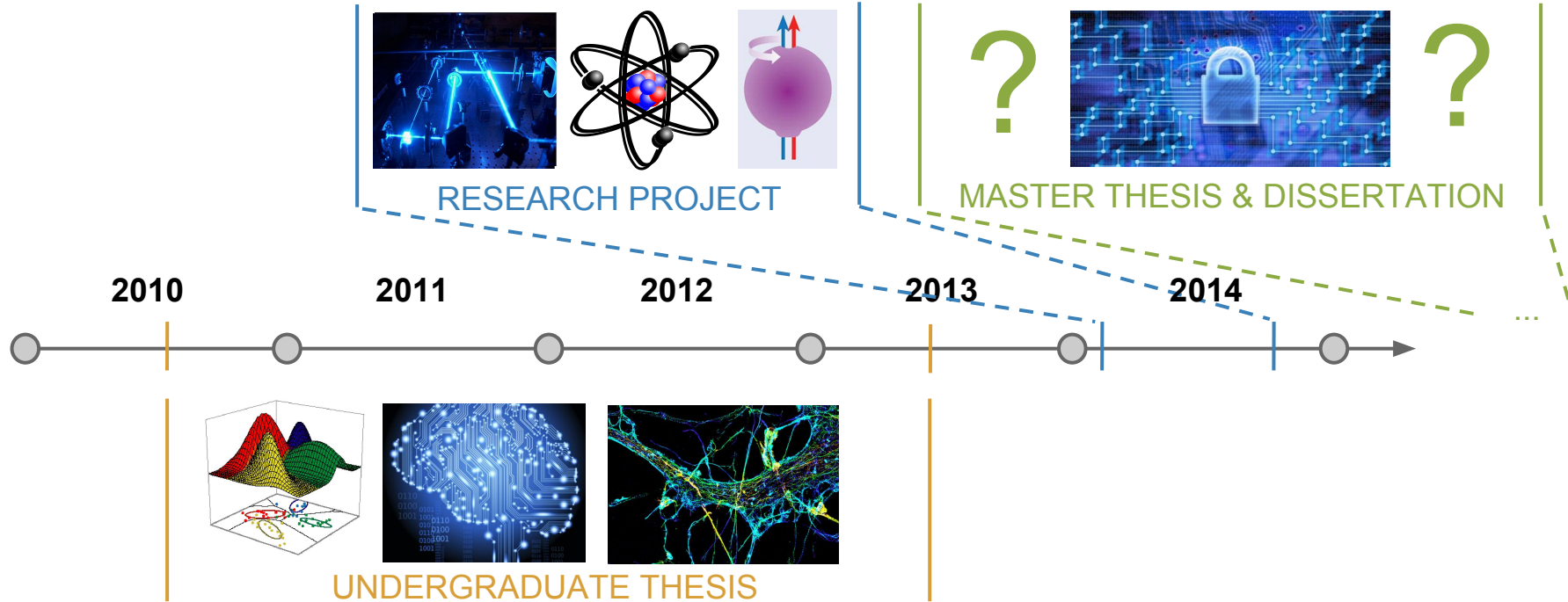
Mostly Germany, some USA and a little bit of China...



Quantum Physics, Computer Science...



...and what combines them...



Why it matters...

STEM



Science • Technology • Engineering • Math

Why it matters...

STEM



The Fundamental
Scientific Theory of
Quantum Physics

Actual Industrial
Realization

The Mathematical
Theory of
Cryptography

Why it matters...

STEM



The Fundamental
Scientific Theory of
Quantum Physics

Actual Industrial
Realization

The Mathematical
Theory of
Cryptography

**Quantum
Cryptography**

As old as Human Civilization...



A Simple Idea with Great Success...



The unbreakable code...?



Great Trust in Great Numbers...

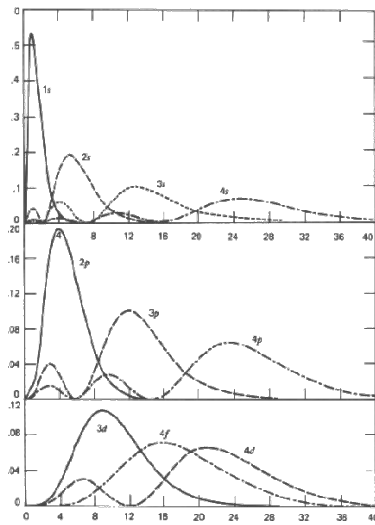
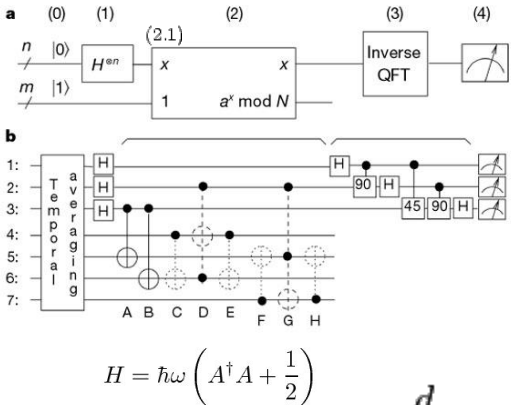
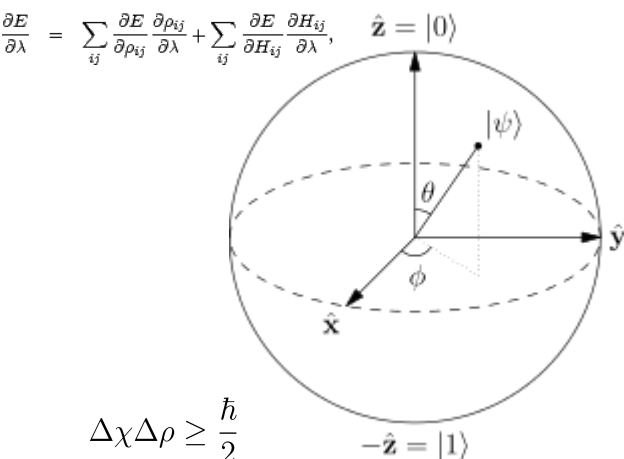
7.900145545423399285584324530571736563179841032857918045046505453908448'.
54269686475396805999350902505048120516638471238179249370533335150467'.
69757632033962013830455970664417287841591362755307185030809072755918'.
55491445804362315480747298228803861431973420537900723634235587754453'.
88503752919885057432882337172137562856751669306470173785120463214232'.
28241831717372361041297275828385160407766204504288958818848045243444'.
50725096374972615123201455621461296370717687502802596367356427075633'.
10626813734885053082569388070936036148230551157463991028120596771747'.
28989167971749500574863694812479649956321729432761161459838479289280'.
60902885529804539758700717244830004135950052675804874787190044439205'.
46142832522524011653847188868079841011615053006919868381182361586878'.
84053263308040654428944411036846235544168996092219790417026983290429'.
68729107782635803858732198984675248984167175763535186812011112630069'.
57213951869429065507224392602789628479106052946180925711669236850049'.
35014828945... $\times 10^{77631168}$

What Quantum Physics taketh away...

$$E = \text{Tr}[\rho H] = \sum_{ij} \rho_{ij} H_{ji}$$

$$\frac{\partial E}{\partial \lambda} = \sum_{ij} \frac{\partial E}{\partial \rho_{ij}} \frac{\partial \rho_{ij}}{\partial \lambda} + \sum_{ij} \frac{\partial E}{\partial H_{ij}} \frac{\partial H_{ij}}{\partial \lambda}$$

$$H(t)|\psi(t)\rangle = i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle \quad |\Psi\rangle = c_1|\uparrow\rangle + c_2|\downarrow\rangle$$



$$\sigma_x = \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \frac{1}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

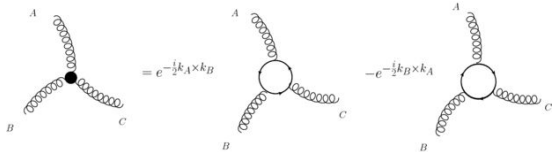
$$\sigma_z = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\Delta\chi\Delta\rho \geq \frac{\hbar}{2}$$

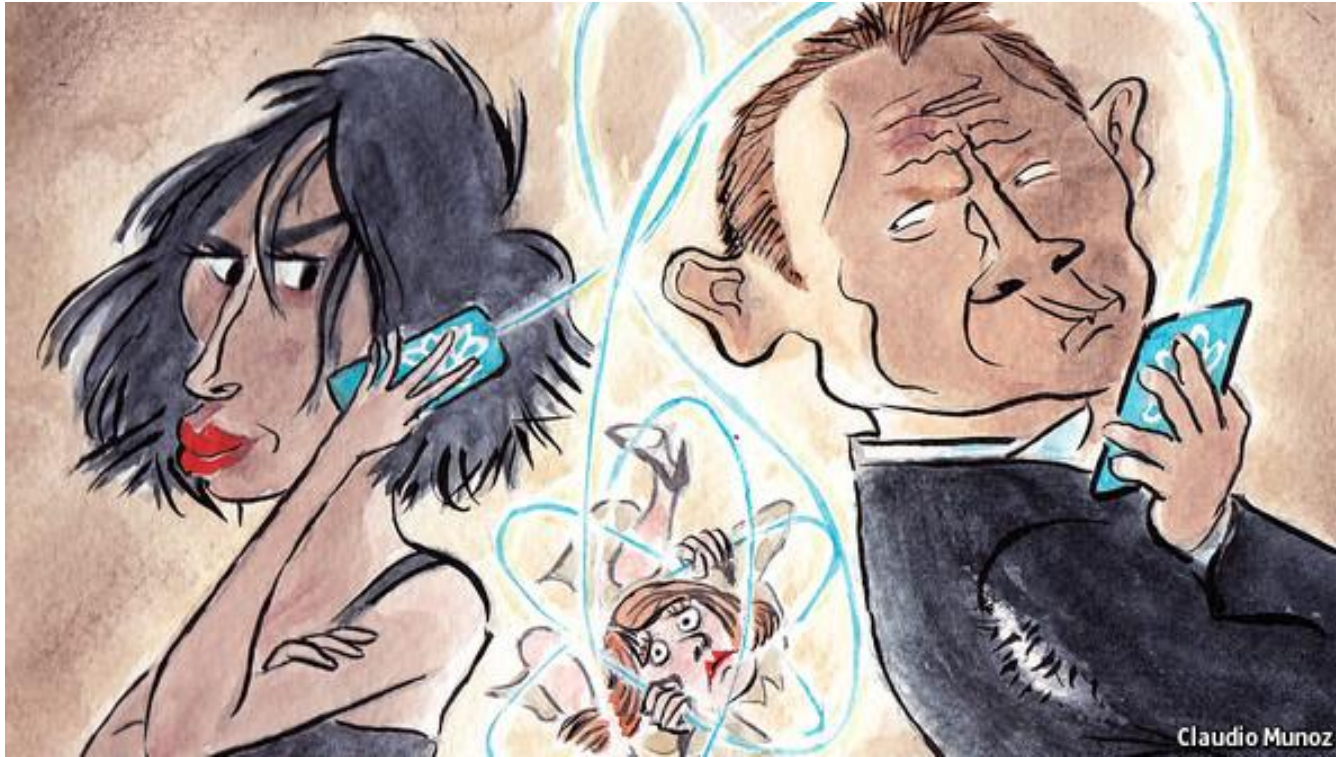
$$\mathcal{L}'_{\text{grav}} = \frac{1}{8\kappa} \left(\partial_0 \hat{\Psi}_\nu^\mu \cdot \partial_0 \hat{\Psi}_\mu^\nu - \frac{1}{2} \partial_0 \hat{\Psi} \cdot \partial_0 \hat{\Psi} \right) + \frac{1}{8\kappa} g_\rho^\sigma \left(\hat{\Psi}_\nu^{\mu,\rho} \hat{\Psi}_{\mu,\sigma}^\nu - \frac{1}{2} \hat{\Psi}^{\rho,\sigma} \hat{\Psi}_{\rho,\sigma} - 2 \hat{\Psi}_\nu^{\rho,\mu} \hat{\Psi}_{\mu,\sigma}^\nu \right)$$

$$\int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} \exp \left(\frac{i}{\hbar} \int_{t_a}^{t_b} L(x(t), v(t), t) dt \right) dx_0 \dots dx_n$$

$$\frac{d}{dt} A(t) = \frac{i}{\hbar} [H, A(t)] + e^{iHt/\hbar} \left(\frac{\partial A}{\partial t} \right) e^{-iHt/\hbar}$$



... Quantum Physics bringeth back



CHAPTER 1

A brief Introduction to One-Time-Pads

Truly unbreakable...

Binary Addition

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Truly unbreakable...

Binary Addition

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Message

Key

Encrypted

Alice

0 1 1 0 1 1 1 0 0 0 1 0

\oplus 1 1 0 1 0 0 1 1 1 1 0 0

1 0 1 1 1 1 0 1 1 1 1 0

Truly unbreakable...

Binary Addition

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Message

Key

Encrypted

Alice

0 1 1 0 1 1 1 0 0 0 1 0

\oplus 1 1 0 1 0 0 1 1 1 1 0 0

1 0 1 1 1 1 0 1 1 1 1 0

Bob

Encrypted

Key

Message

1 0 1 1 1 1 0 1 1 1 1 0

\oplus 1 1 0 1 0 0 1 1 1 1 0 0

0 1 1 0 1 1 1 0 0 0 1 0

How do we get the Key safely from Alice to Bob...?

CHAPTER 2

A brief Introduction to Quantum Physics

Superpositions, the first weird thing...

Classical Physics



OR



Superpositions, the first weird thing...

Classical Physics



OR



Quantum Physics



Superpositions, the first weird thing...

Classical Physics



OR



Quantum Physics



=



+



Superpositions, the first weird thing...

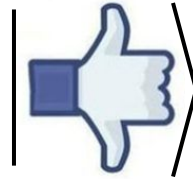
Classical Physics



OR



Quantum Physics



$$= \frac{1}{\sqrt{2}} \left(\left| \text{thumbs up} \right\rangle + \left| \text{thumbs down} \right\rangle \right)$$

Superpositions, the first weird thing...

Classical Physics

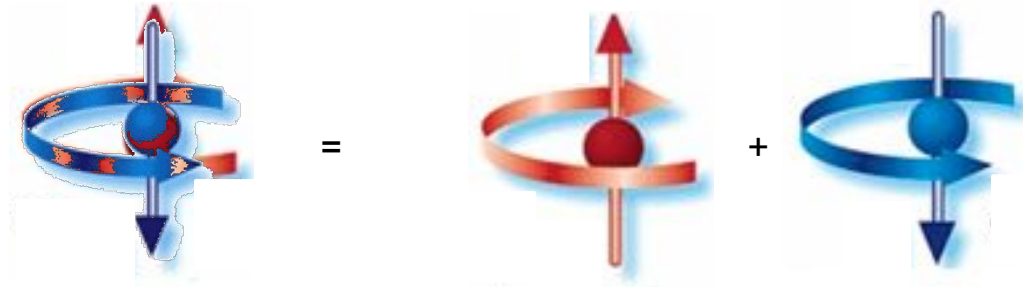
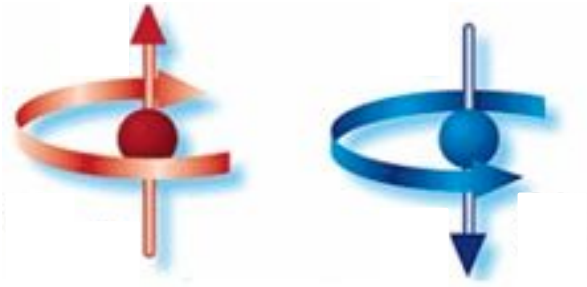


OR



Quantum Physics

$$\left| \text{thumbs up} \right\rangle = \frac{1}{\sqrt{2}} \left(\left| \text{thumbs up} \right\rangle + \left| \text{thumbs down} \right\rangle \right)$$



Superpositions, the first weird thing...

Classical Physics



Quantum Physics

$$\left| \text{thumbs up} \right\rangle = \frac{1}{\sqrt{2}} \left(\left| \text{thumbs up} \right\rangle + \left| \text{thumbs down} \right\rangle \right)$$



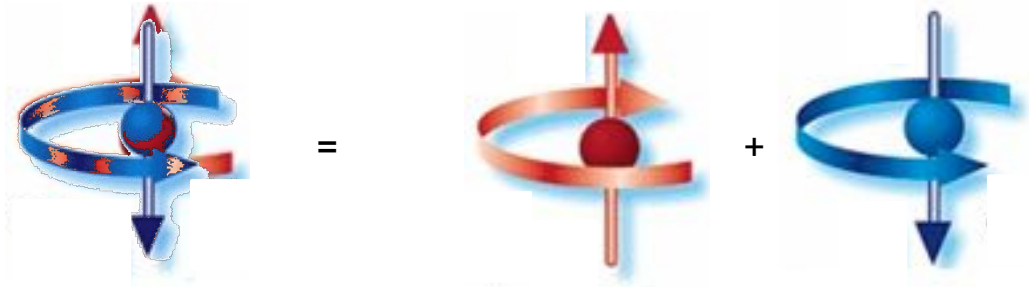
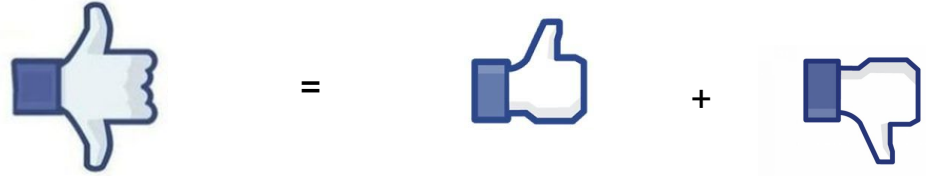
$$\left| \text{superposition} \right\rangle = \frac{1}{\sqrt{2}} \left[\left| \text{red sphere up} \right\rangle + \left| \text{blue sphere down} \right\rangle \right]$$

Superpositions, the first weird thing...

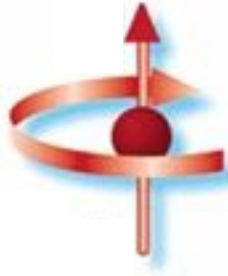
Classical Physics



Quantum Physics



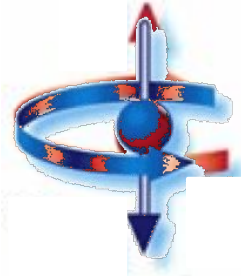
The Spin, as 'Quantum' as it gets...



'Spin Up'

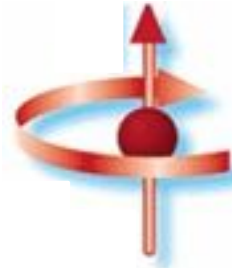


'Spin Down'



Superposition

=

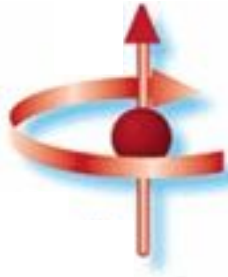


+



$$= \frac{1}{\sqrt{2}} \left[\text{'Spin Up'} + \text{'Spin Down'} \right]$$

The Spin, as 'Quantum' as it gets...



'Spin Up'

 $|\uparrow\rangle$ 

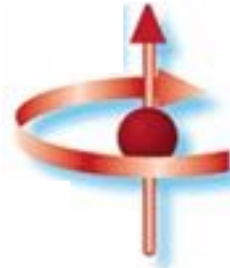
'Spin Down'

 $|\downarrow\rangle$ 

Superposition

 $|S\rangle$

=

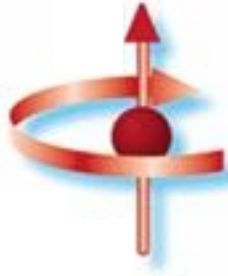


+



$$= \frac{1}{\sqrt{2}} \left[\text{'Spin Up'} + \text{'Spin Down'} \right]$$
$$= \frac{1}{\sqrt{2}} \left[|\uparrow\rangle + |\downarrow\rangle \right]$$

The Spin, as 'Quantum' as it gets...



'Spin Up'

 $|\uparrow\rangle$ $|0\rangle$ 

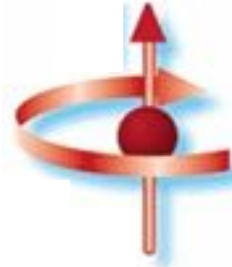
'Spin Down'

 $|\downarrow\rangle$ $|1\rangle$ 

Superposition

 $|S\rangle$ $|S\rangle$

=



+



$$= \frac{1}{\sqrt{2}} \left[\text{'Spin Up'} + \text{'Spin Down'} \right]$$

$$= \frac{1}{\sqrt{2}} \left[|\uparrow\rangle + |\downarrow\rangle \right]$$

$$= \frac{1}{\sqrt{2}} \left[|0\rangle + |1\rangle \right]$$

Measurements, the second weird thing...



Chris Klumpp

Just now · New Haven, CT

Today is a beautiful day.

Measurements, the second weird thing...



Mark has full control
over Quantum Physics



Chris Klumpp

Just now · New Haven, CT



Today is a beautiful day.

Measurements, the second weird thing...



Mark has full control
over Quantum Physics



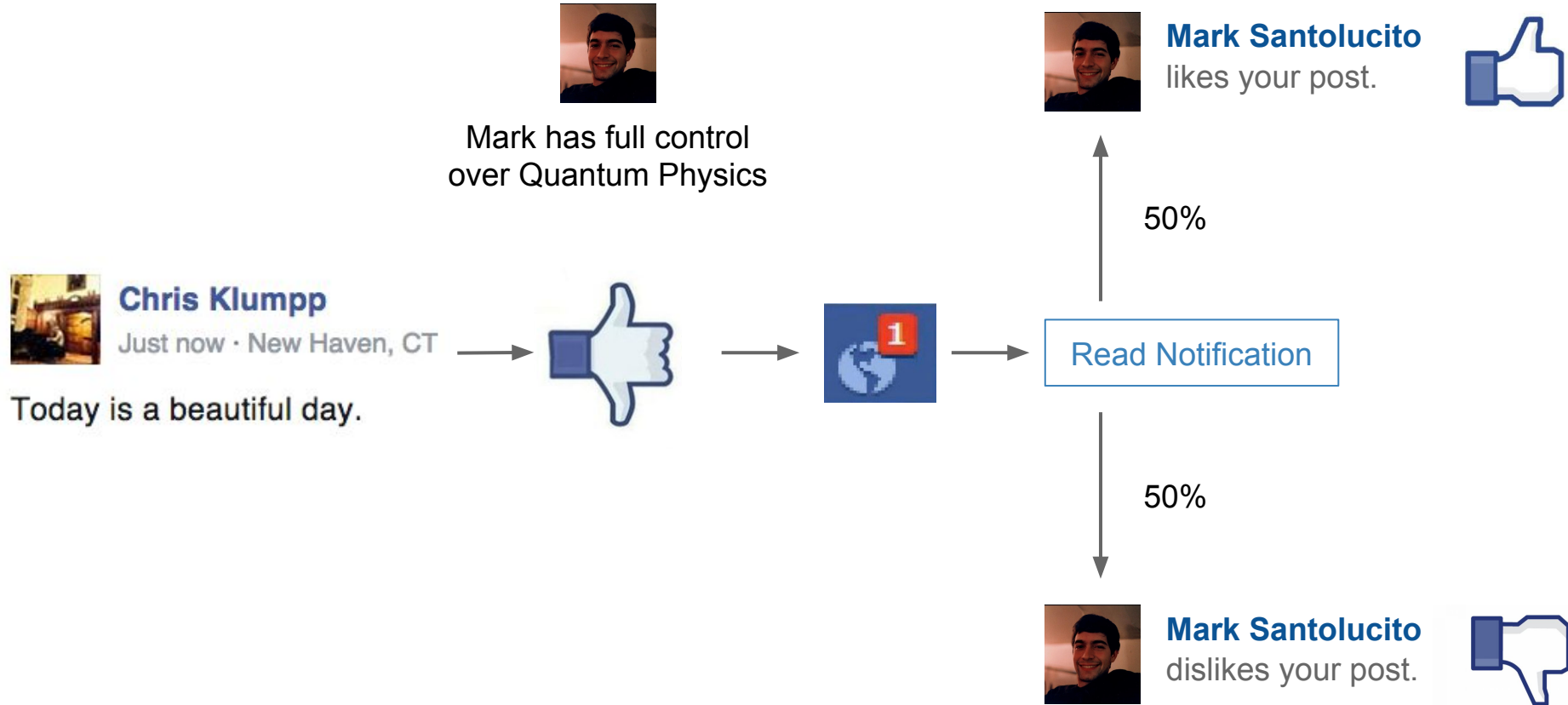
Chris Klumpp

Just now · New Haven, CT

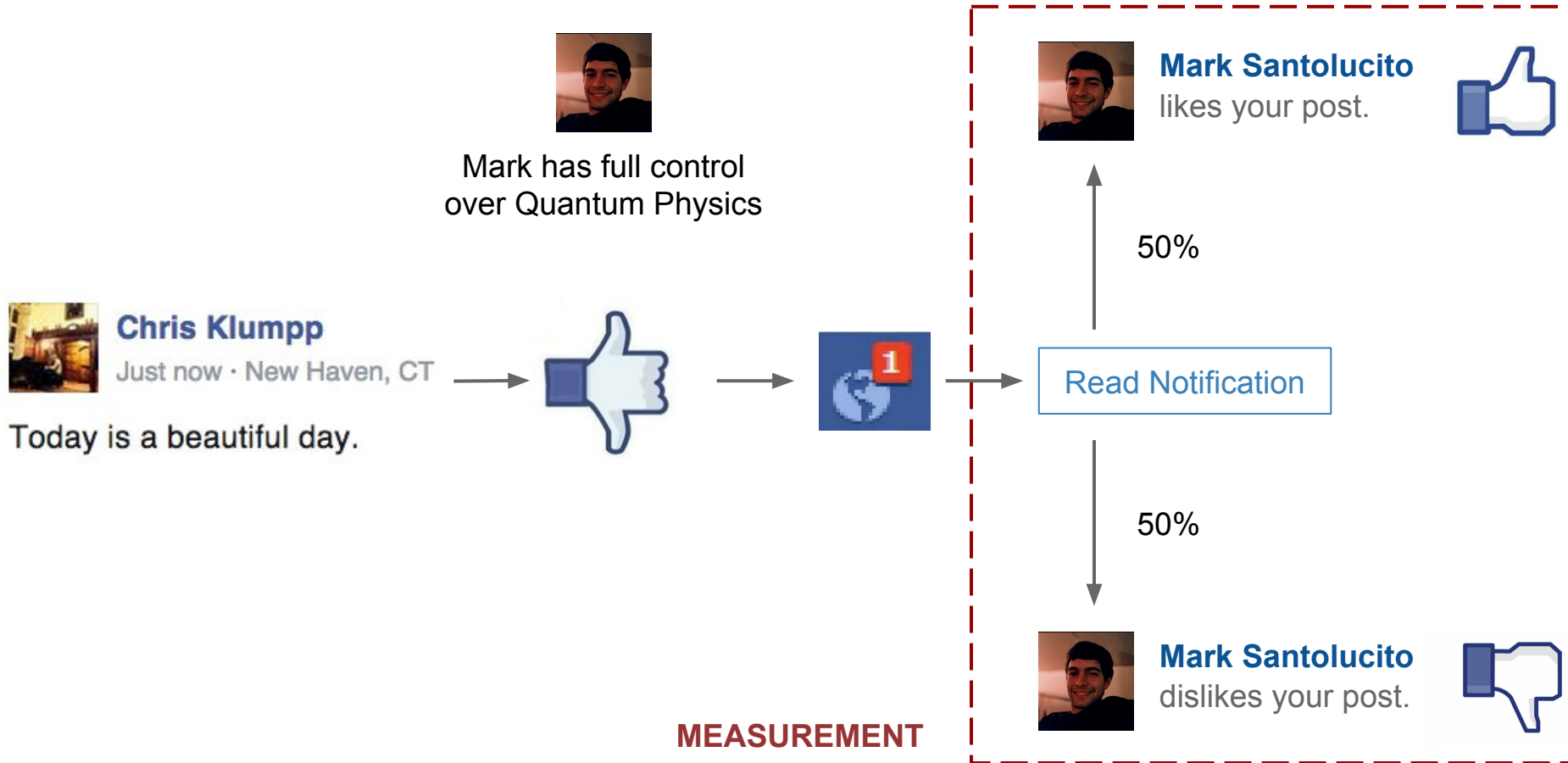
Today is a beautiful day.



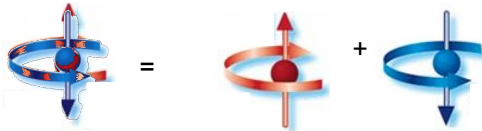
Measurements, the second weird thing...



Measurements, the second weird thing...



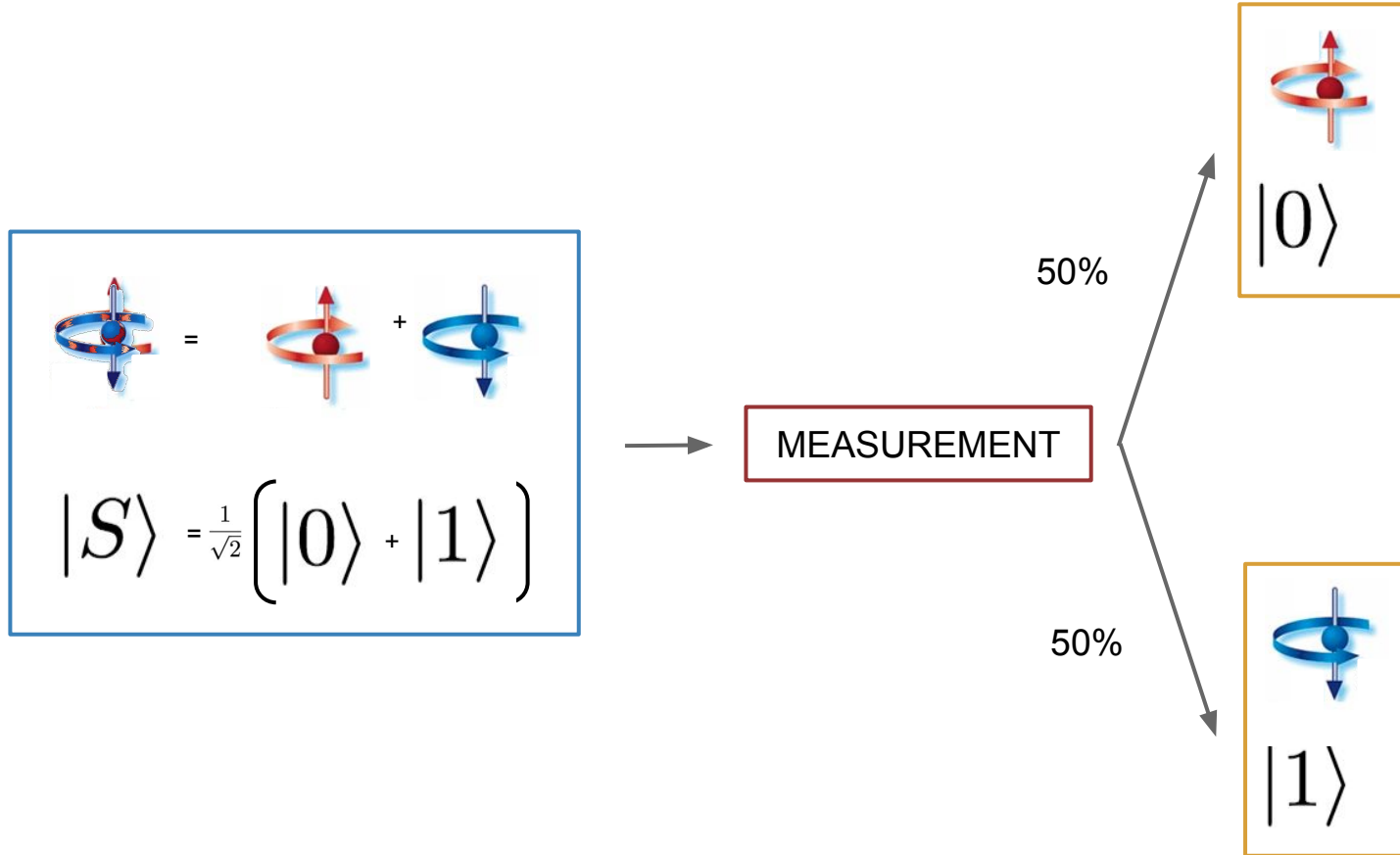
Measurements, the second weird thing...


$$|S\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right)$$

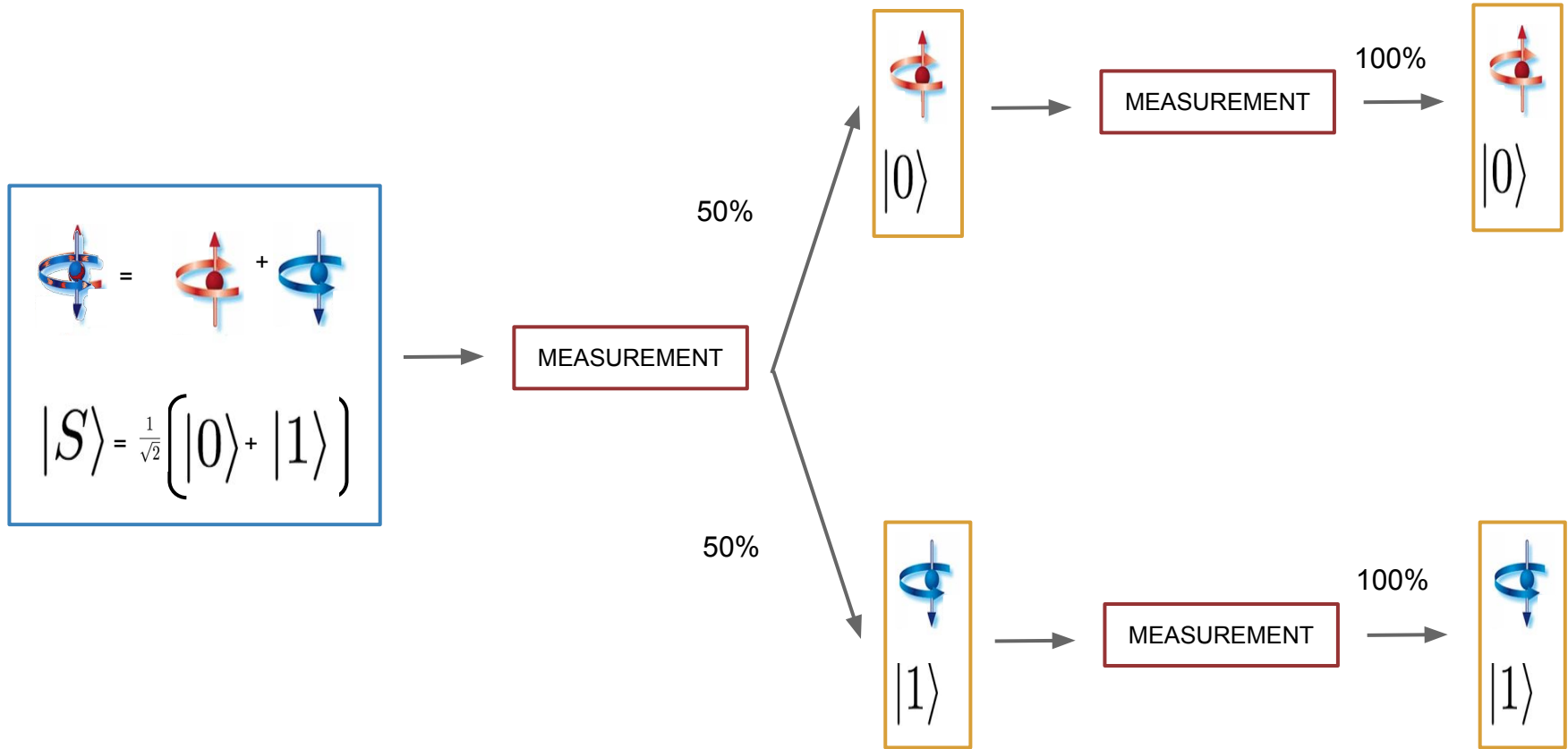


MEASUREMENT

Measurements, the second weird thing...



Measurements, the second weird thing...

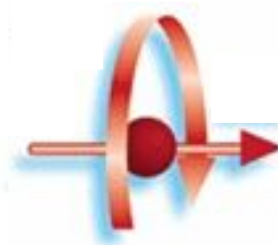


It just gets a tiny bit weirder...

Particles can 'spin' in different directions...



$|1\rangle_X$



$|0\rangle_X$

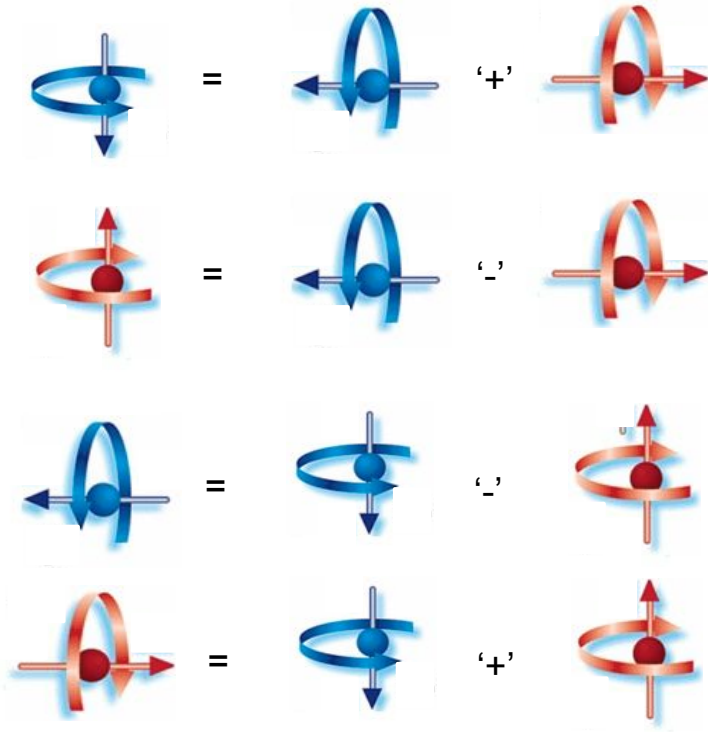


$|1\rangle_Z$



$|0\rangle_Z$

It just gets a tiny bit weirder...



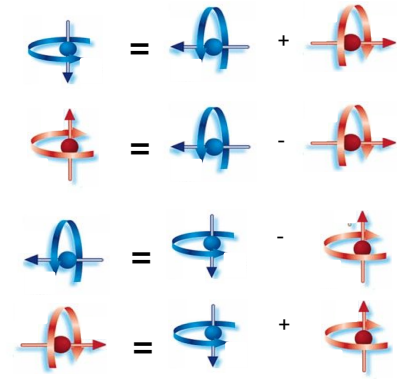
$$|0\rangle_Z = \frac{1}{\sqrt{2}} (|0\rangle_X + |1\rangle_X)$$

$$|1\rangle_Z = \frac{1}{\sqrt{2}} (|0\rangle_X - |1\rangle_X)$$

$$|0\rangle_X = \frac{1}{\sqrt{2}} (|0\rangle_Z + |1\rangle_Z)$$

$$|1\rangle_X = \frac{1}{\sqrt{2}} (|0\rangle_Z - |1\rangle_Z)$$

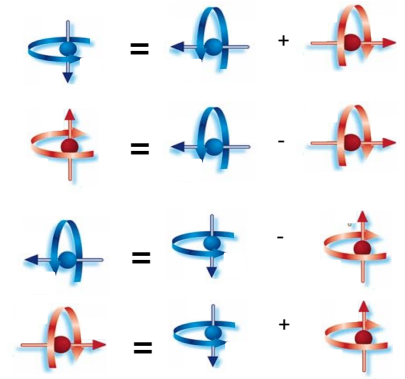
It just gets a tiny bit weirder...



SERIES OF MEASUREMENTS



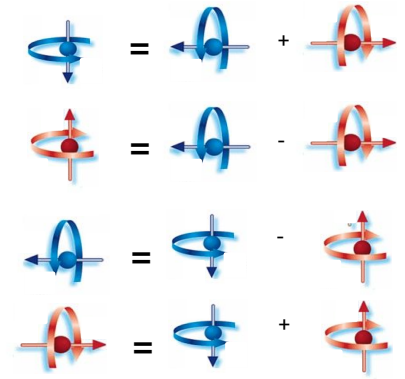
It just gets a tiny bit weirder...



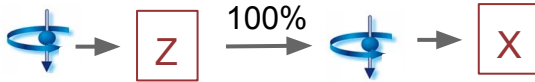
SERIES OF MEASUREMENTS



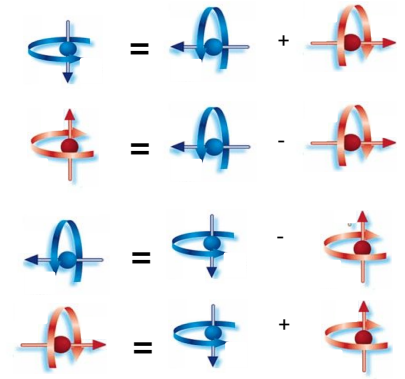
It just gets a tiny bit weirder...



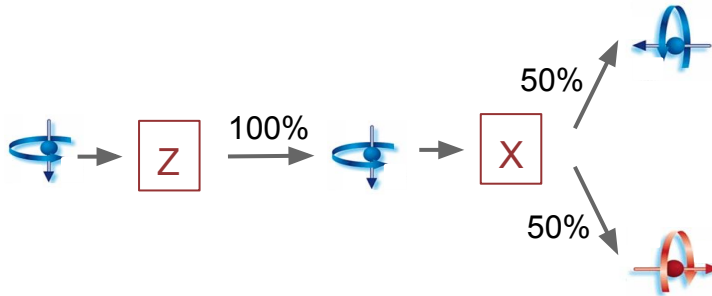
SERIES OF MEASUREMENTS



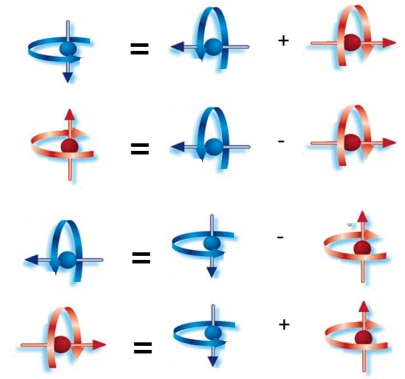
It just gets a tiny bit weirder...



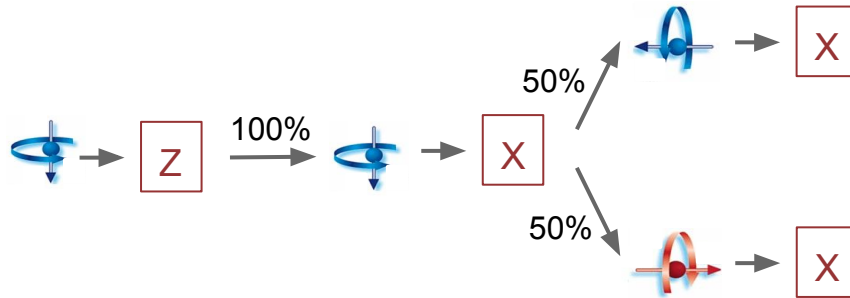
SERIES OF MEASUREMENTS



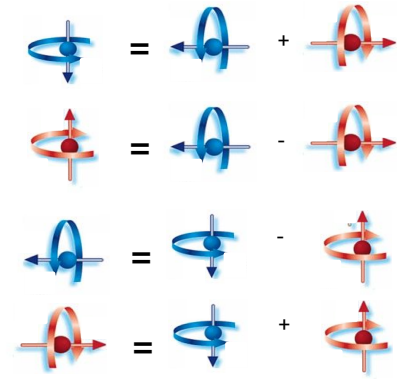
It just gets a tiny bit weirder...



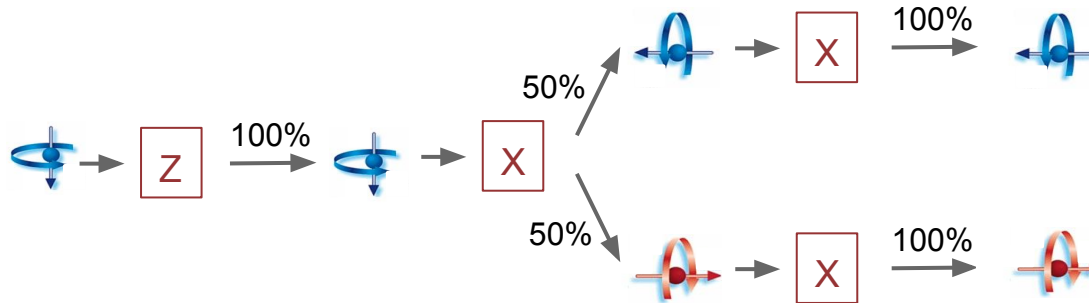
SERIES OF MEASUREMENTS



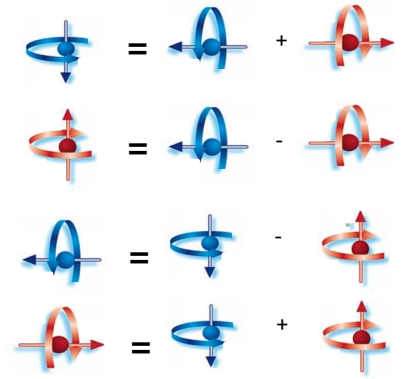
It just gets a tiny bit weirder...



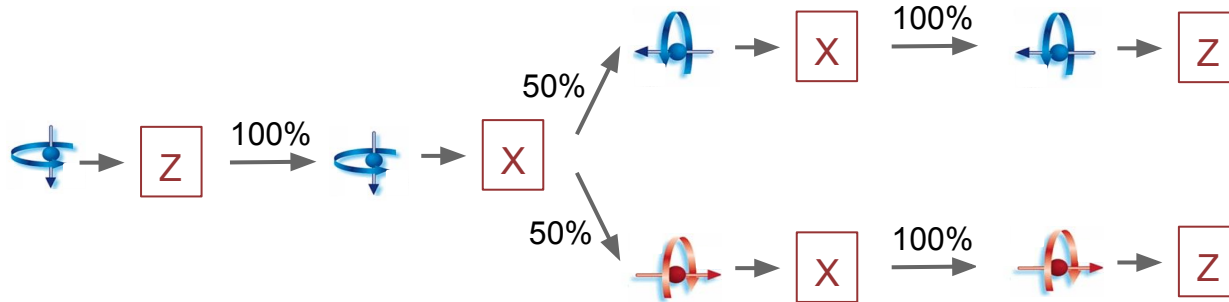
SERIES OF MEASUREMENTS



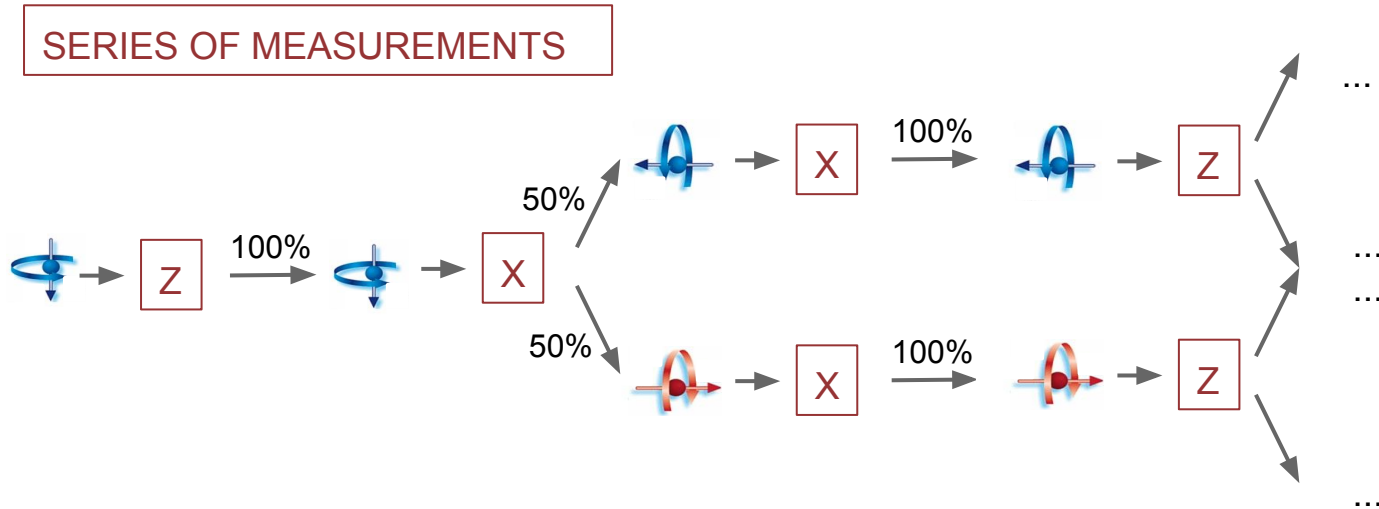
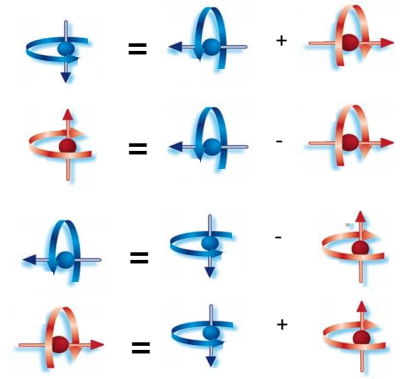
It just gets a tiny bit weirder...



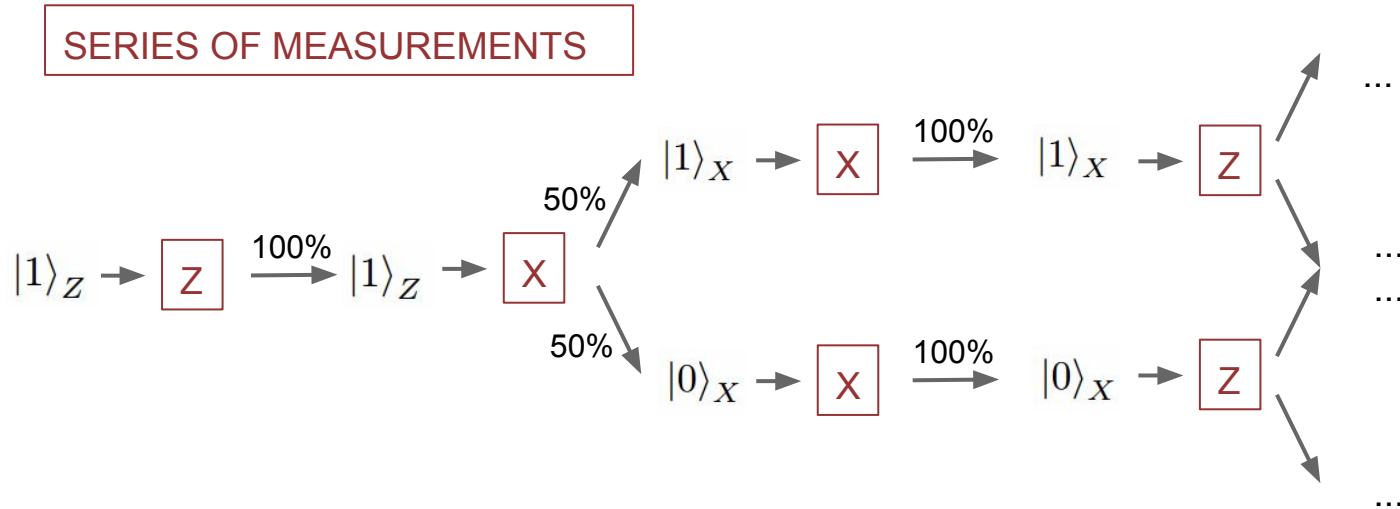
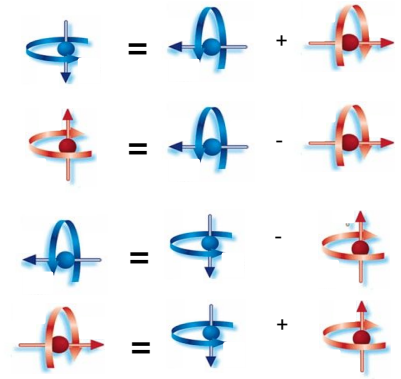
SERIES OF MEASUREMENTS



It just gets a tiny bit weirder...



It just gets a tiny bit weirder...



That is it. That is all you need.

CHAPTER 3

Quantum Cryptography

BB84 Protocol (Idea)

Qubits produced in two Bases

$$|0\rangle_Z, |1\rangle_Z \quad |0\rangle_X, |1\rangle_X$$

$$|0\rangle_Z = \frac{1}{\sqrt{2}} (|0\rangle_X + |1\rangle_X)$$

$$|1\rangle_Z = \frac{1}{\sqrt{2}} (|0\rangle_X - |1\rangle_X)$$

$$|0\rangle_X = \frac{1}{\sqrt{2}} (|0\rangle_Z + |1\rangle_Z)$$

$$|1\rangle_X = \frac{1}{\sqrt{2}} (|0\rangle_Z - |1\rangle_Z)$$

Possible Realizations

Electron Spins



Photon Polarizations (more convenient)



BB84 (Procedure)

Single
Particle
Source

Alice

1. Randomly choose
basis

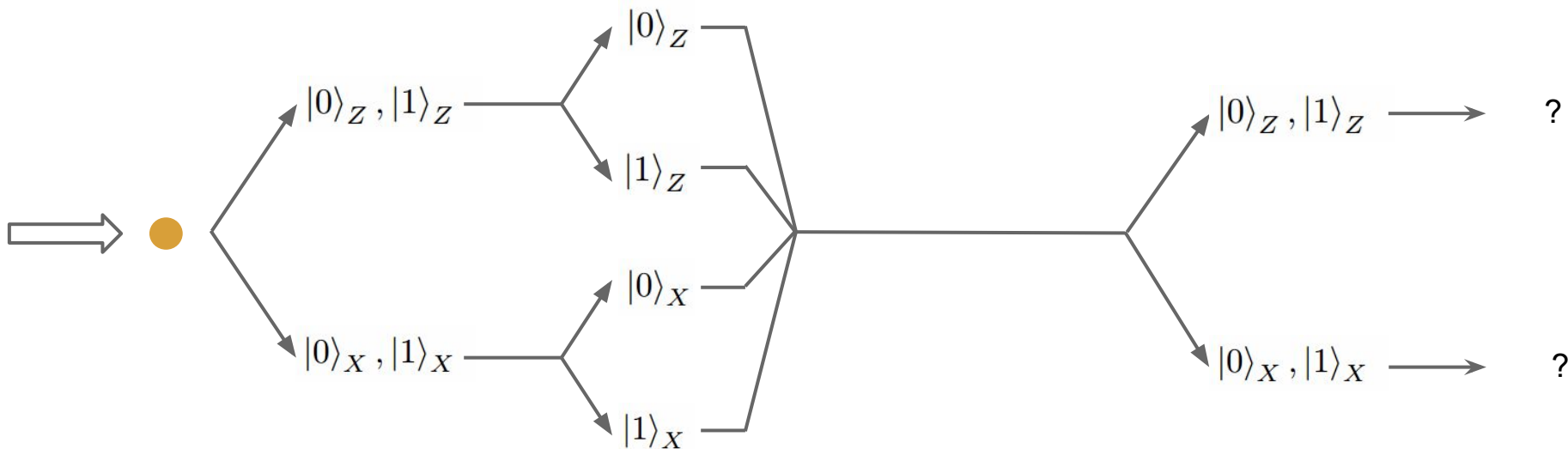
2. Prepare in random
state

3. Transmit through Quantum
Channel

Bob

4. Randomly choose
basis

5. Measure



BB84 (Procedure)

Single
Particle
Source

Alice

1. Randomly choose
basis

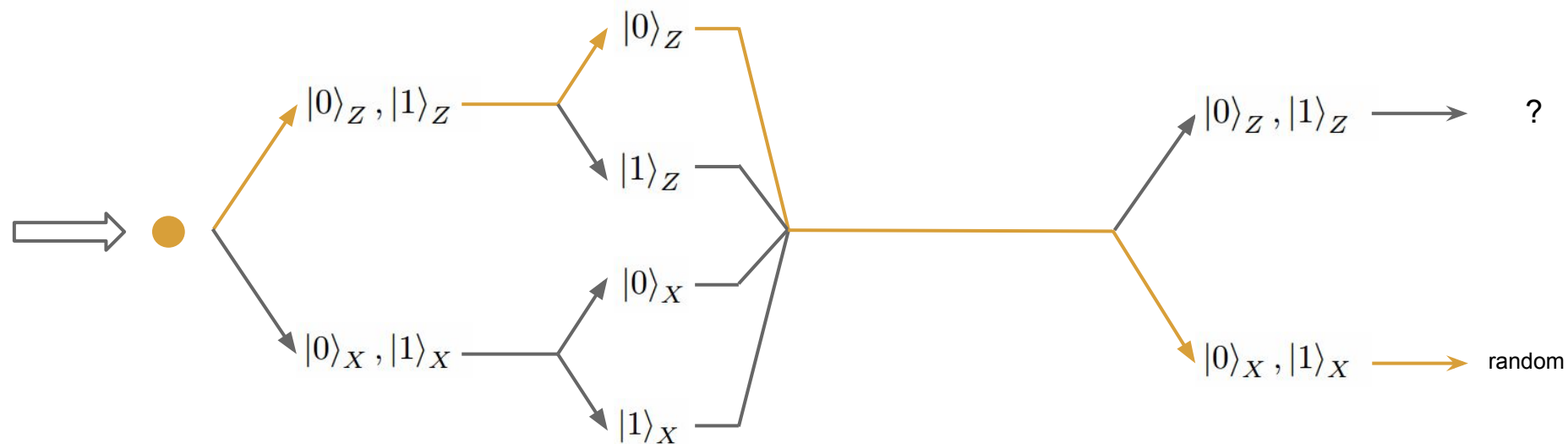
2. Prepare in random
state

3. Transmit through Quantum
Channel

Bob

4. Randomly choose
basis

5. Measure



BB84 (Procedure)

Single
Particle
Source

Alice

1. Randomly choose
basis

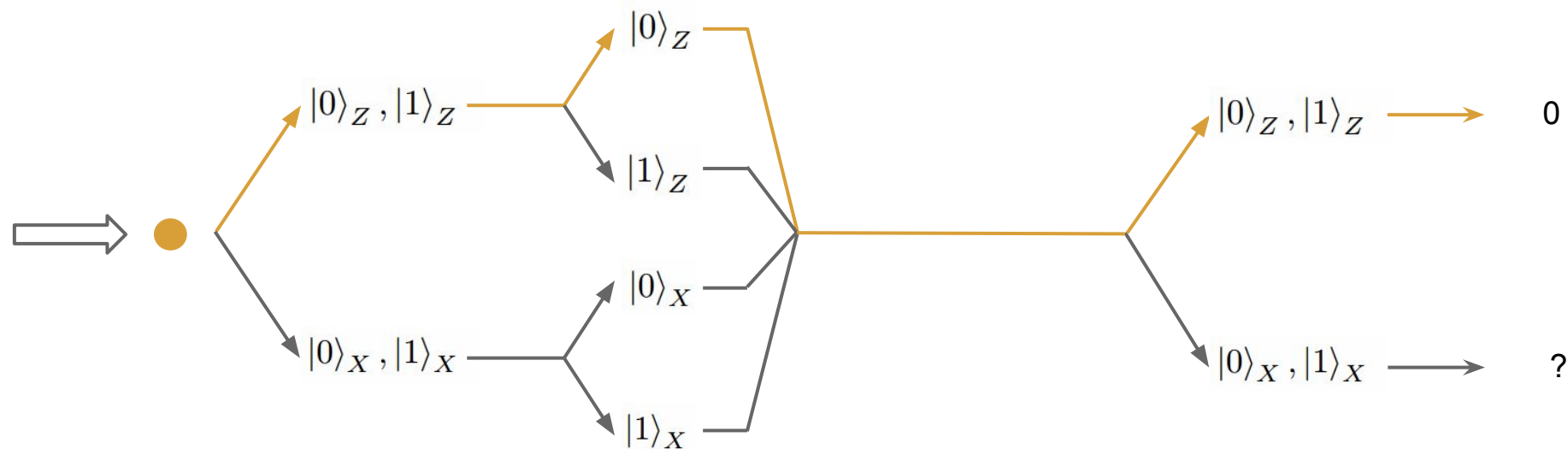
2. Prepare in random
state

3. Transmit through Quantum
Channel

Bob

4. Randomly choose
basis

5. Measure



BB84 (Procedure)

Single
Particle
Source

Alice

1. Randomly choose
basis

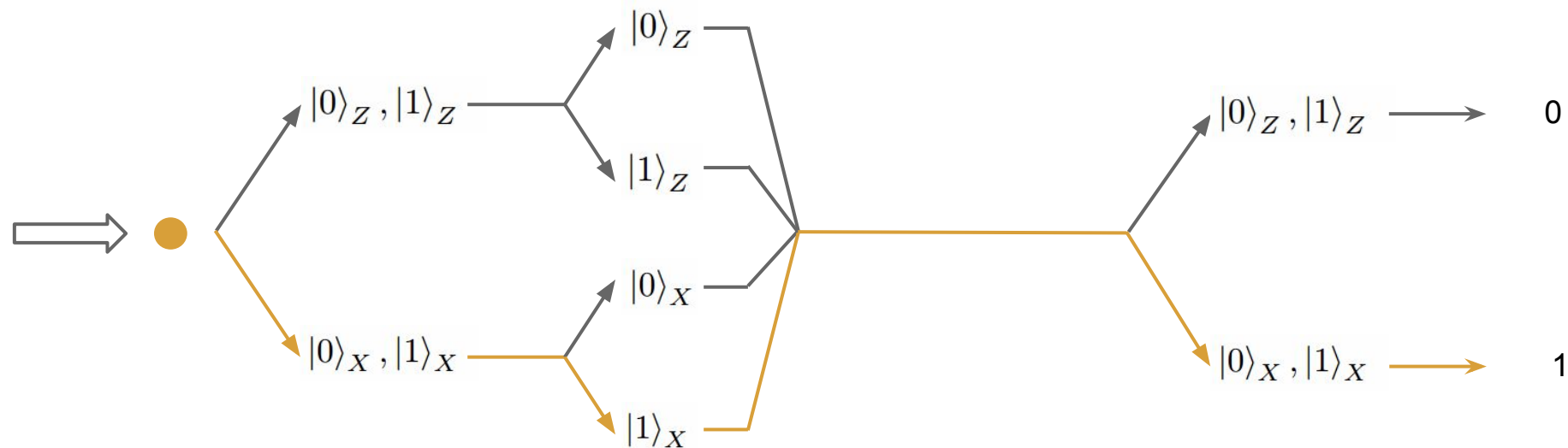
2. Prepare in random
state

3. Transmit through Quantum
Channel

Bob

4. Randomly choose
basis

5. Measure



BB84 (Procedure)

Single
Particle
Source

Alice

1. Randomly choose
basis

2. Prepare in random
state

3. Transmit through Quantum
Channel

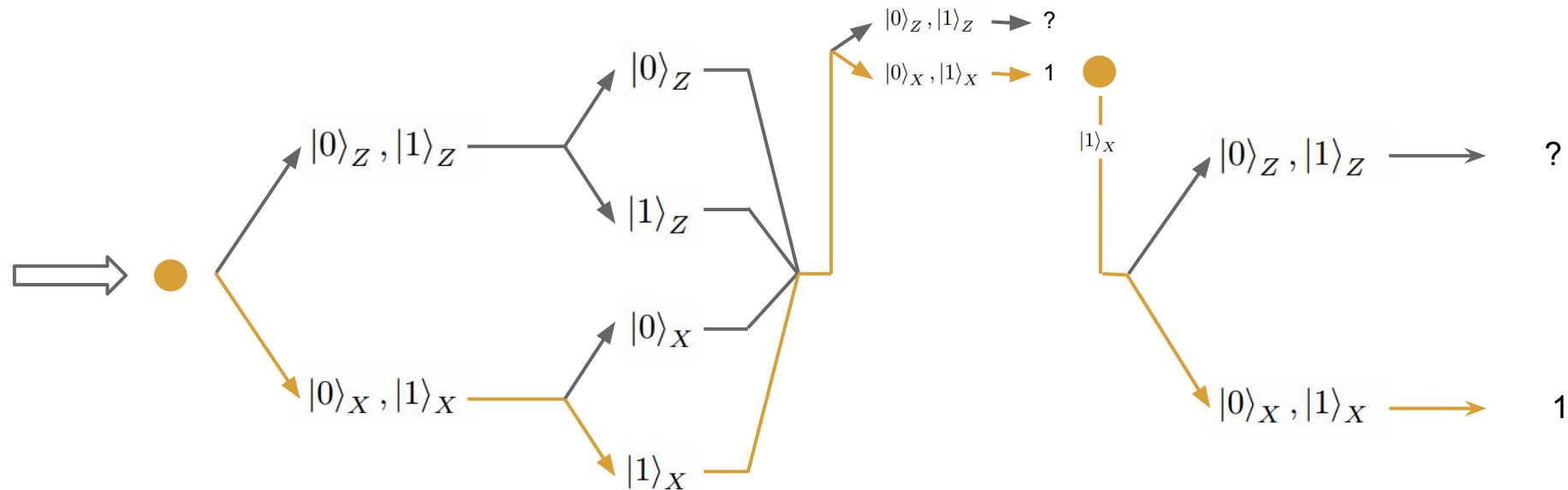
Bob

4. Randomly choose
basis

5. Measure

Eve

Measure and re-
prepare



BB84 (Procedure)

Single
Particle
Source

Alice

1. Randomly choose
basis

2. Prepare in random
state

3. Transmit to Bob through
Quantum Channel

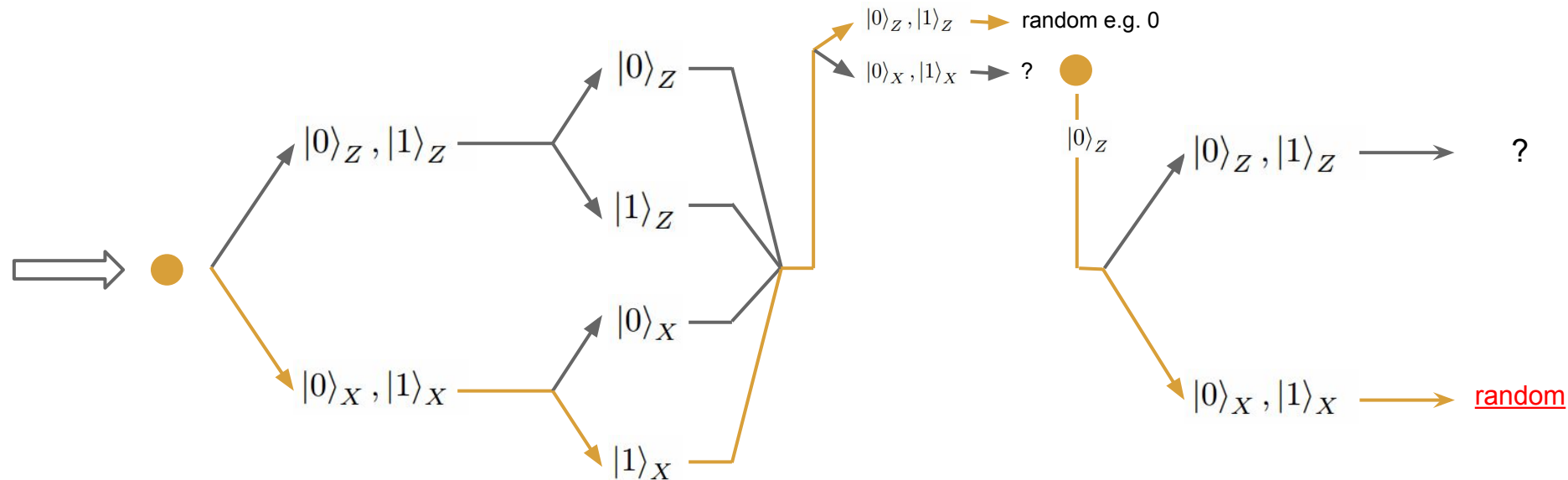
Bob

4. Randomly choose
basis

5. Measure

Eve

Measure, re-prepare,
transmit to Bob



BB84 (Procedure)

Single
Particle
Source

Alice

1. Randomly choose
basis

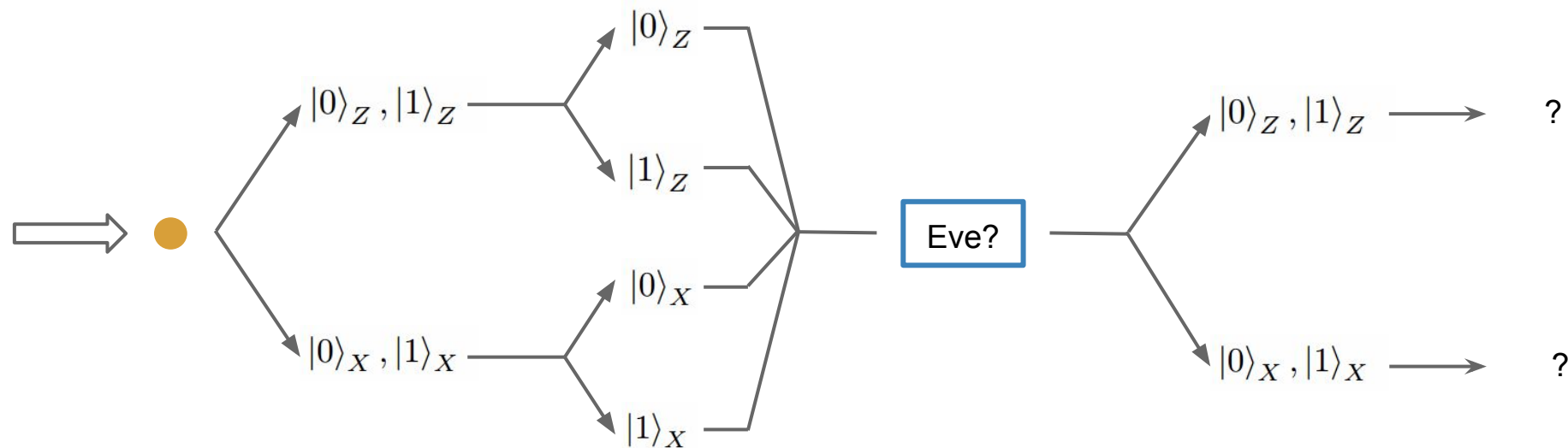
2. Prepare in random
state

3. Transmit through Quantum
Channel

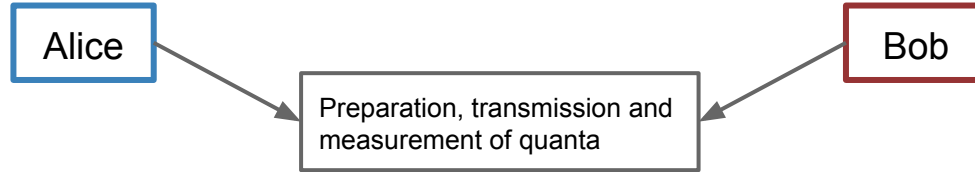
Bob

4. Randomly choose
basis

5. Measure



BB84 (Procedure)

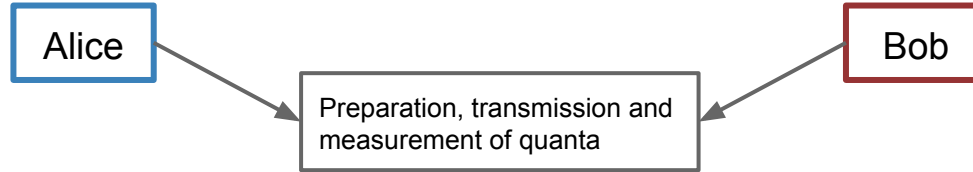


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical
Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

BB84 (Procedure)

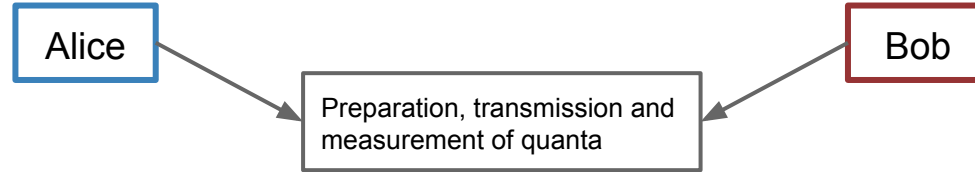


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical
Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

BB84 (Procedure)

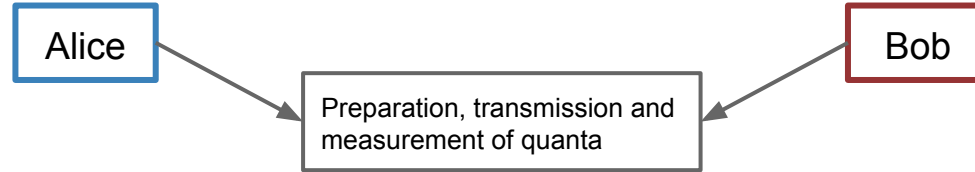


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical
Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

BB84 (Procedure)



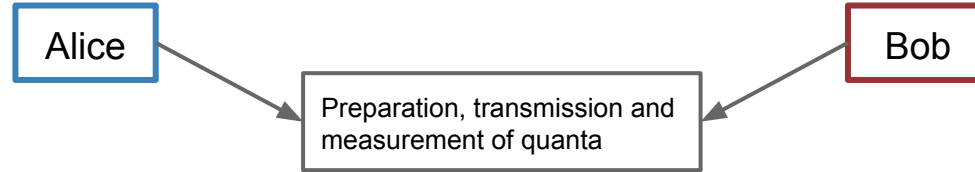
Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

The diagram illustrates the BB84 procedure. It shows two tables representing the quantum states and classical bits for Alice and Bob. The first table (Alice's) has a blue border and the second table (Bob's) has a red border. A double-headed arrow labeled 'Classical Channel' connects the two tables. In the Alice table, the first three columns (Z, Z, X) and the corresponding classical bits (0, 1, 1) are highlighted in blue. In the Bob table, the first three columns (X, Z, X) and the corresponding classical bits (1, 1, 1) are highlighted in blue. This indicates that they have used the same basis for those three bits.

BB84 (Procedure)



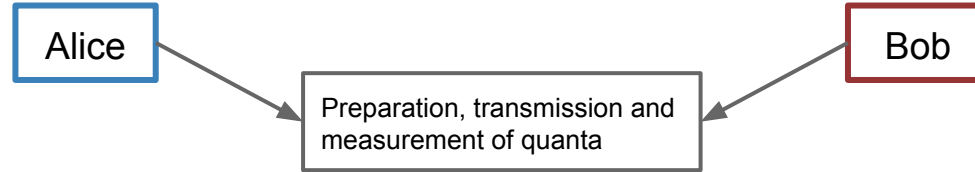
Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

The diagram illustrates the BB84 procedure. It shows two tables representing the quantum states and classical bits for Alice and Bob. The first table (Alice's) has a blue border and the second table (Bob's) has a red border. A double-headed arrow labeled 'Classical Channel' connects the two tables. In the first table, the first four columns (Z, Z, X, Z) are highlighted in blue, and the corresponding classical bits (0, 1, 1, 1) are also in blue. In the second table, the first four columns (X, Z, X, X) are highlighted in blue, and the corresponding classical bits (1, 1, 1, 1) are also in blue. This indicates that Alice and Bob have used the same basis for the first four bits.

BB84 (Procedure)



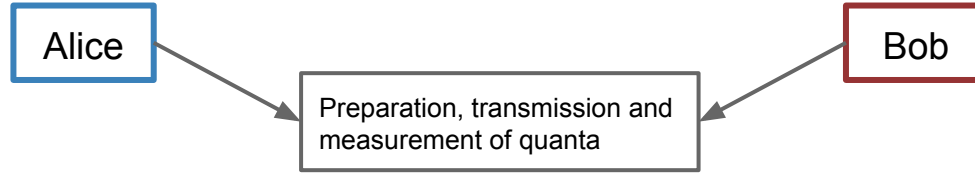
Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

The diagram illustrates the BB84 procedure. It shows two tables representing the quantum states and classical bits for Alice and Bob. The first table (Alice's) has a blue border and the second table (Bob's) has a red border. A double-headed arrow labeled 'Classical Channel' connects the two tables. In both tables, the first four columns are shaded blue, indicating successful measurements, while the remaining columns are white, indicating failed measurements.

BB84 (Procedure)



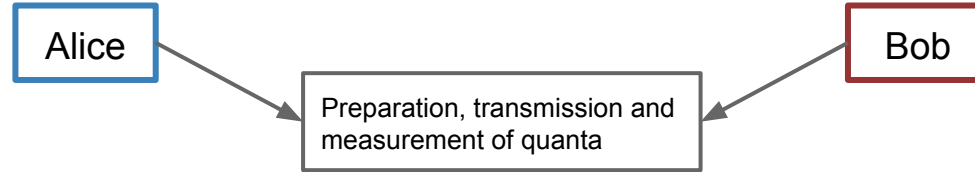
Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

The diagram illustrates the BB84 procedure. It shows two tables representing the quantum states and classical bits for Alice and Bob. The first table (Alice's) has a blue border and the second table (Bob's) has a red border. A double-headed arrow labeled 'Classical Channel' connects the two tables. The tables show the sequence of bases (Z or X) and the corresponding classical bits (0 or 1) for each quanta.

BB84 (Procedure)



Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

The diagram illustrates the BB84 procedure. It shows two tables representing the quantum states and classical bits exchanged between Alice and Bob. The first table (Alice's) has a red highlight on the 7th column (X, 0). The second table (Bob's) has a red highlight on the 7th column (X, 1). A double-headed arrow labeled 'Classical Channel' connects the two tables.

BB84 (Procedure)

Alice

Bob

Preparation, transmission and measurement of quanta

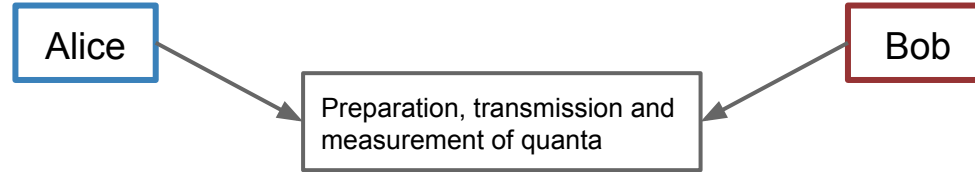
Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	1	0	0	...

Presence of Eve proven, start a physical search

Start over

BB84 (Procedure)

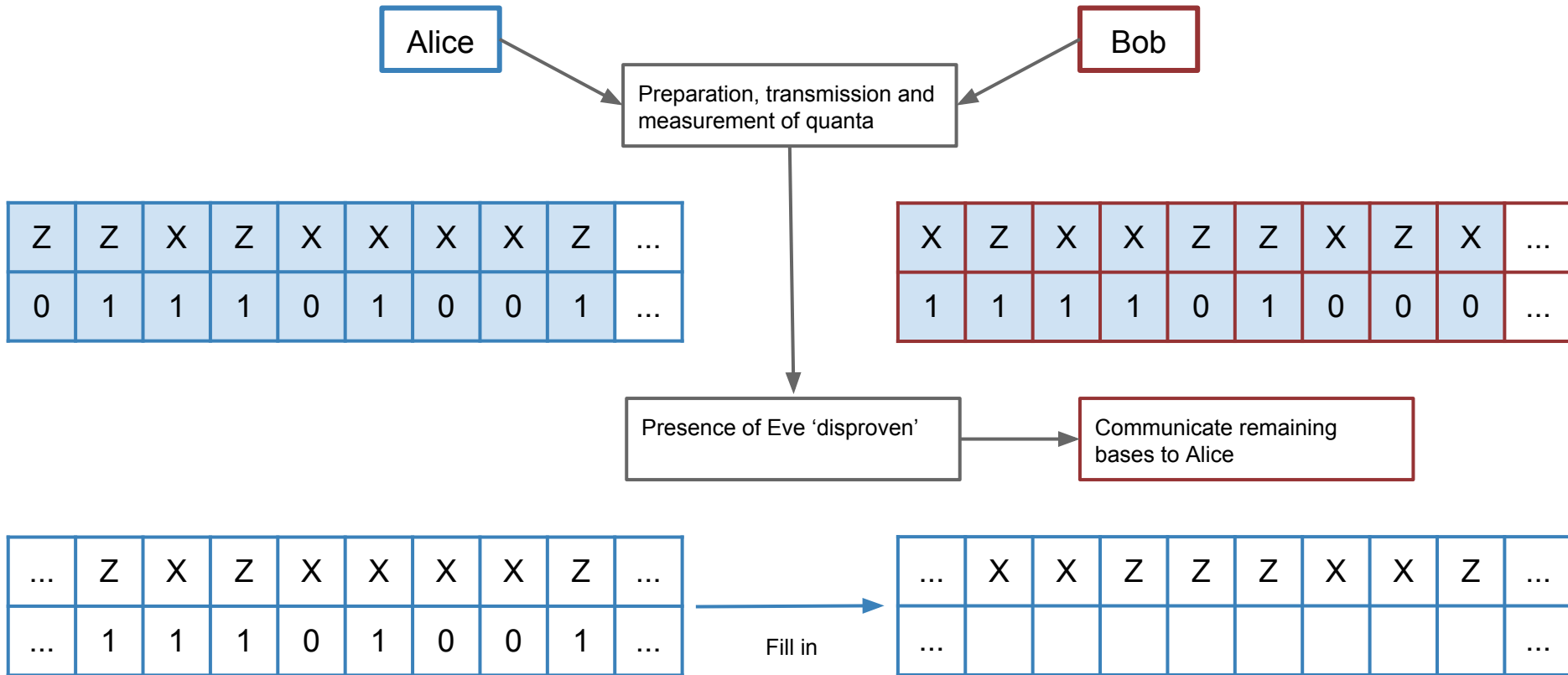


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	0	0	0	...

BB84 (Procedure)



BB84 (Procedure)

Alice

Bob

Preparation, transmission and
measurement of quanta

Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	0	0	0	...

Presence of Eve 'disproven'

Communicate remaining
bases to Alice

...	Z	X	Z	X	X	X	X	Z	...
...	1	1	1	0	1	0	0	1	...

Fill in

...	X	X	Z	Z	Z	X	X	Z	...
...	?								...

BB84 (Procedure)

Alice

Bob

Preparation, transmission and measurement of quanta

Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	0	0	0	...

Presence of Eve 'disproven'

Communicate remaining bases to Alice

...	Z	X	Z	X	X	X	X	Z	...
...	1	1	1	0	1	0	0	1	...

Fill in

...	X	X	Z	Z	Z	X	X	Z	...
...	?	1							...

BB84 (Procedure)

Alice

Bob

Preparation, transmission and measurement of quanta

Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	0	0	0	...

Presence of Eve 'disproven'

Communicate remaining bases to Alice

...	Z	X	Z	X	X	X	X	Z	...
...	1	1	1	0	1	0	0	1	...

Fill in

...	X	X	Z	Z	Z	X	X	Z	...
...	?	1	1						...

BB84 (Procedure)

Alice

Bob

Preparation, transmission and measurement of quanta

Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

X	Z	X	X	Z	Z	X	Z	X	...
1	1	1	1	0	1	0	0	0	...

Communicate which measurements form key

Presence of Eve 'disproven'

Communicate remaining bases to Alice

...	Z	X	Z	X	X	X	X	Z	...
...	1	1	1	0	1	0	0	1	...

Fill in

...	X	X	Z	Z	Z	X	X	Z	...
...	?	1	1	?	?	0	0	1	...

Questions?