Quantum Cryptography

Christian Klumpp

christian.klumpp@yale.edu

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

SHANGHAI

2010 2011 2012 2013 2014

HEIDELBERG

YALE

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

SHANGHAI

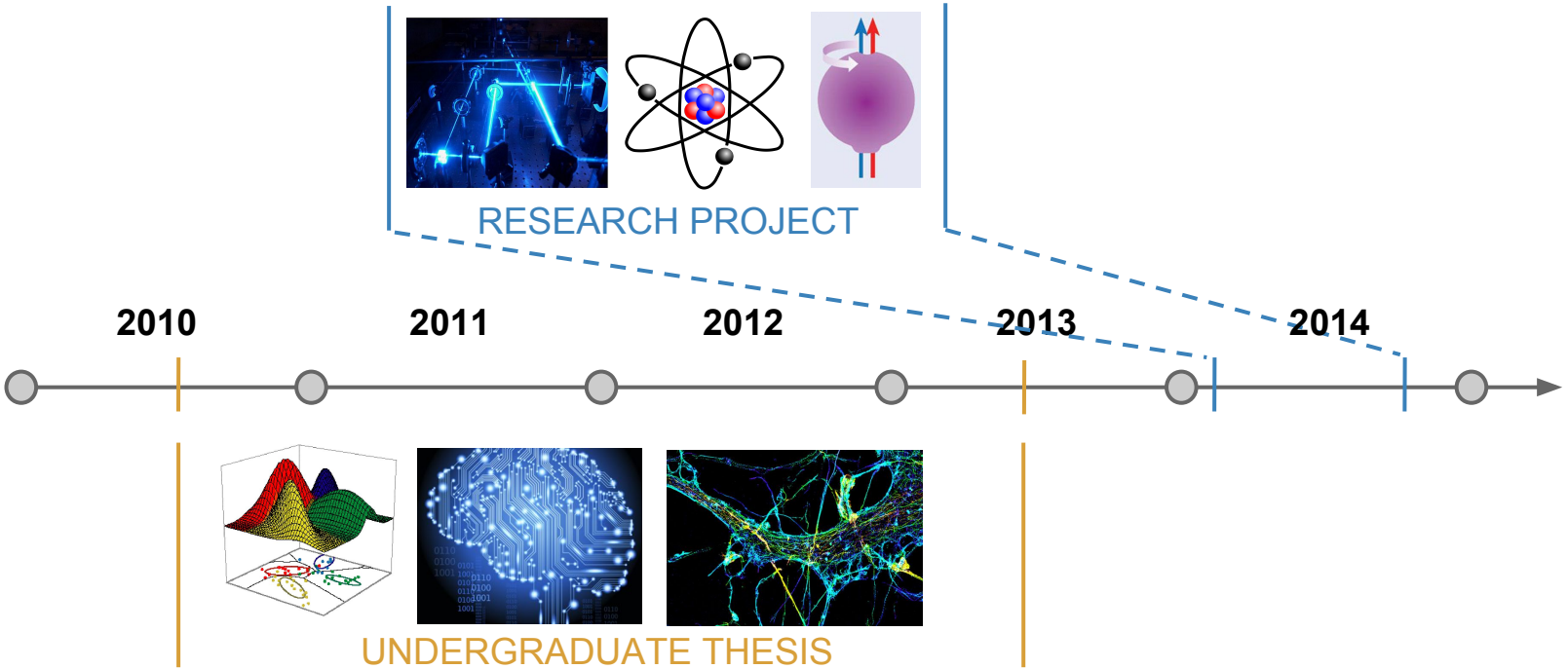
ZÜRICH

2010 2011 2012 2013 2014 ...

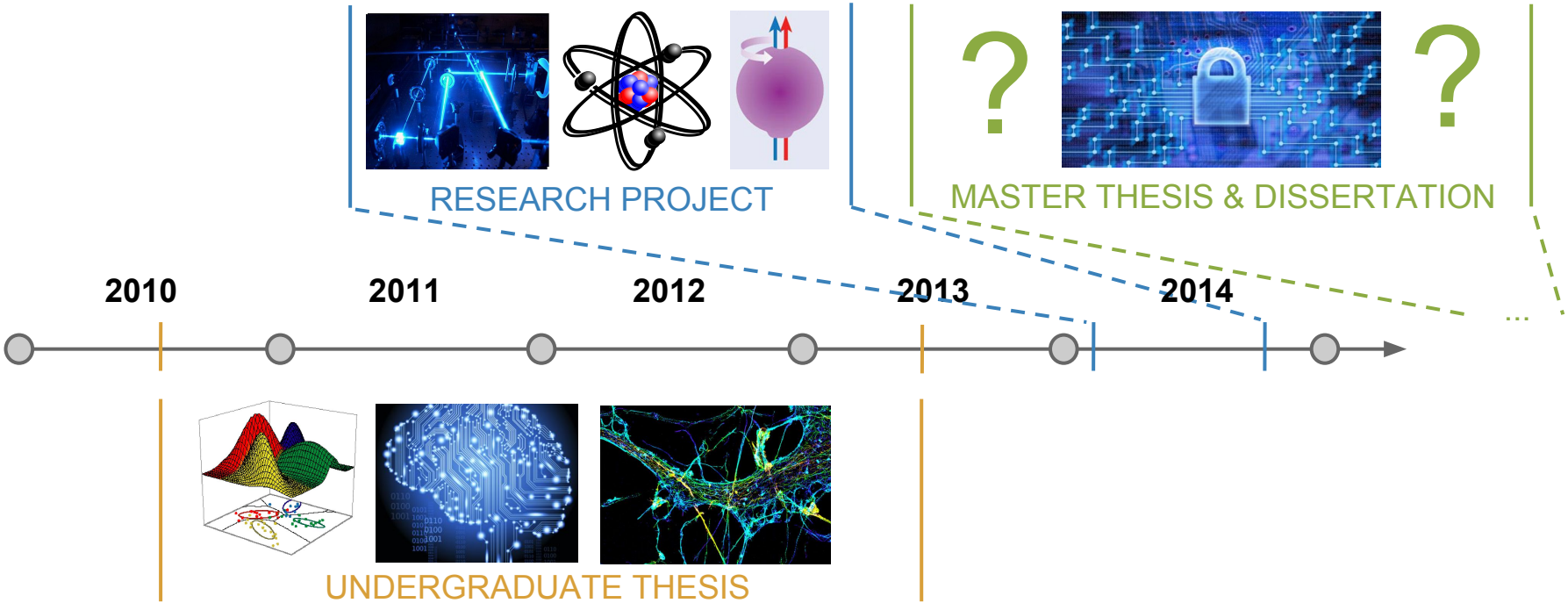
HEIDELBERG

YALE

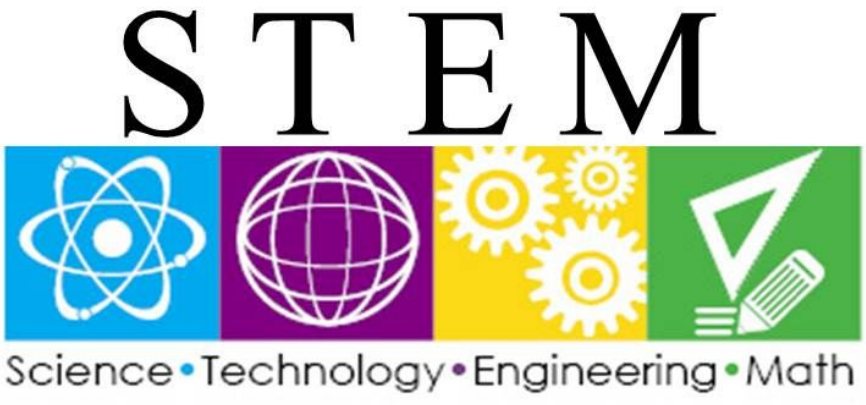
Quantum Physics, Computer Science...



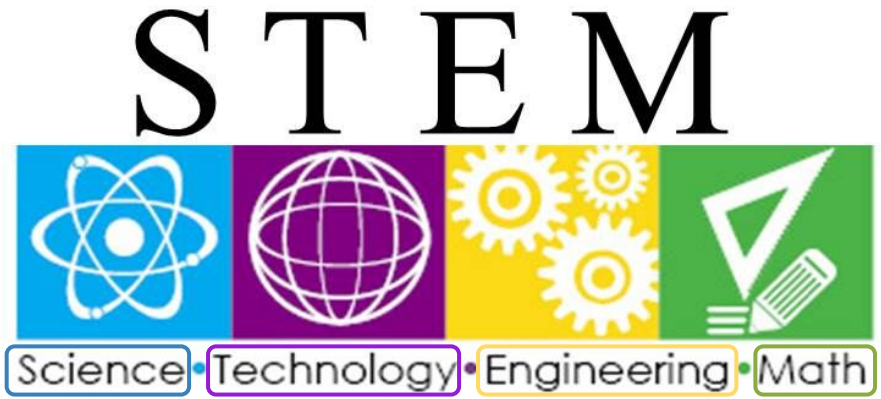
...and what combines them…



Why it matters...



Why it matters...

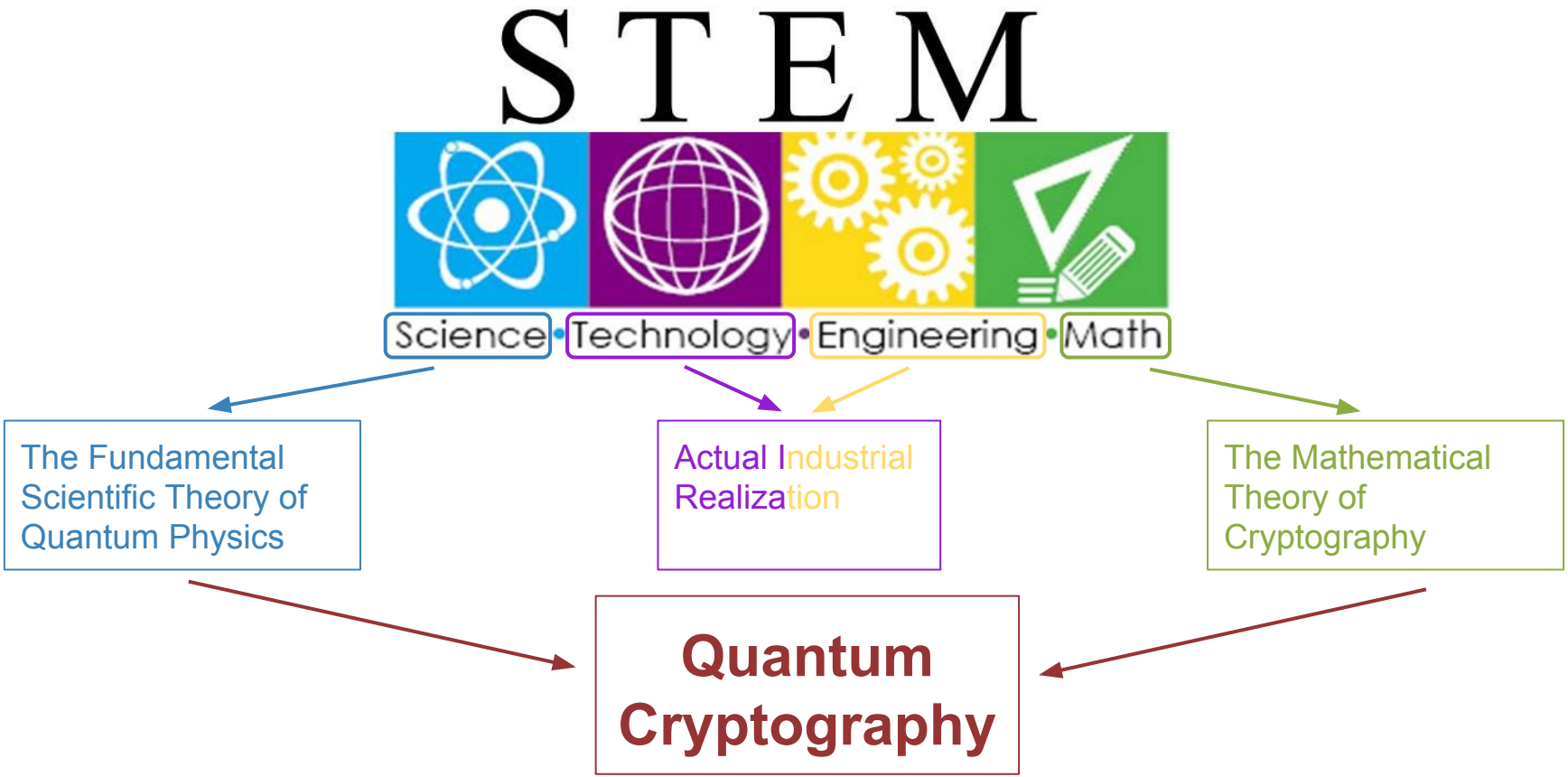


The Fundamental Scientific Theory of Quantum Physics

Actual Industrial Realization

The Mathematical Theory of Cryptography

Why it matters...



As old as Human Civilization…

A Simple Idea with Great Success...

The unbreakable code...?

Great Trust in Great Numbers...

$$7.900145545423399285584324530571736563179841032857918045046505453908448\ldots$$
$$5426968647539680599935090250504812051663847123817924937053333515046 7\ldots$$
$$6975763203396201383045597066441728784159136275530718503080907275591 8\ldots$$
$$5549144580436231548074729822880386143197342053790072363423558775445 3\ldots$$
$$8850375291988505743288233717213756285675166930647017378512046321423 2\ldots$$
$$2824183171737236104129727582838516040776620450428895881884804524344 4\ldots$$
$$5072509637497261512320145562146129637071768750280259636735642707563 3\ldots$$
$$1062681373488505308256938807093603614823055115746399102812059677174 7\ldots$$
$$2898916797174950057486369481247964995632172943276116145983847928928 0\ldots$$
$$6090288552980453975870071724483000413595005267580487478719004443920 5\ldots$$
$$4614283252252401165384718886807984101161505300691986838118236158687 8\ldots$$
$$8405326330804065442894441103684623554416899609221979041702698329042 9\ldots$$
$$6872910778263580385873219898467524898416717576353518681201111263006 9\ldots$$
$$5721395186942906550722439260278962847910605294618092571166923685004 9\ldots$$
$$35014828945\ldots \times 10^{77631168}$$

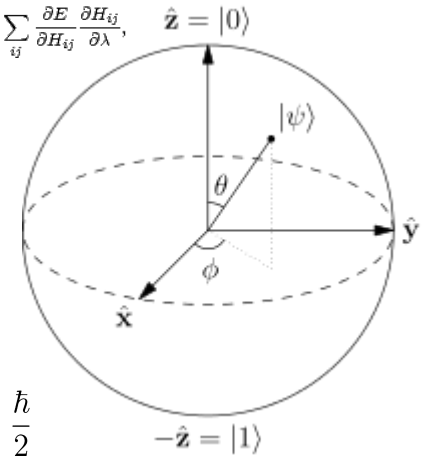
What Quantum Physics taketh away...

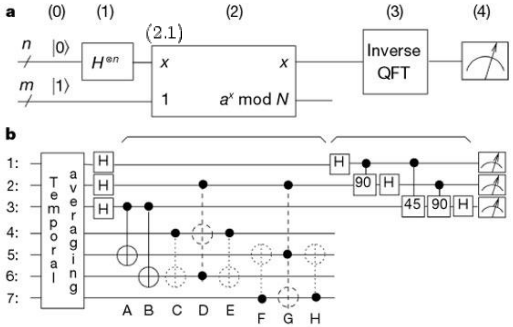
$$E = Tr[\rho H] = \sum_{ij} \rho_{ij} H_{ji},$$

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

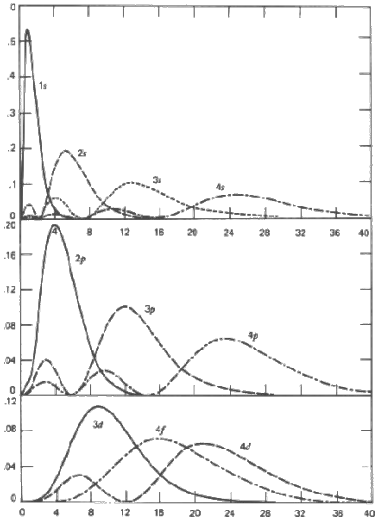
$$H(t)|\psi(t)\rangle = i\hbar \frac{\partial}{\partial t}|\psi(t)\rangle$$

$$|\Psi\rangle = c_1|\uparrow\rangle + c_2|\downarrow\rangle$$





$$H = \hbar\omega\left(A^\dagger A + \frac{1}{2}\right)$$



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

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

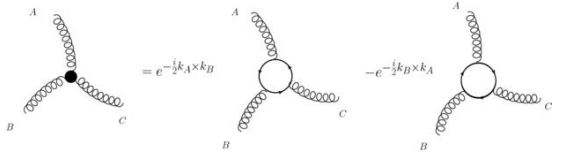
$$\sigma_z = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

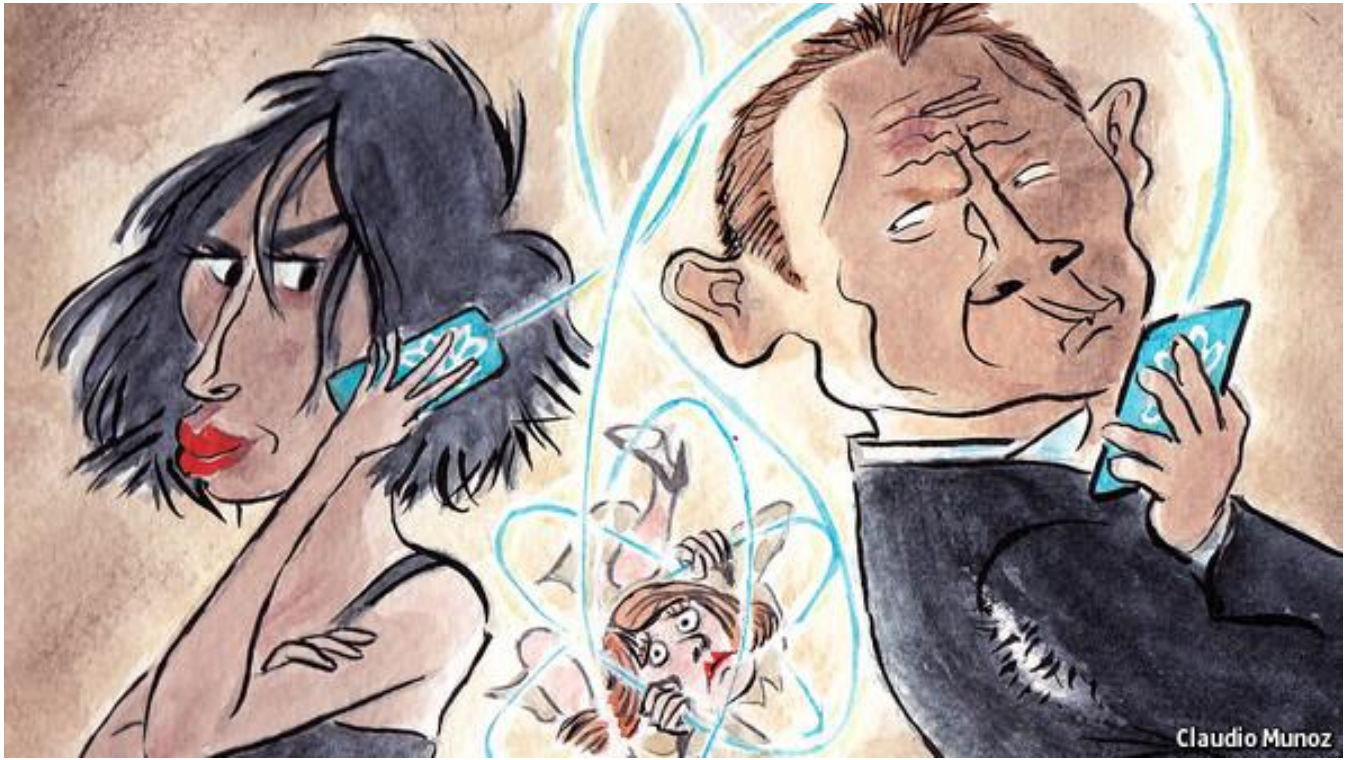
$$\frac{d}{dt}A(t) = \frac{i}{\hbar}[H, A(t)] + e^{iHt/\hbar}\left(\frac{\partial A}{\partial t}\right)e^{-iHt/\hbar},$$

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

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



… Quantum Physics bringeth back



CHAPTER 1
A brief Introduction to One-Time-Pads

Truly unbreakable...

Binary Addition

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

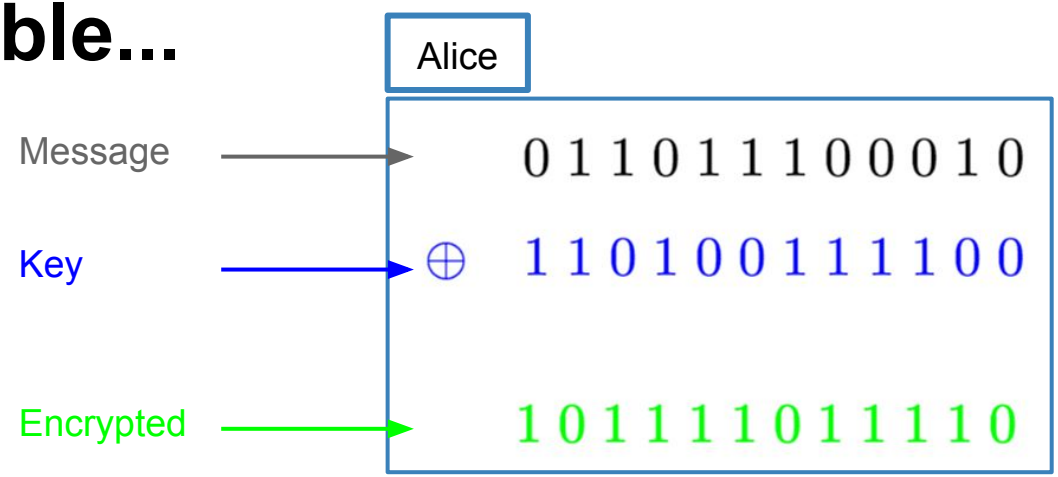
$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Truly unbreakable...

Binary Addition

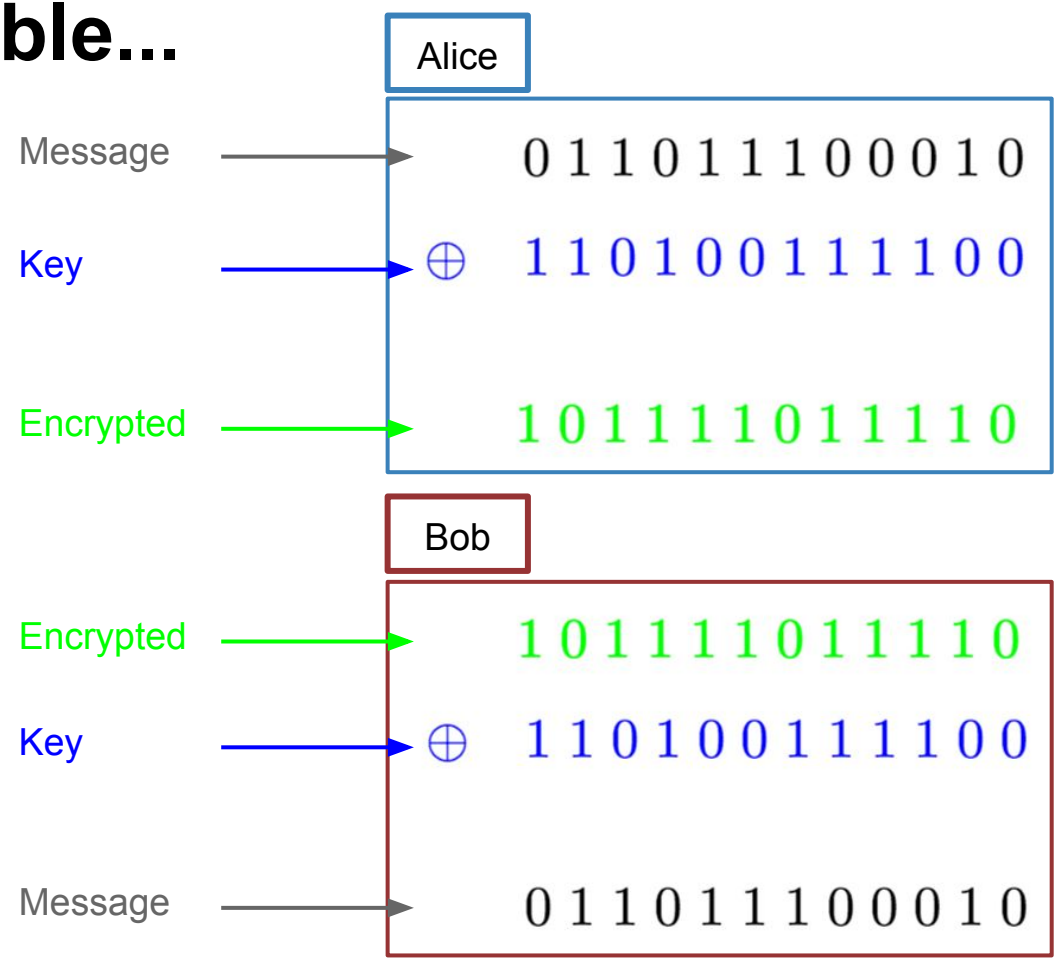
$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$



Truly unbreakable...

Binary Addition

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$



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

CHAPTER 2
A brief Introduction to Quantum Physics

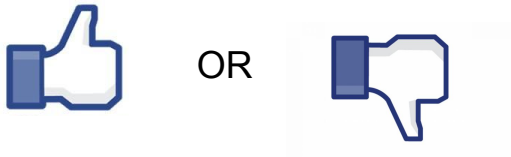
Superpositions, the first weird thing…

Classical Physics

OR

Superpositions, the first weird thing…

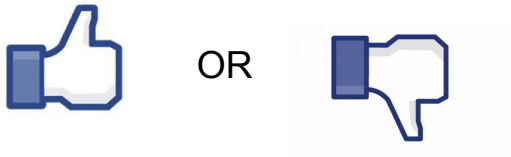
Classical Physics



Quantum Physics

Superpositions, the first weird thing…

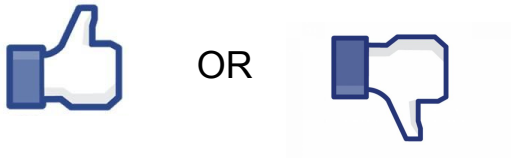
Classical Physics



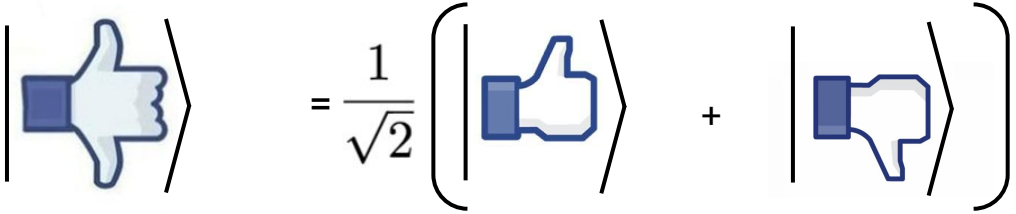
Quantum Physics

Superpositions, the first weird thing…

Classical Physics

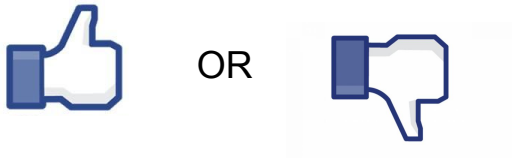


Quantum Physics



Superpositions, the first weird thing…

Classical Physics

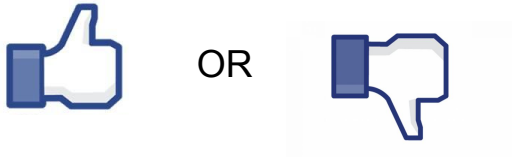


Quantum Physics

$$\left|\text{👍}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\text{👍}\right\rangle + \left|\text{👎}\right\rangle\right)$$

Superpositions, the first weird thing…

Classical Physics



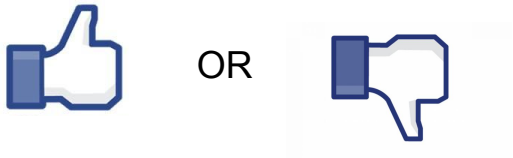
Quantum Physics

$$\left|\text{👍}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\text{👍}\right\rangle + \left|\text{👎}\right\rangle\right)$$

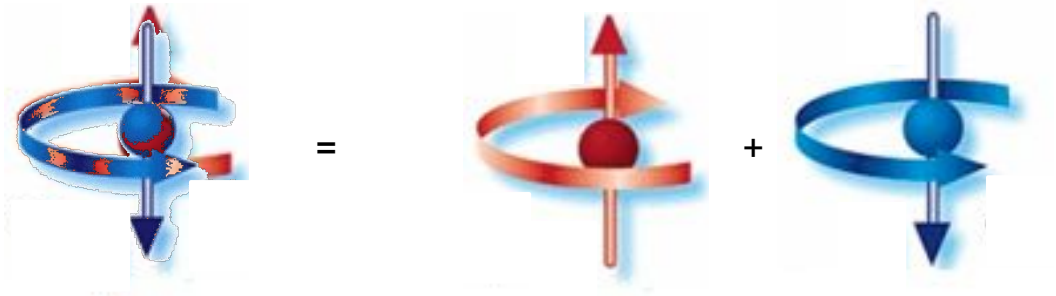
$$\left|\text{⟳}\right\rangle = \frac{1}{\sqrt{2}}\left[\left|\text{⟳}\right\rangle + \left|\text{⟲}\right\rangle\right]$$

Superpositions, the first weird thing…

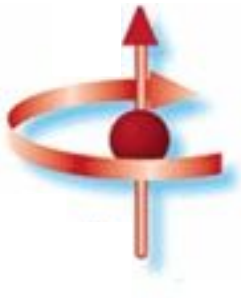
Classical Physics



Quantum Physics



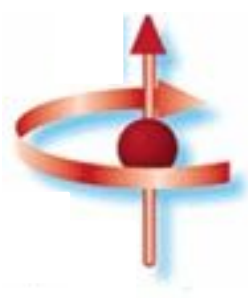
The Spin, as ‘Quantum’ as it gets...



‘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’ ‘Spin Down’

$|\uparrow\rangle$ $|\downarrow\rangle$

Superposition $= \frac{1}{\sqrt{2}}$ (‘Spin Up’ + ‘Spin Down’)

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

The Spin, as ‘Quantum’ as it gets...

‘Spin Up’ ‘Spin Down’

$$|\uparrow\rangle \qquad |\downarrow\rangle$$

$$|0\rangle \qquad |1\rangle$$

Superposition $= \frac{1}{\sqrt{2}}$ (‘Spin Up’ + ‘Spin Down’)

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

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

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

Measurements, the second weird thing...

Mark has full control
over Quantum Physics

Measurements, the second weird thing...

Mark has full control
over Quantum Physics

Chris Klumpp
Just now · New Haven, CT

Today is a beautiful day.

Read Notification

50%

Mark Santolucito
likes your post.

50%

Mark Santolucito
dislikes your post.

Measurements, the second weird thing...

Mark has full control
over Quantum Physics

Chris Klumpp
Just now · New Haven, CT

Today is a beautiful day.

Read Notification

50%

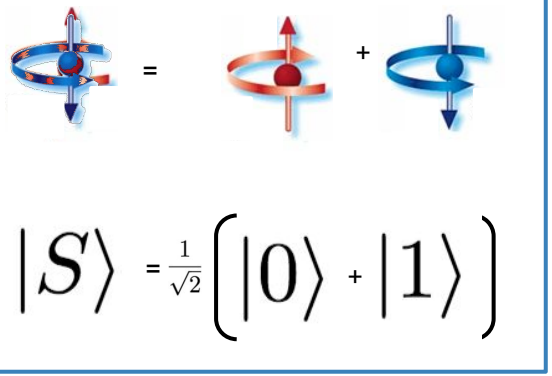
50%

Mark Santolucito
likes your post.

Mark Santolucito
dislikes your post.

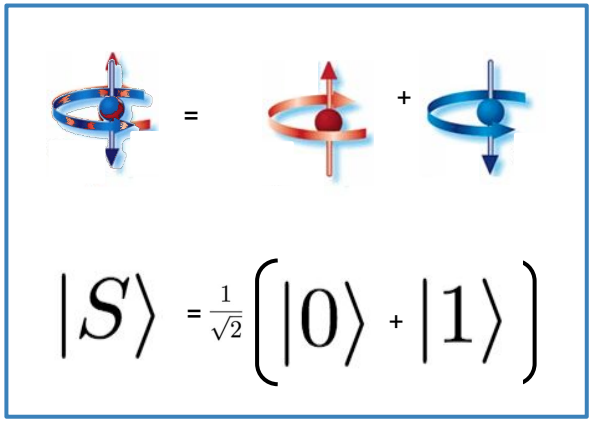
MEASUREMENT

Measurements, the second weird thing...



MEASUREMENT

Measurements, the second weird thing...

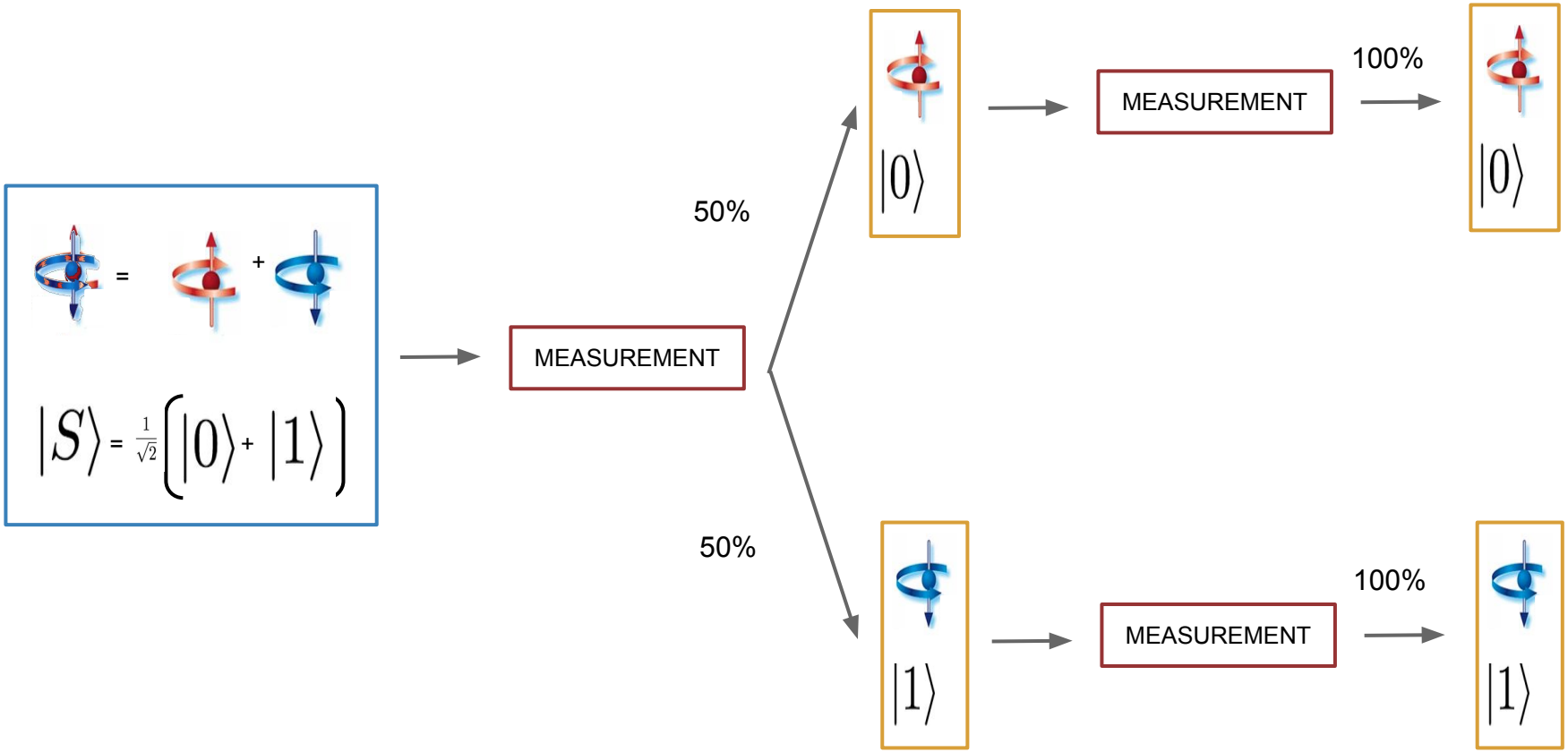


MEASUREMENT

50%

50%

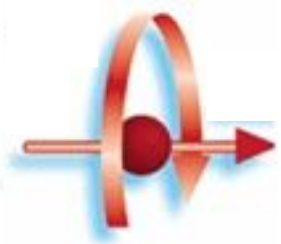
Measurements, the second weird thing...



It just gets a tiny bit weirder...

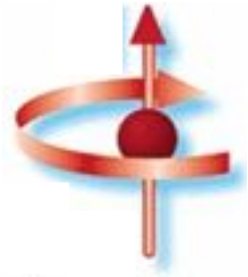
Particles can ‘spin’ in different directions...

$|1\rangle_X$



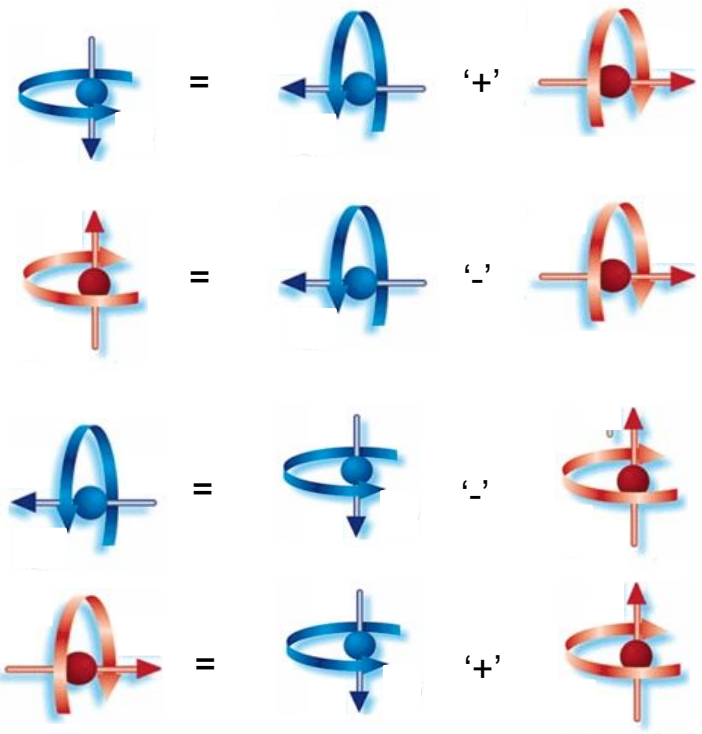
$|0\rangle_X$

$|1\rangle_Z$



$|0\rangle_Z$

It just gets a tiny bit weirder...



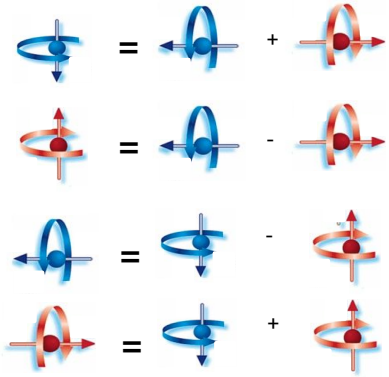
$$|0\rangle_Z = \frac{1}{\sqrt{2}}(|0\rangle_X + |1\rangle_X)$$

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

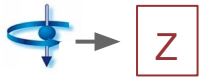
$$|0\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle_Z + |1\rangle_Z)$$

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

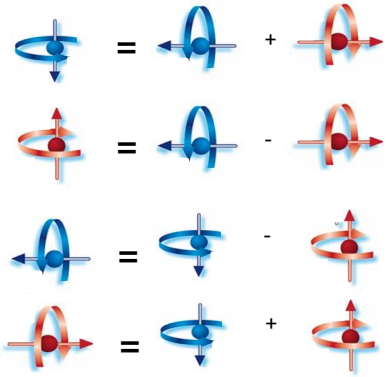
It just gets a tiny bit weirder...



SERIES OF MEASUREMENTS

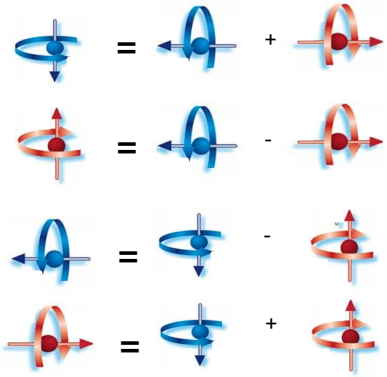


It just gets a tiny bit weirder...

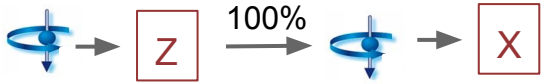


SERIES OF MEASUREMENTS

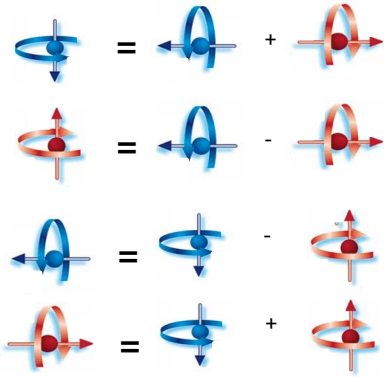
It just gets a tiny bit weirder...



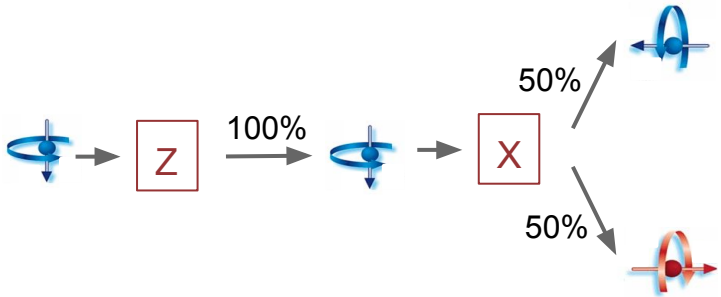
SERIES OF MEASUREMENTS



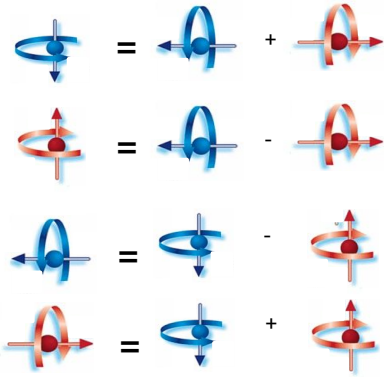
It just gets a tiny bit weirder...



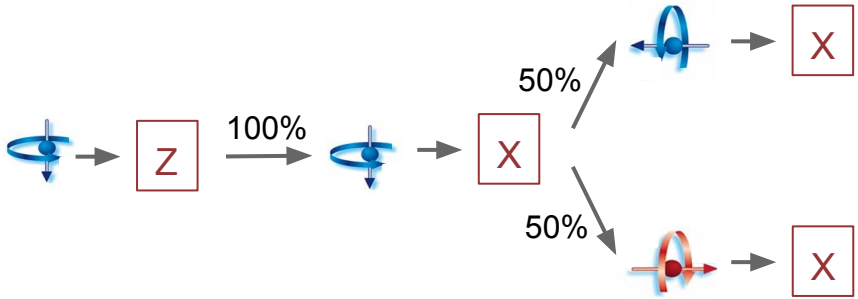
SERIES OF MEASUREMENTS



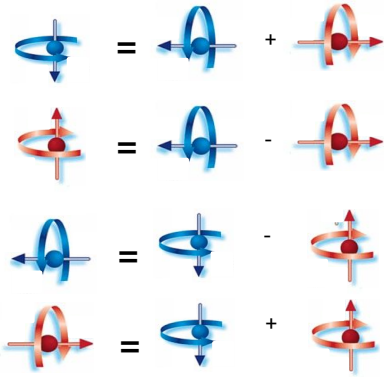
It just gets a tiny bit weirder...



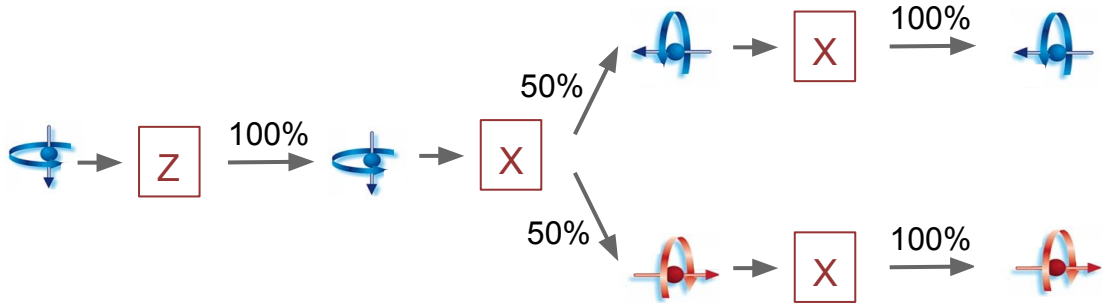
SERIES OF MEASUREMENTS



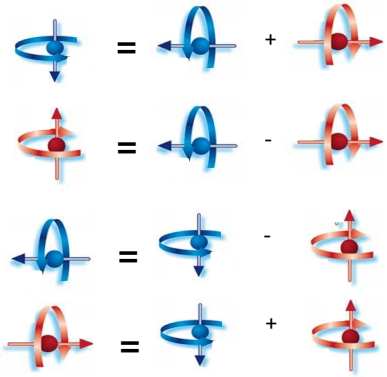
It just gets a tiny bit weirder...



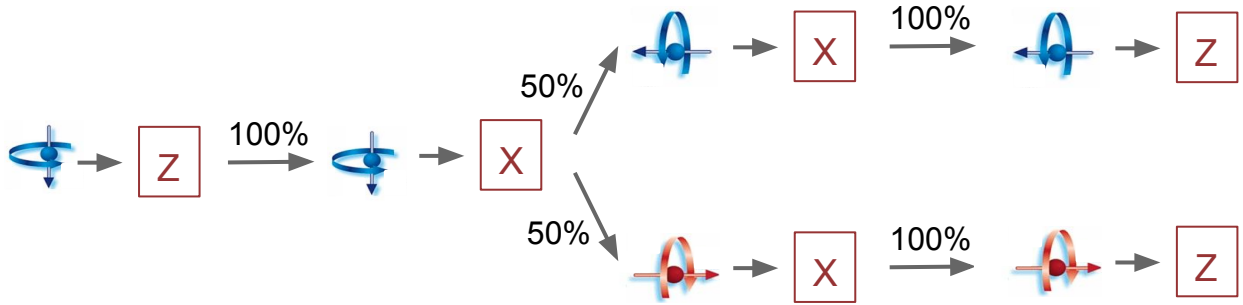
SERIES OF MEASUREMENTS



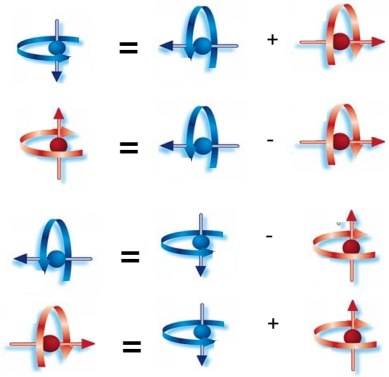
It just gets a tiny bit weirder...

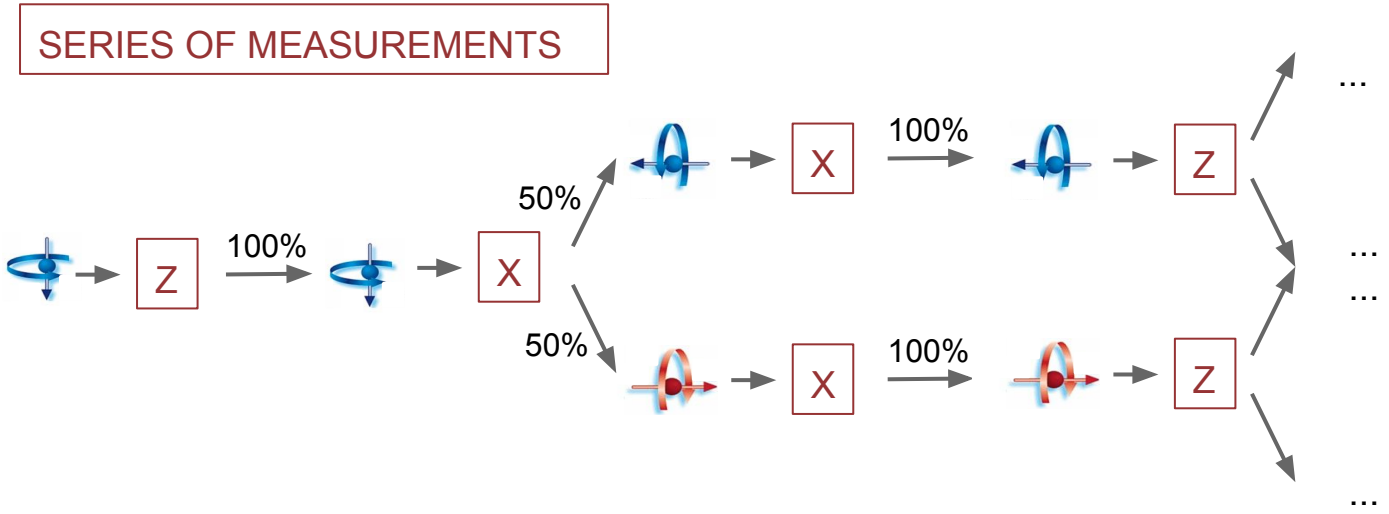


SERIES OF MEASUREMENTS

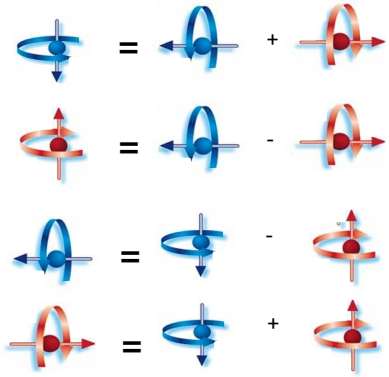


It just gets a tiny bit weirder...

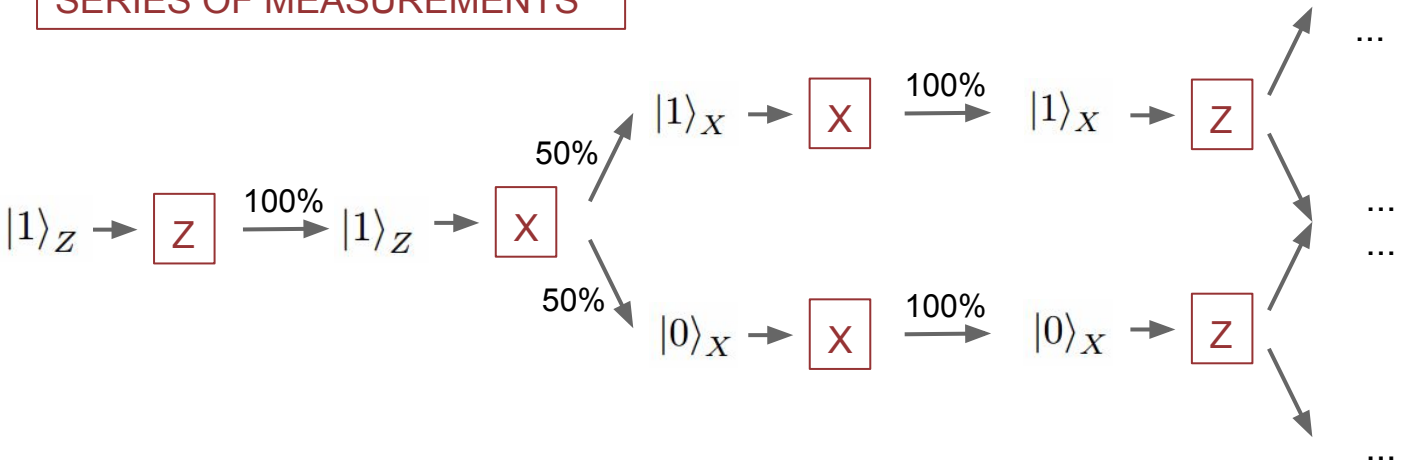




It just gets a tiny bit weirder...



SERIES OF MEASUREMENTS



That is it. That is all you need.

CHAPTER 3
Quantum Cryptography

BB84 Protocol (Idea)

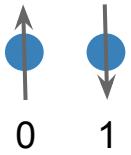
QuBits produced in two Bases

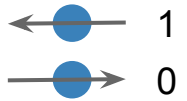
$$|0\rangle_Z, |1\rangle_Z \qquad |0\rangle_X, |1\rangle_X$$

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

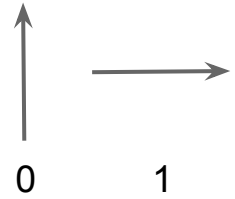
Possible Realizations

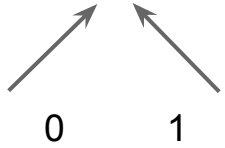
Electron Spins





Photon Polarizations (more convenient)





BB84 (Procedure)

Single Particle Source

Alice

1. Randomly choose basis

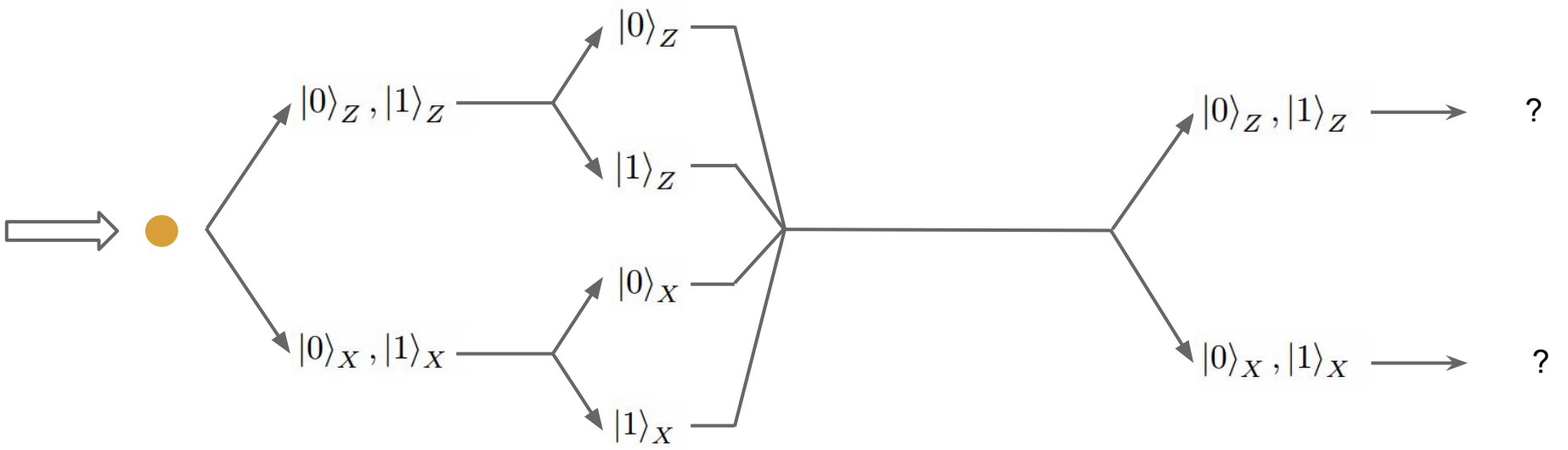
2. Prepare in random state

3. Transmit through Quantum Channel

Bob

4. Randomly choose basis

5. Measure



BB84 (Procedure)

Single Particle Source

Alice

1. Randomly choose basis

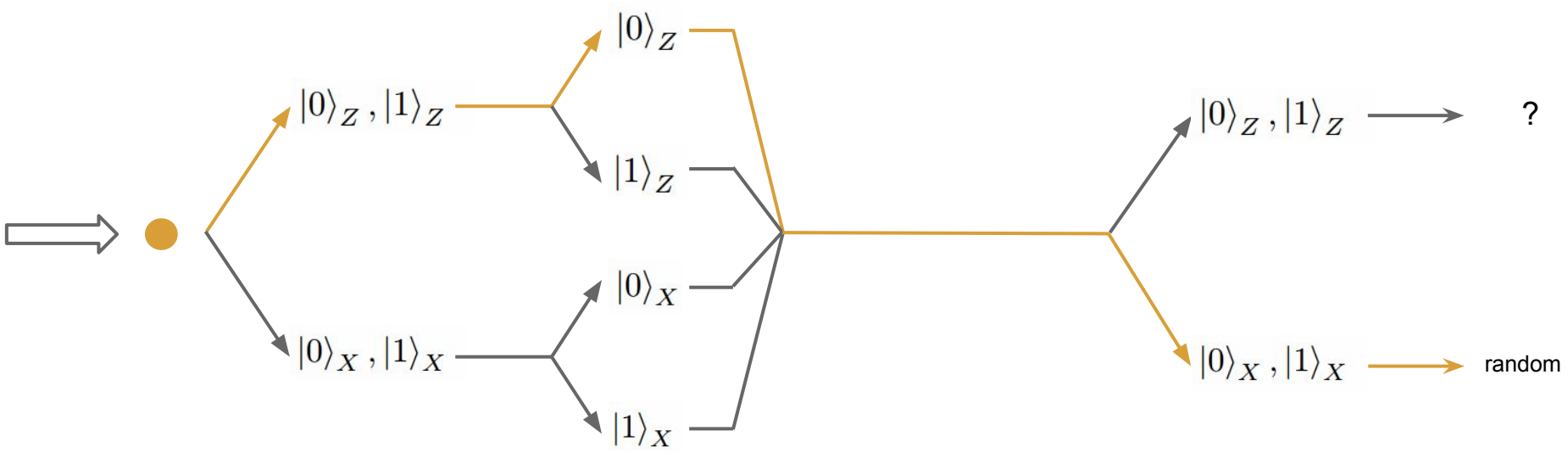
2. Prepare in random state

3. Transmit through Quantum Channel

Bob

4. Randomly choose basis

5. Measure



BB84 (Procedure)

Single Particle Source

Alice

1. Randomly choose basis

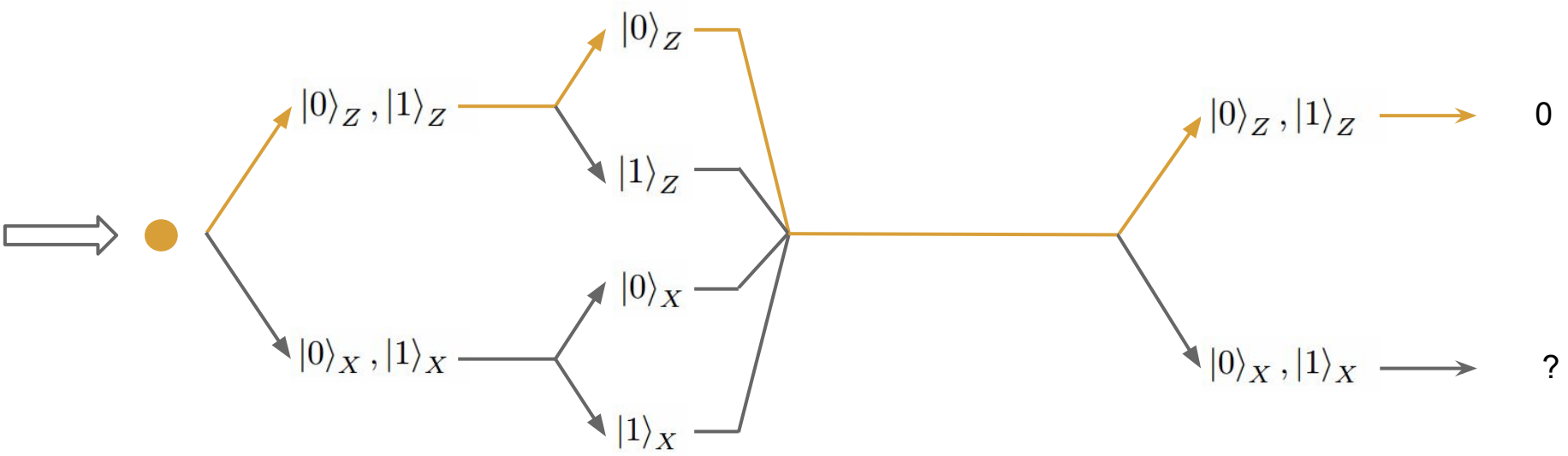
2. Prepare in random state

3. Transmit through Quantum Channel

Bob

4. Randomly choose basis

5. Measure



BB84 (Procedure)

Single Particle Source

Alice

1. Randomly choose basis

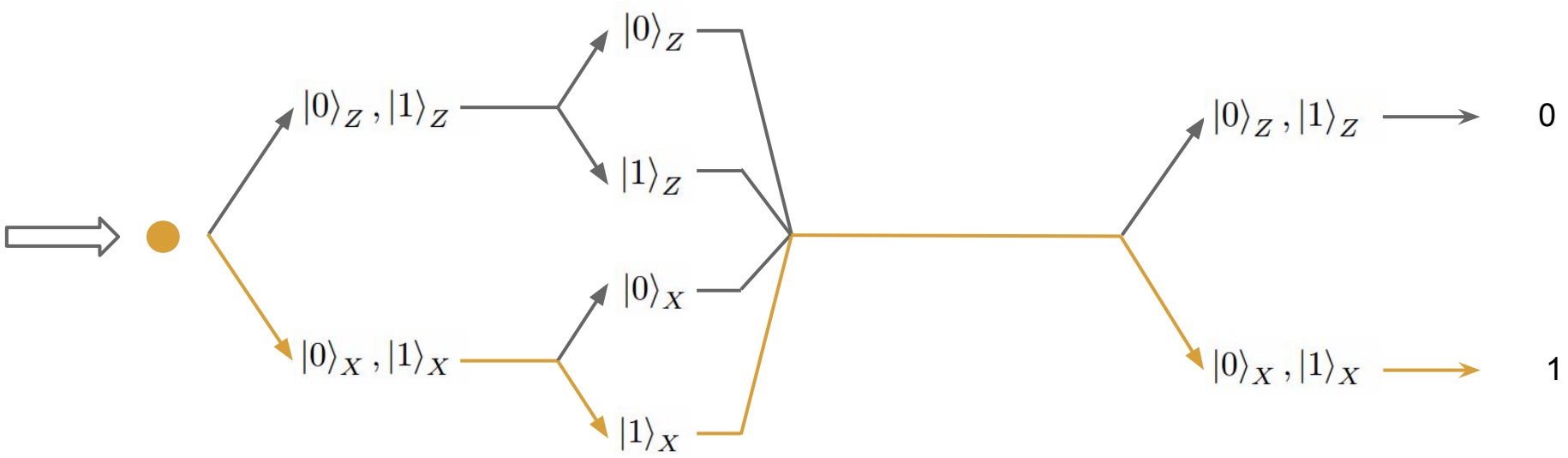
2. Prepare in random state

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

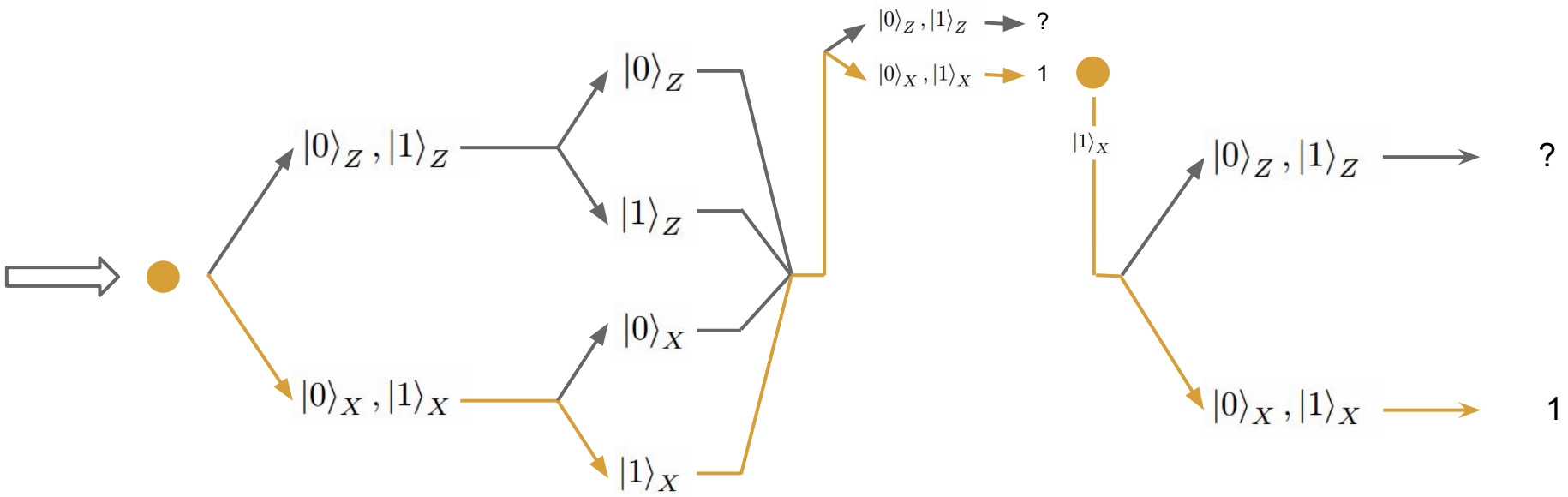
Bob

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

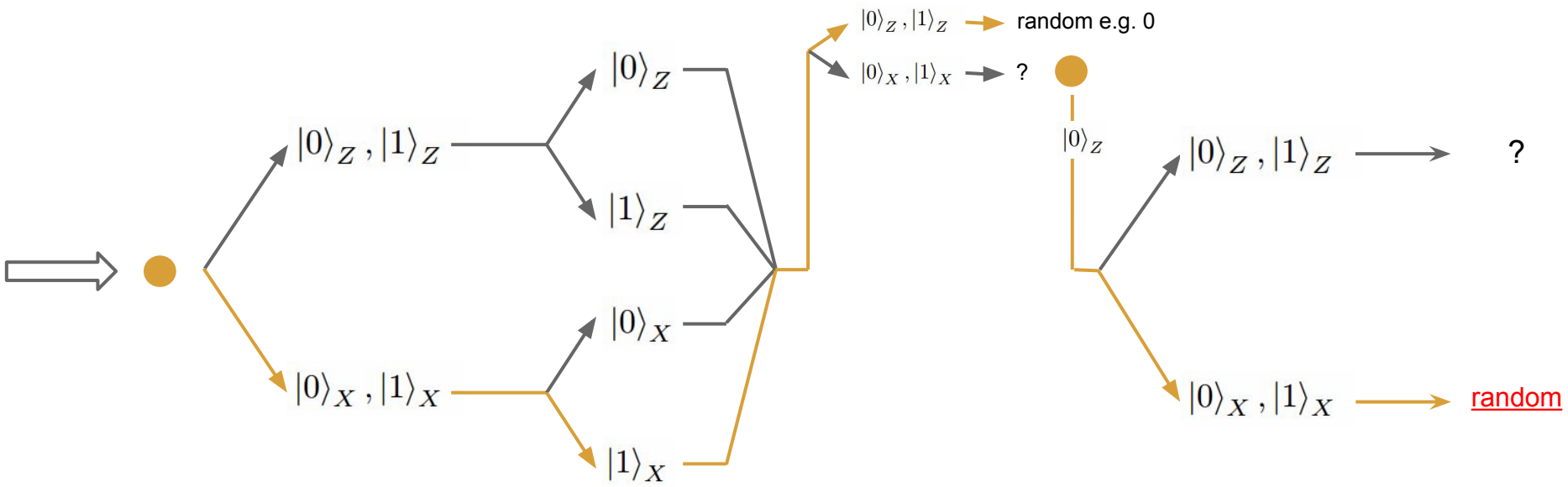
Bob

4. Randomly choose basis

5. Measure

Eve

Measure, re-prepare, transmit to Bob



BB84 (Procedure)

Single Particle Source

Alice

1. Randomly choose basis

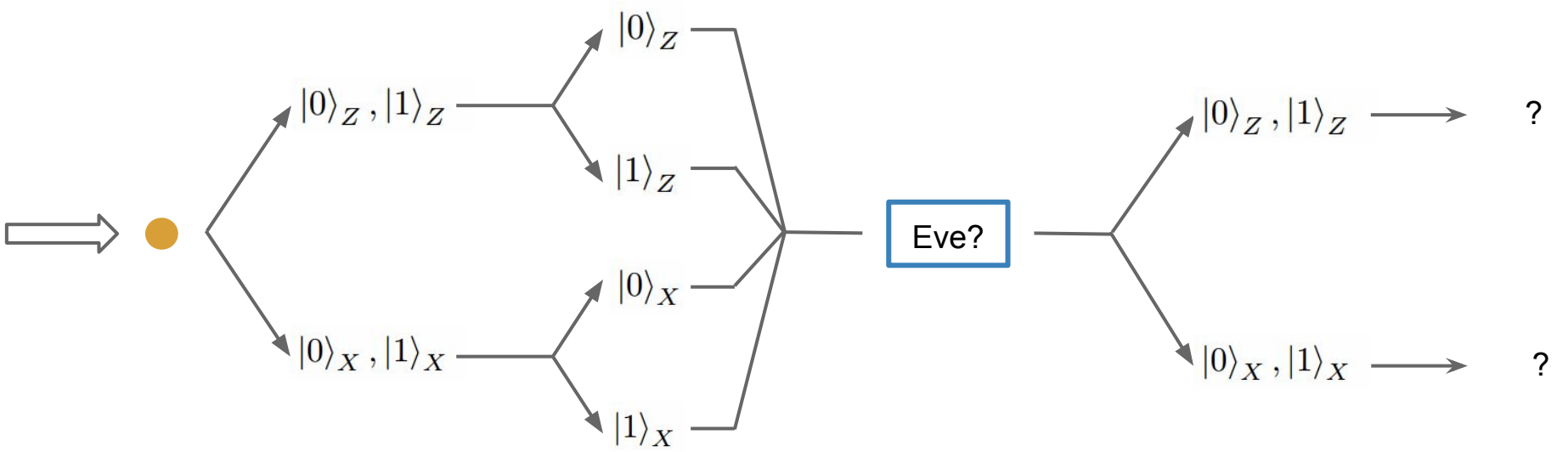
2. Prepare in random state

3. Transmit through Quantum Channel

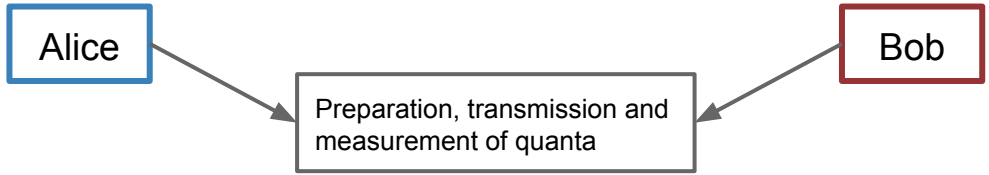
Bob

4. Randomly choose basis

5. Measure



BB84 (Procedure)

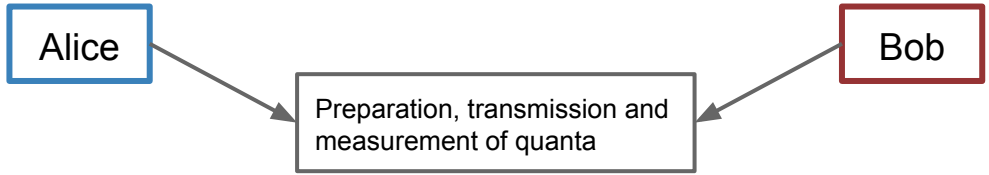


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

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

BB84 (Procedure)

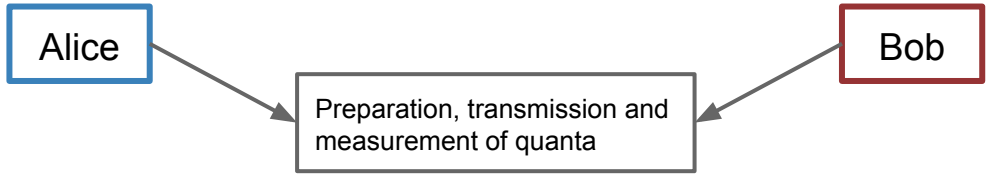


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

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

BB84 (Procedure)

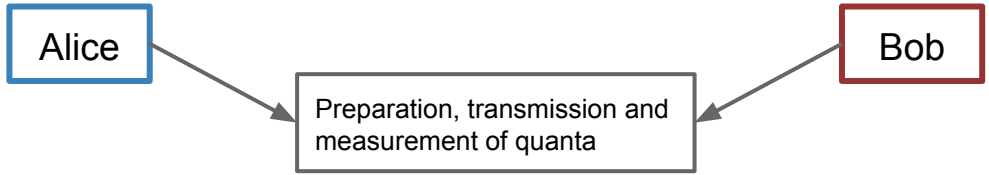


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

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

BB84 (Procedure)

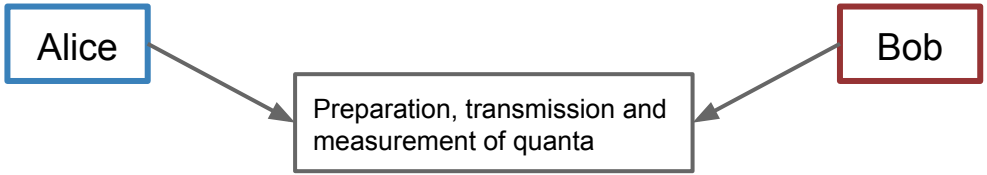


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

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

BB84 (Procedure)

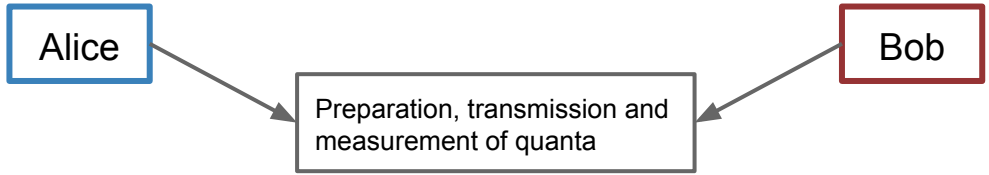


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

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

BB84 (Procedure)

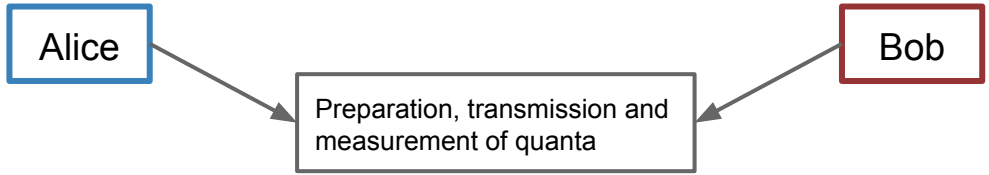


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

Classical Channel

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

BB84 (Procedure)

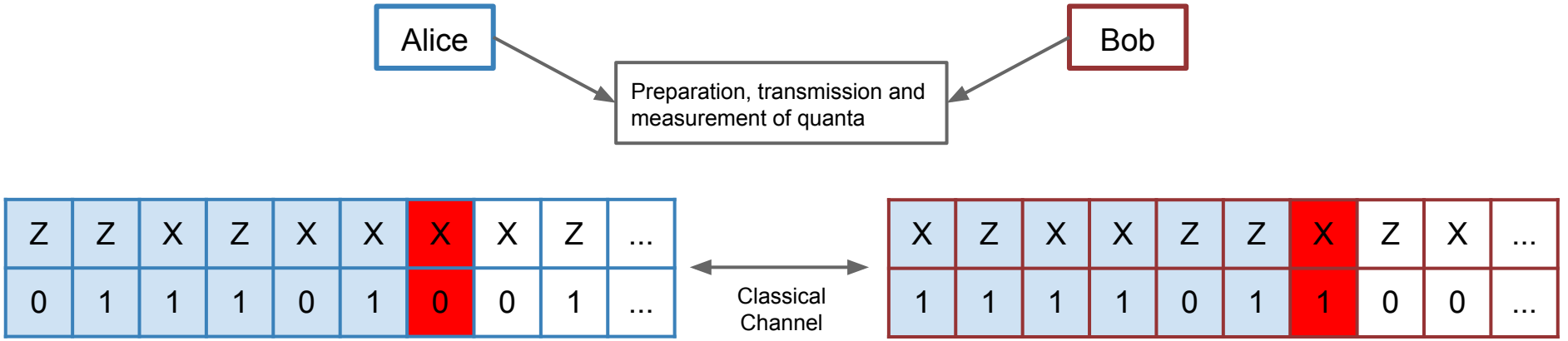


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

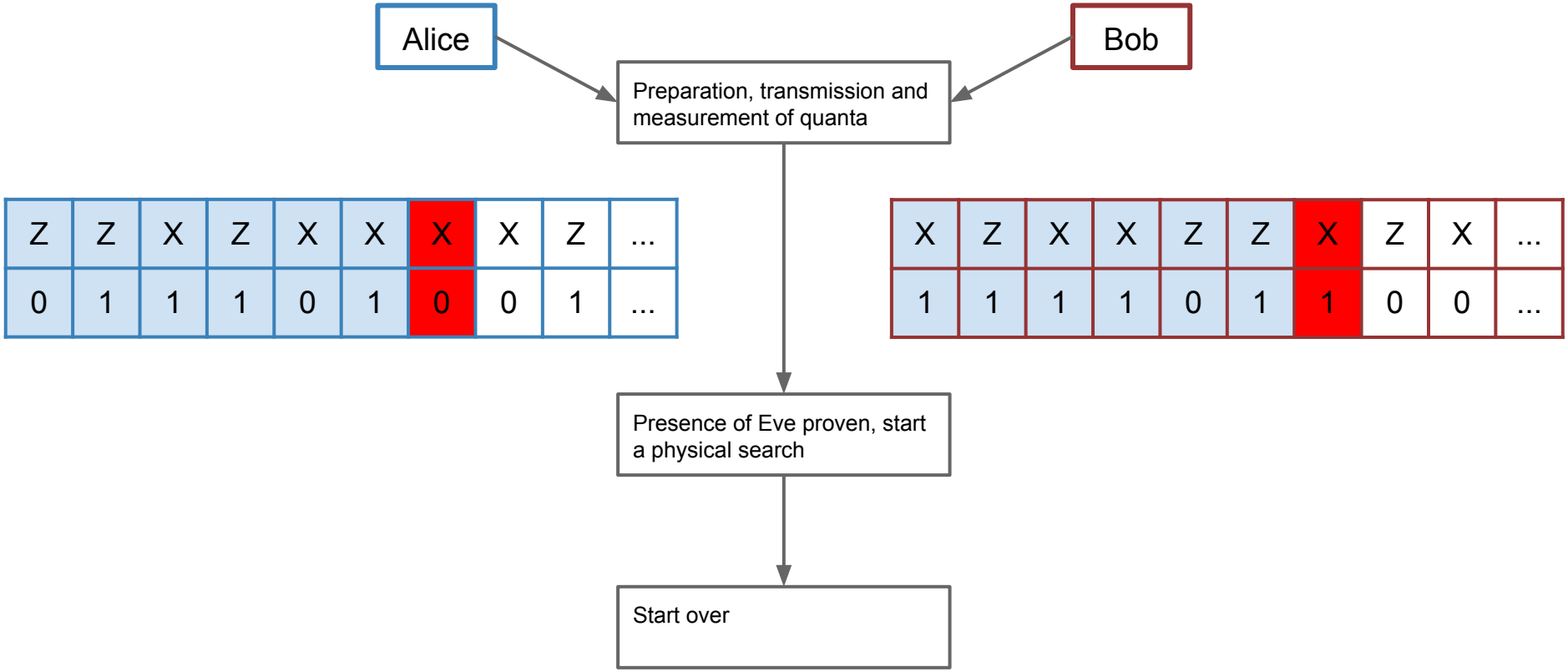
Classical Channel

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

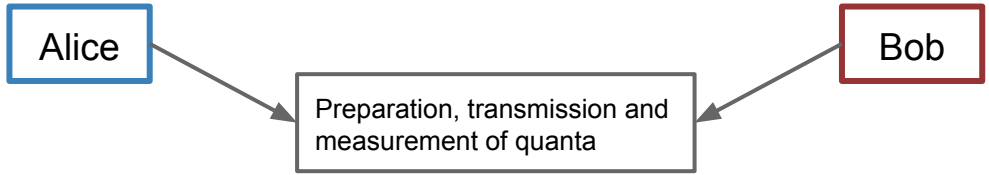
BB84 (Procedure)



BB84 (Procedure)



BB84 (Procedure)

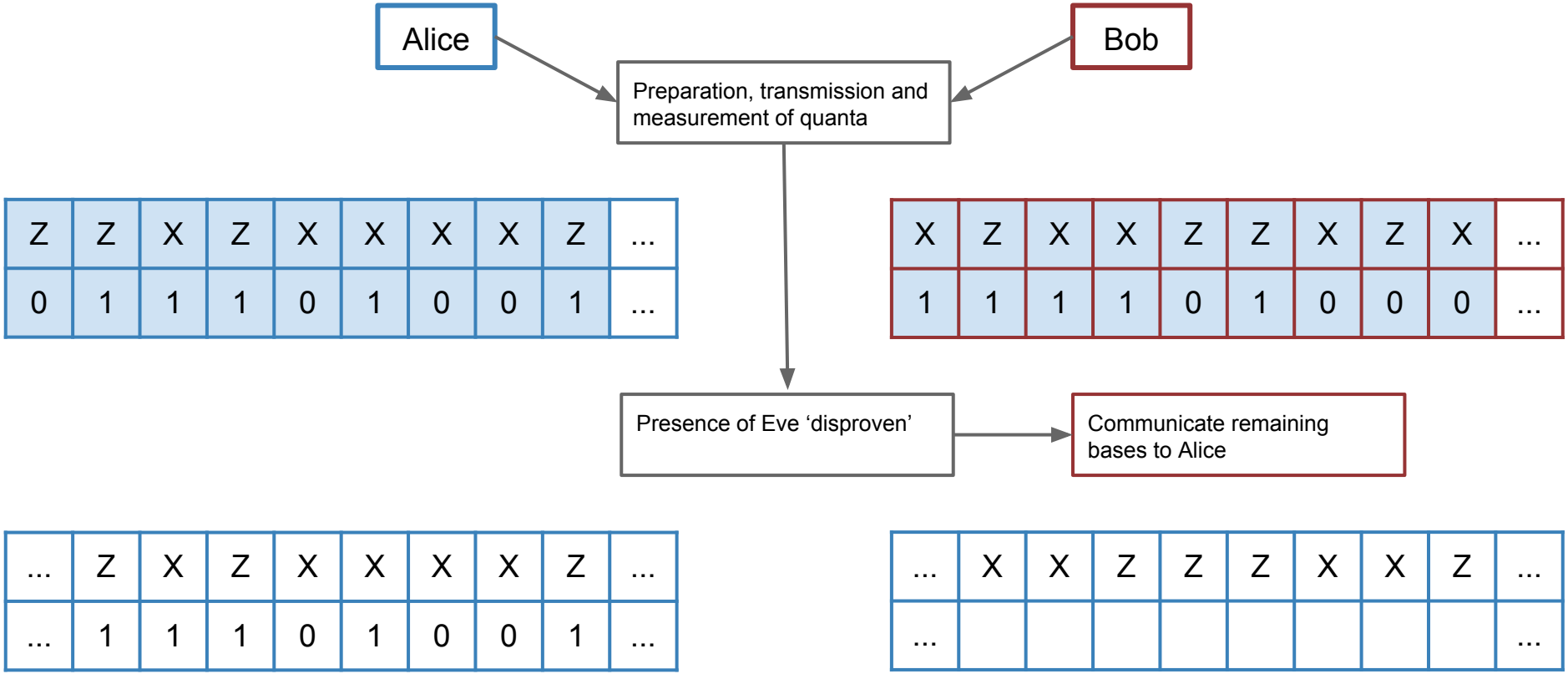


Z	Z	X	Z	X	X	X	X	Z	...
0	1	1	1	0	1	0	0	1	...

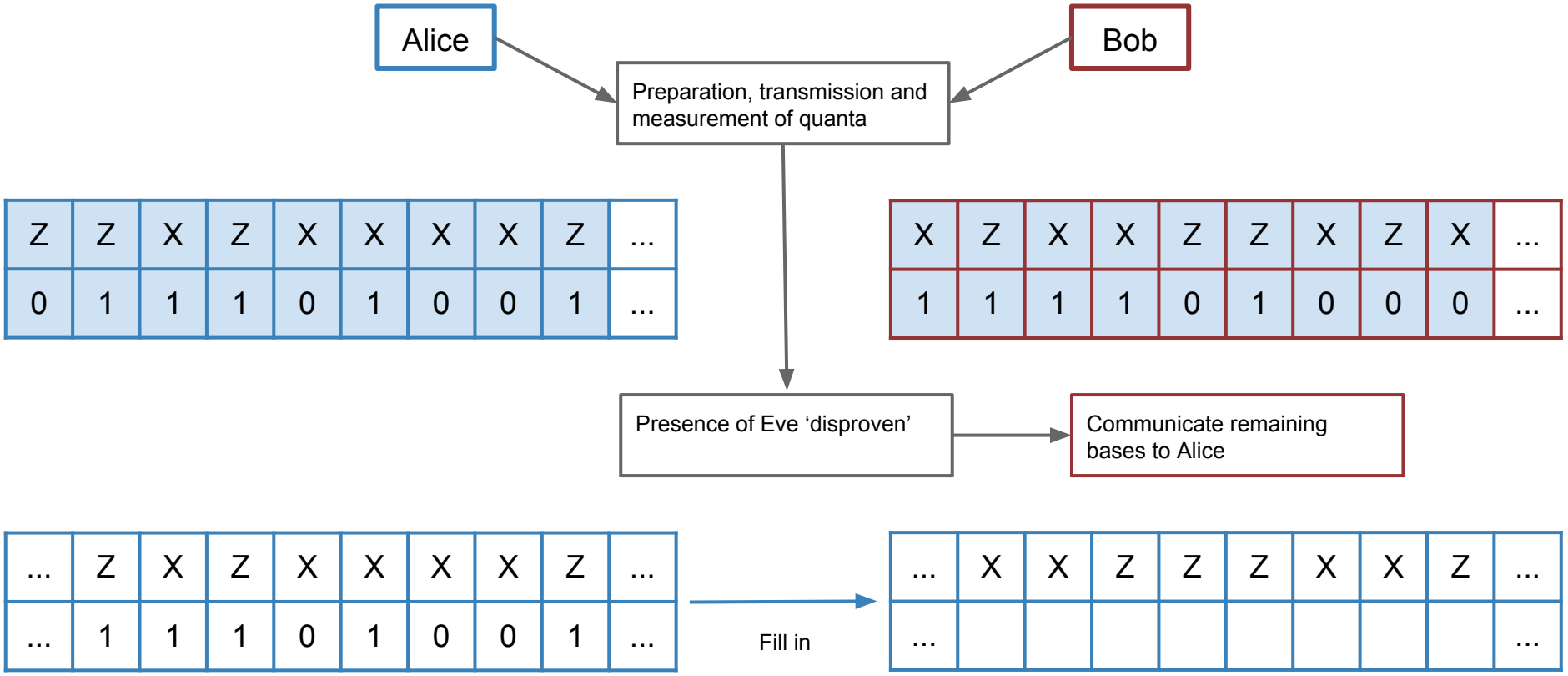
Classical Channel

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

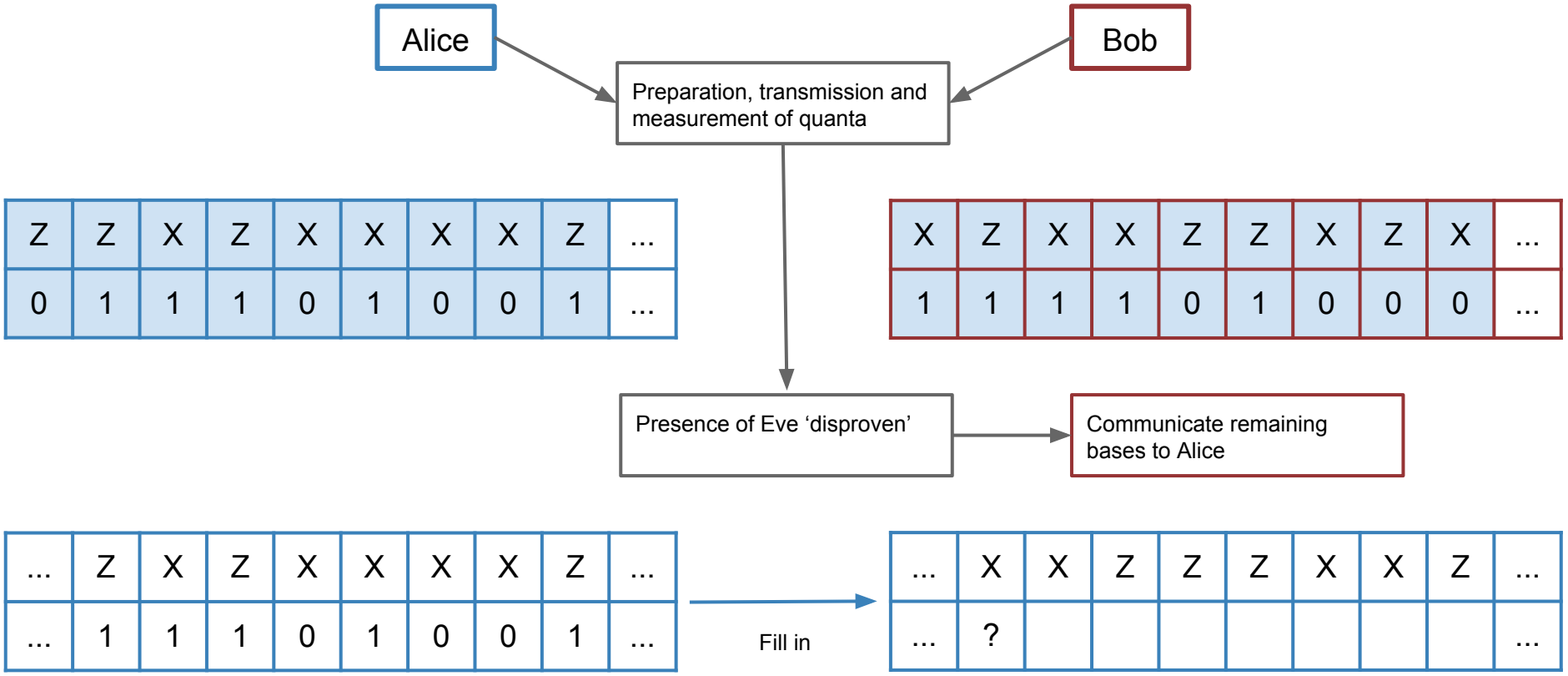
BB84 (Procedure)



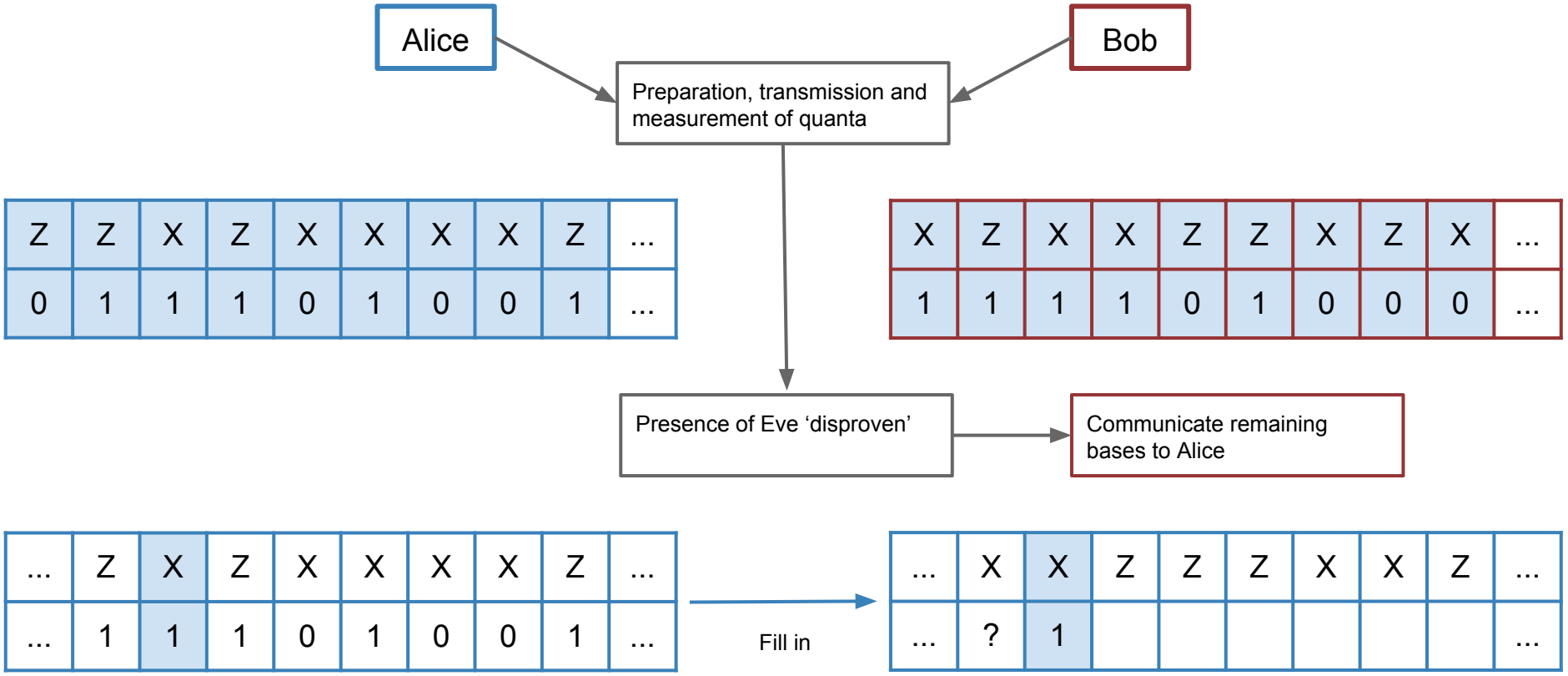
BB84 (Procedure)



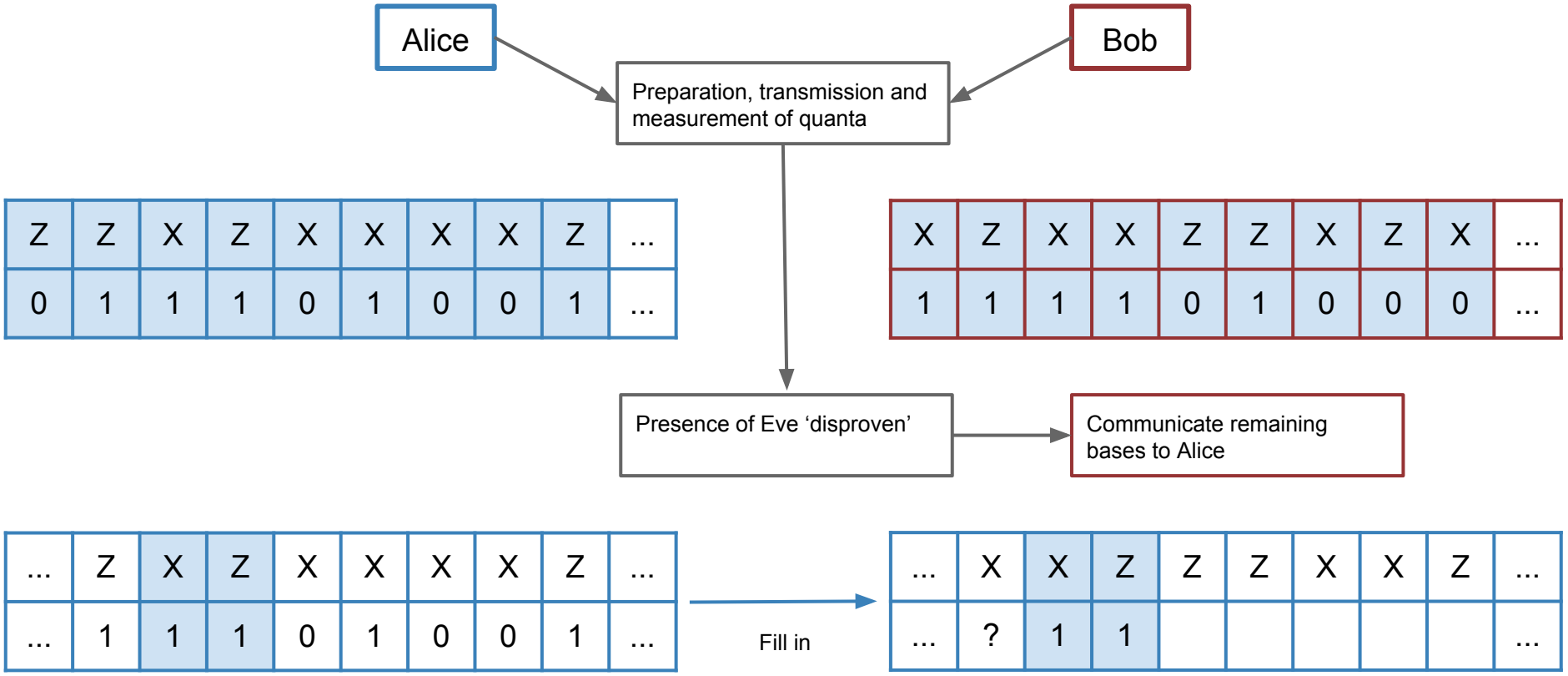
BB84 (Procedure)



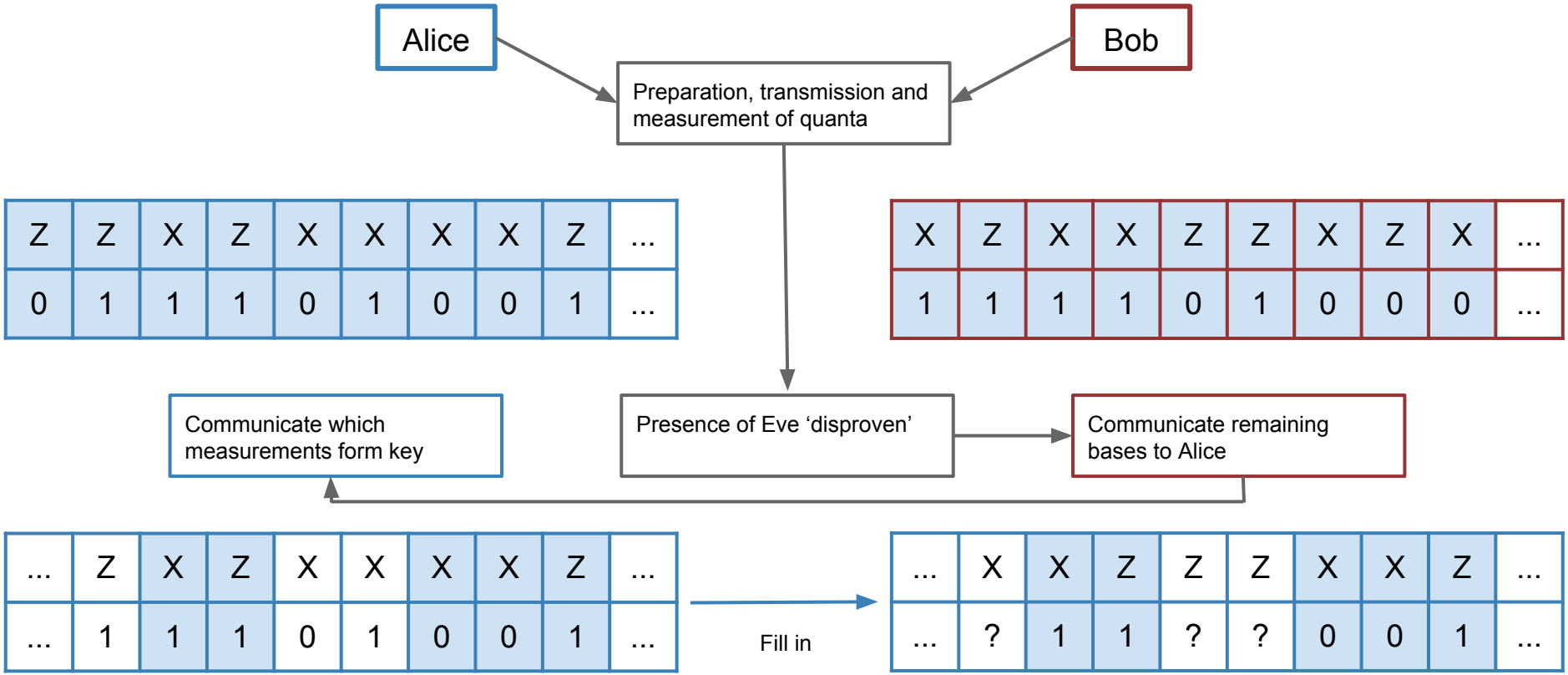
BB84 (Procedure)



BB84 (Procedure)



BB84 (Procedure)



Questions?