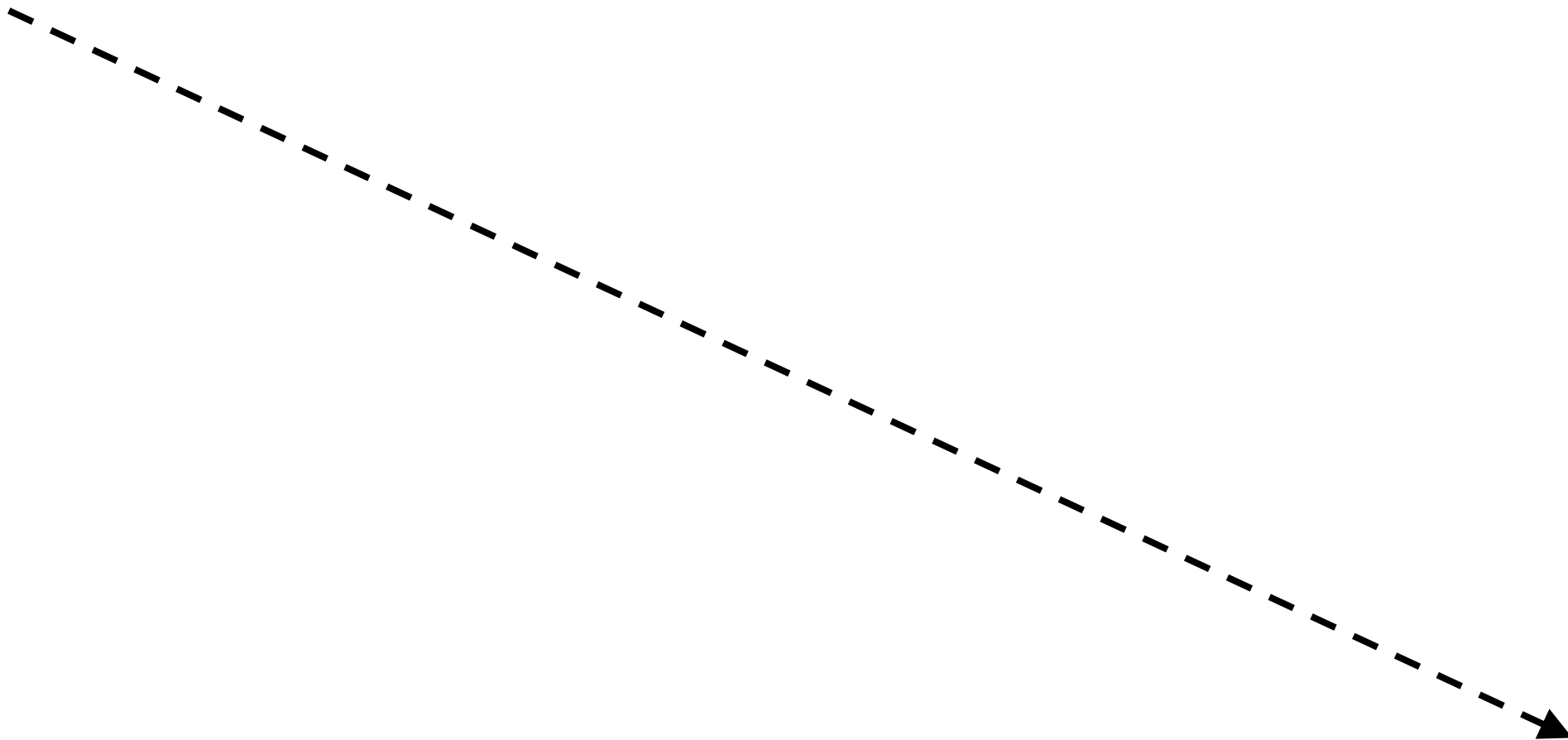
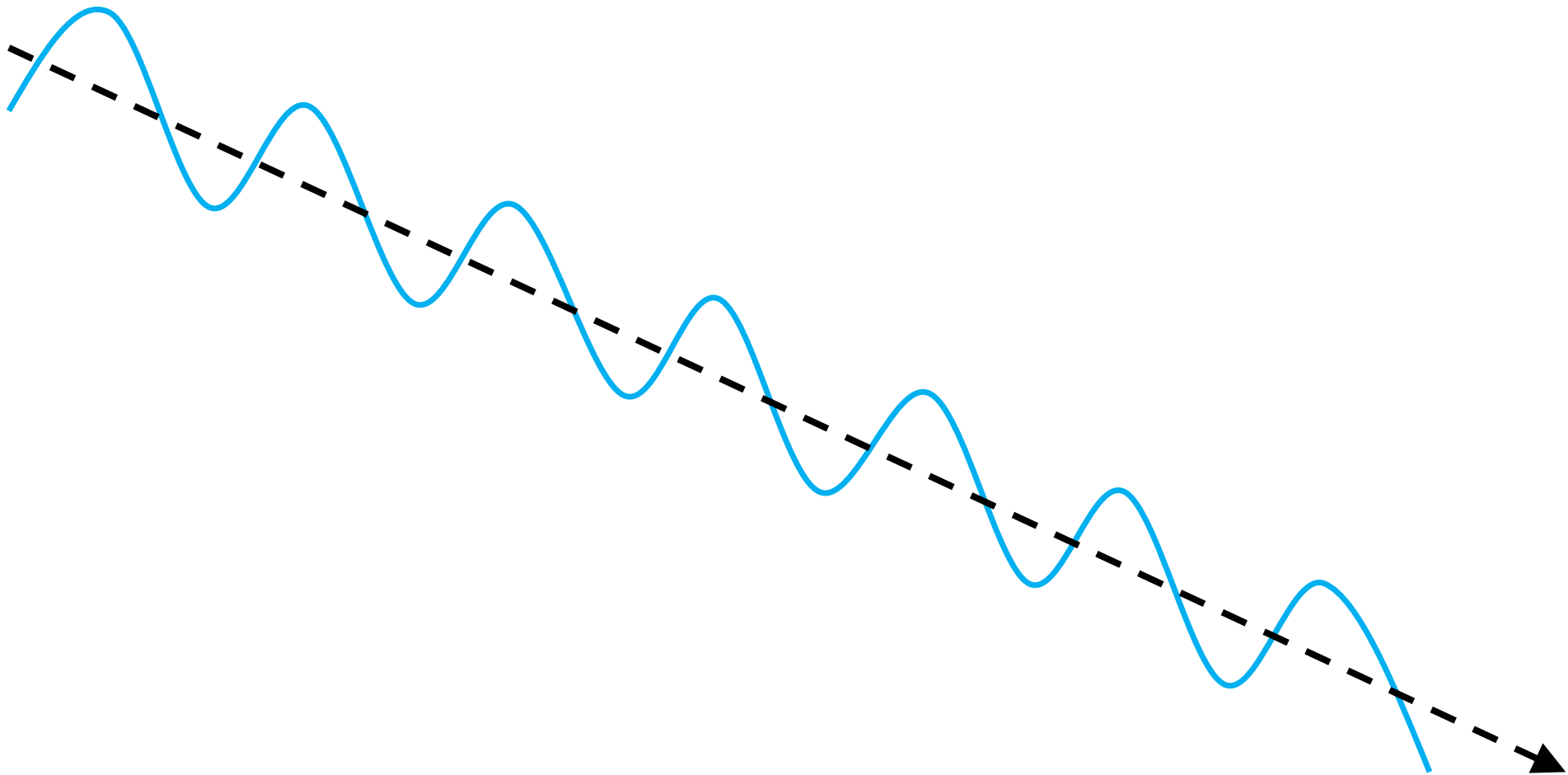
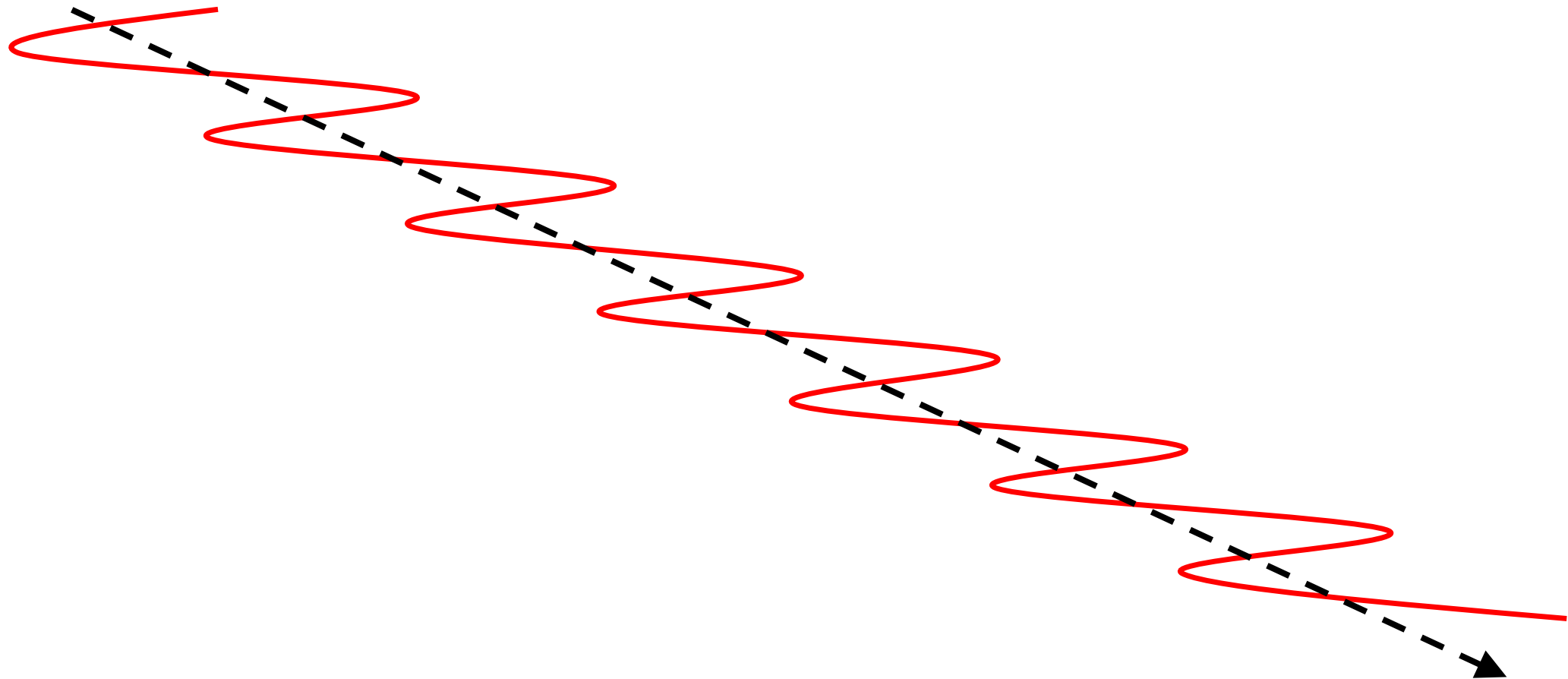


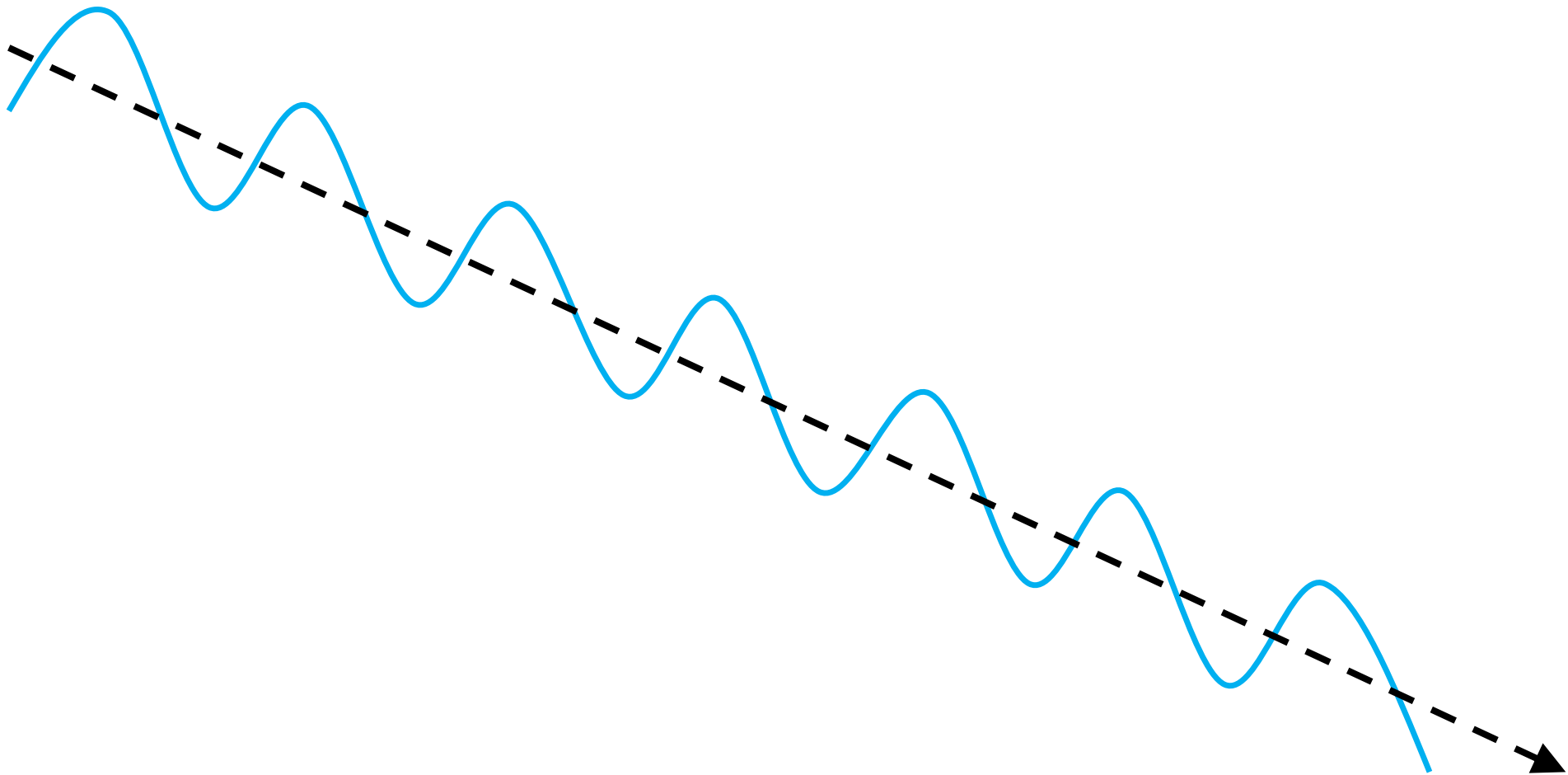
Quantum Computing

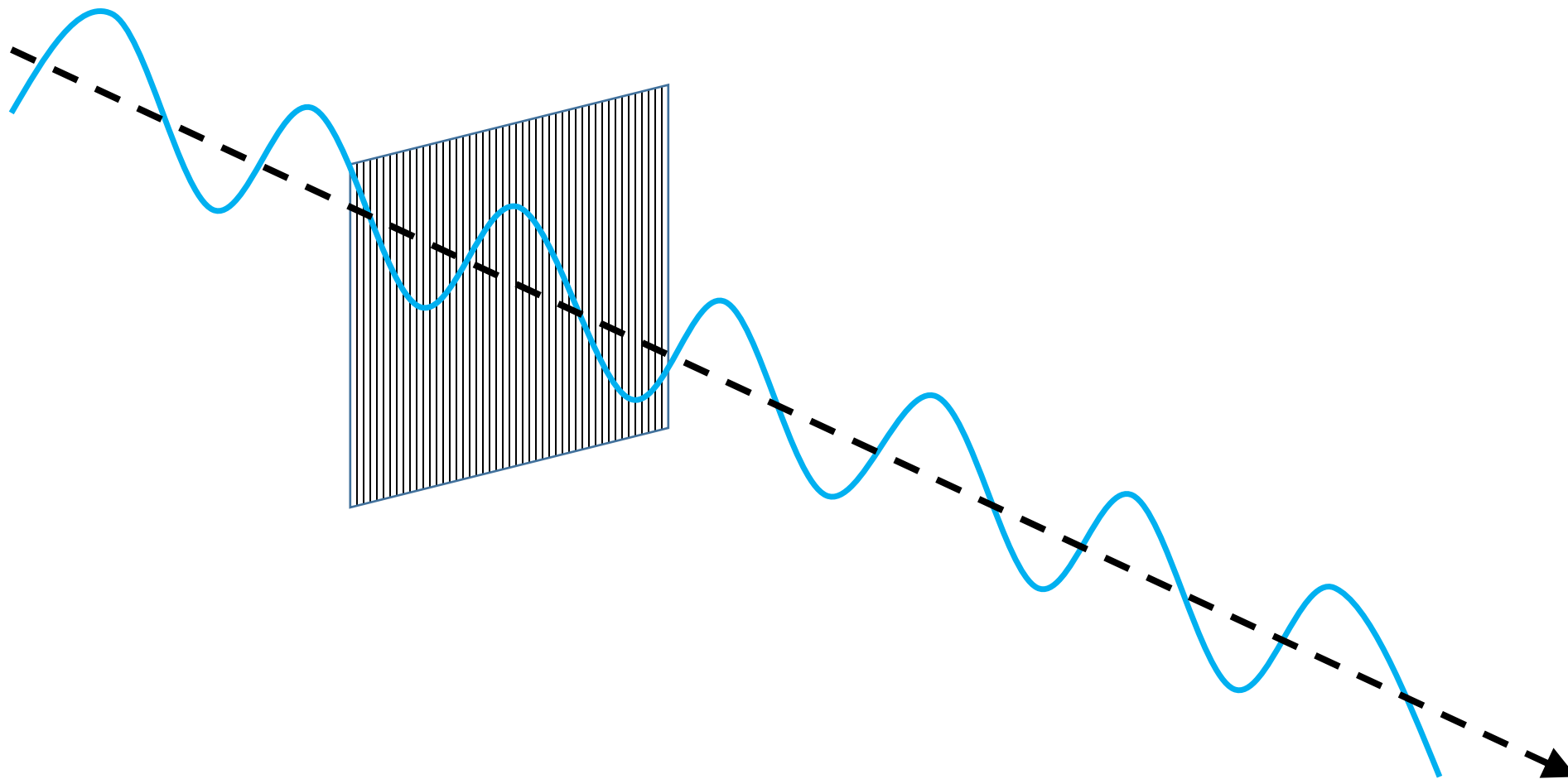
Some interesting bits and bobs and squashed misconceptions

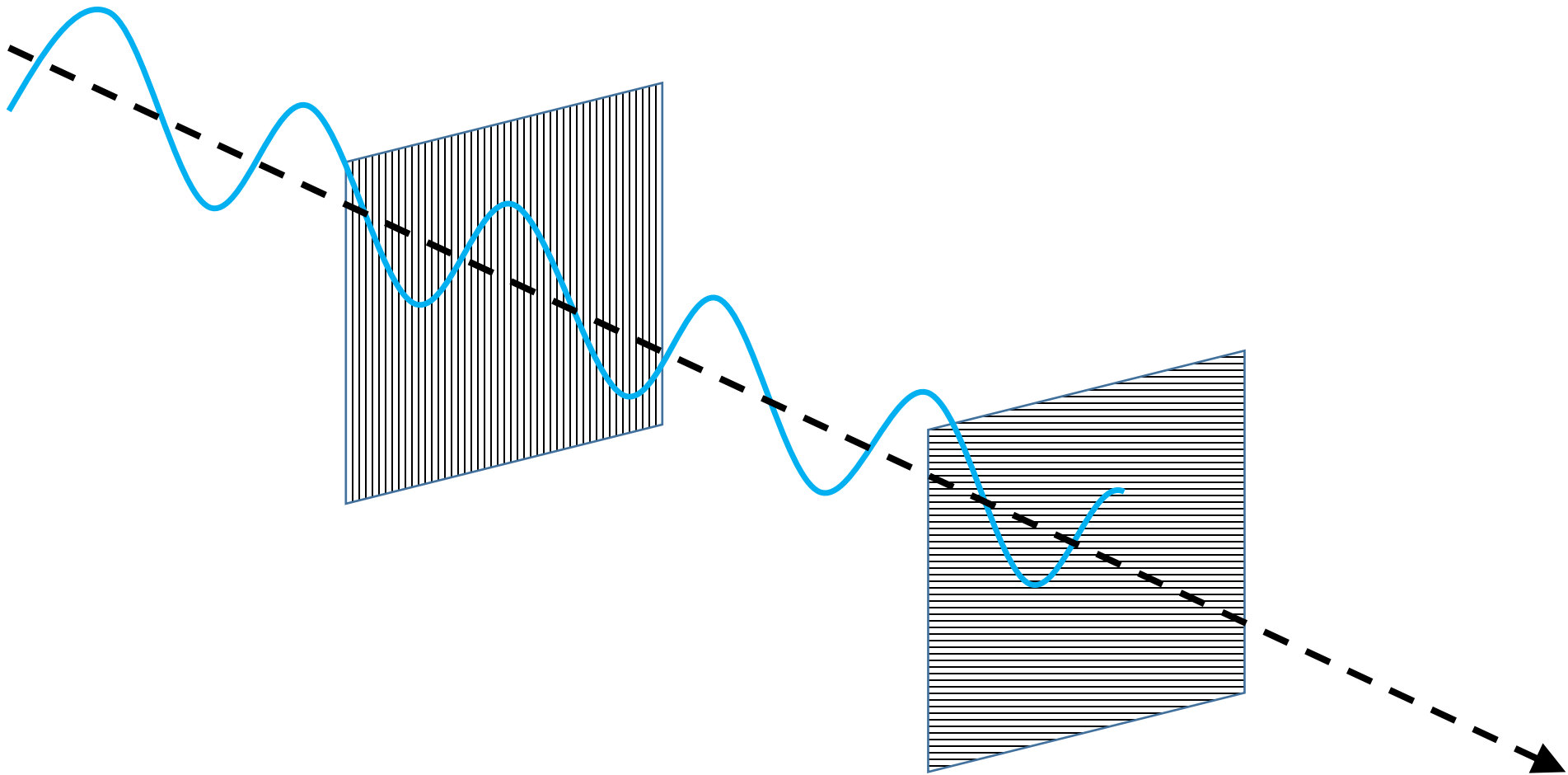


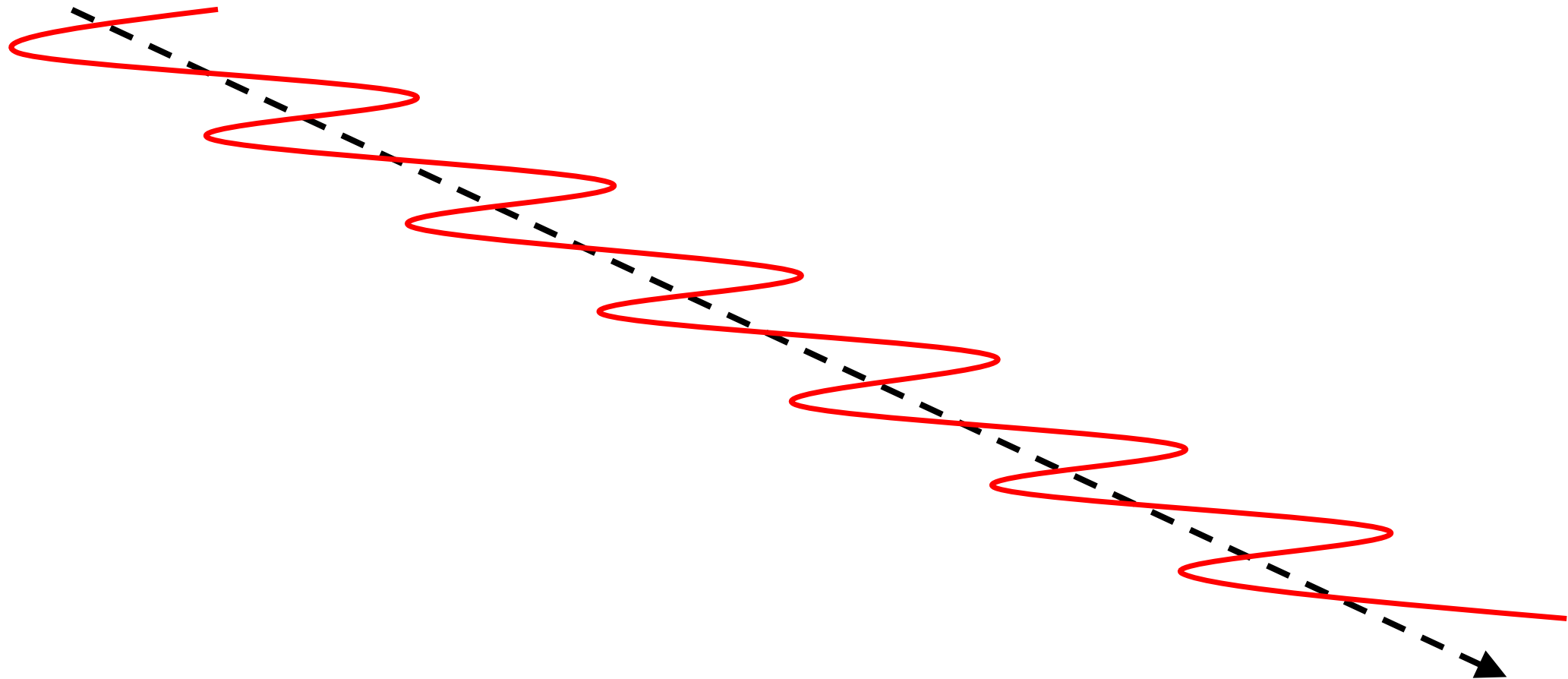


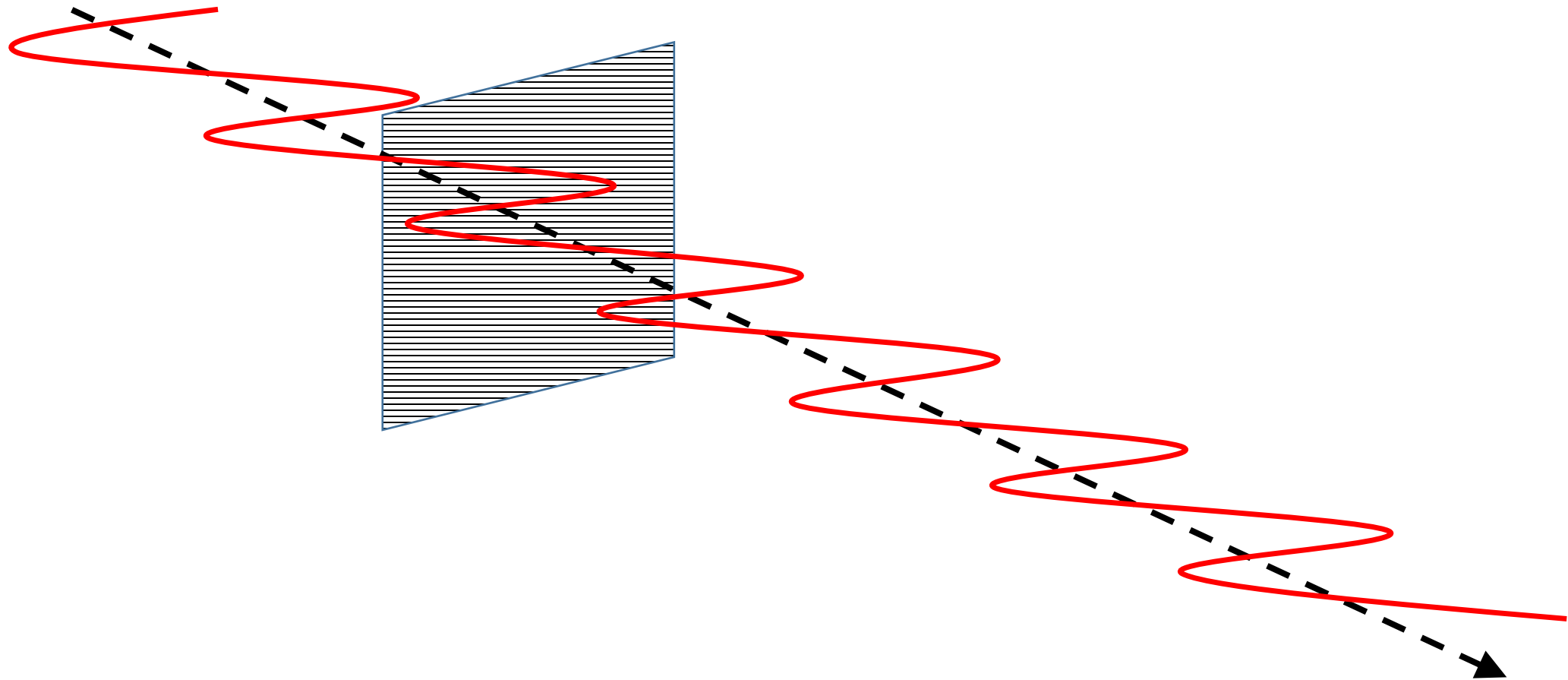


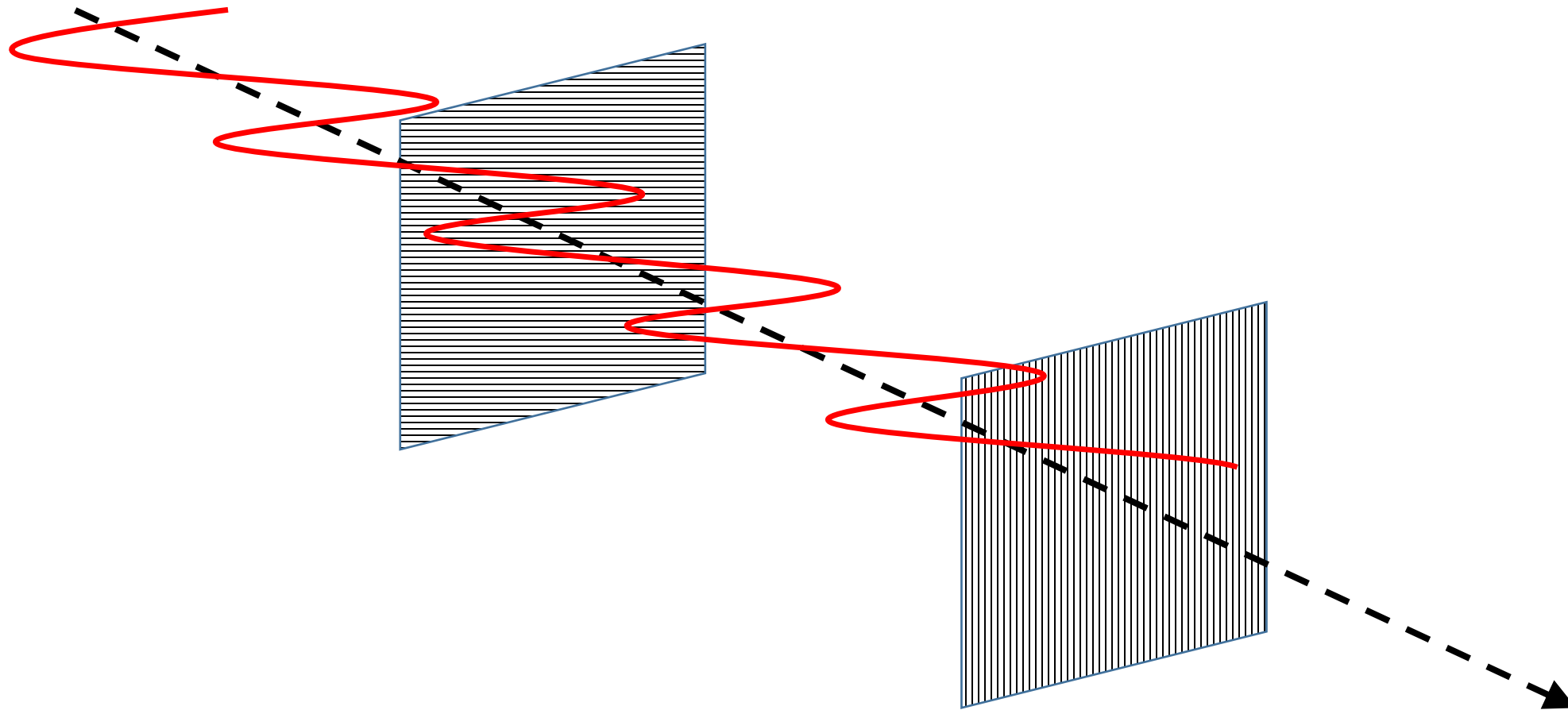


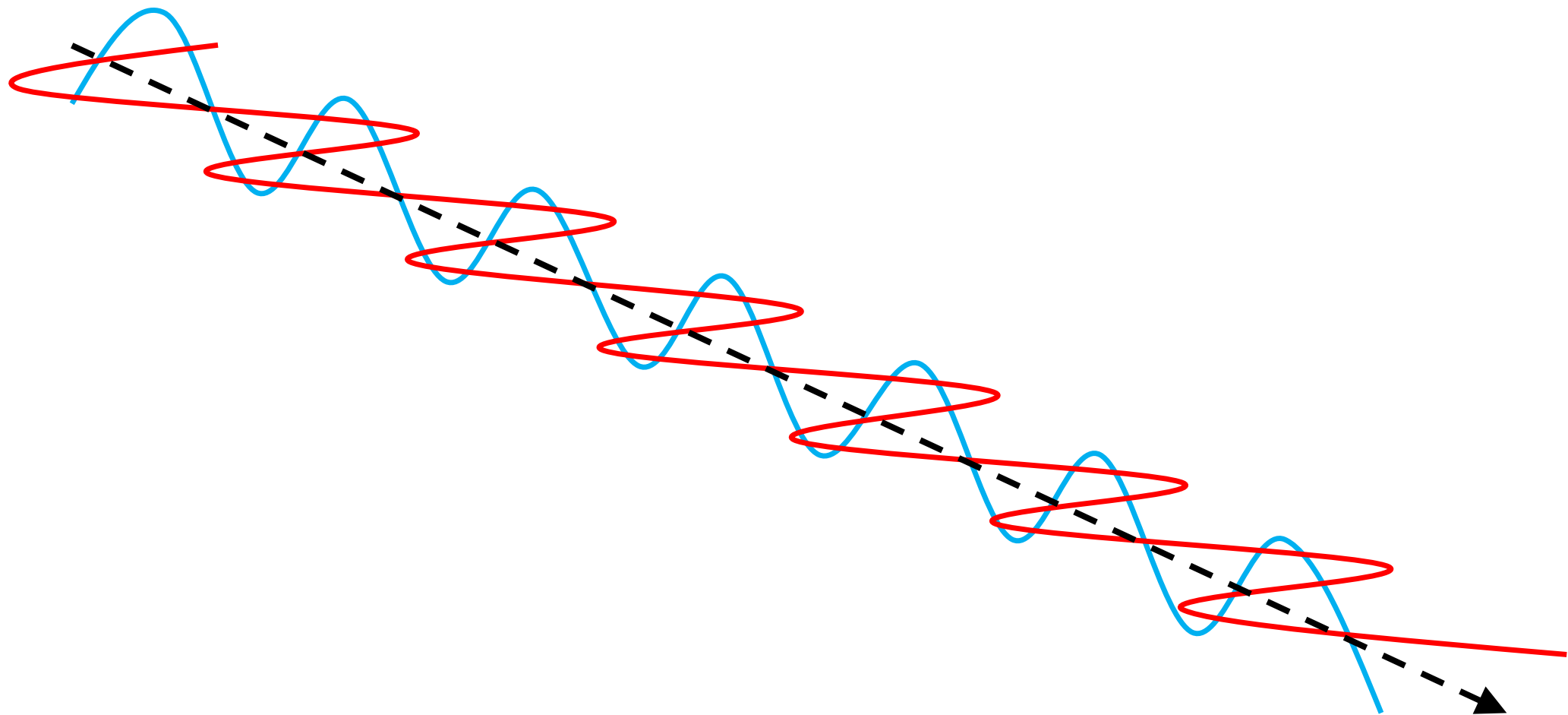


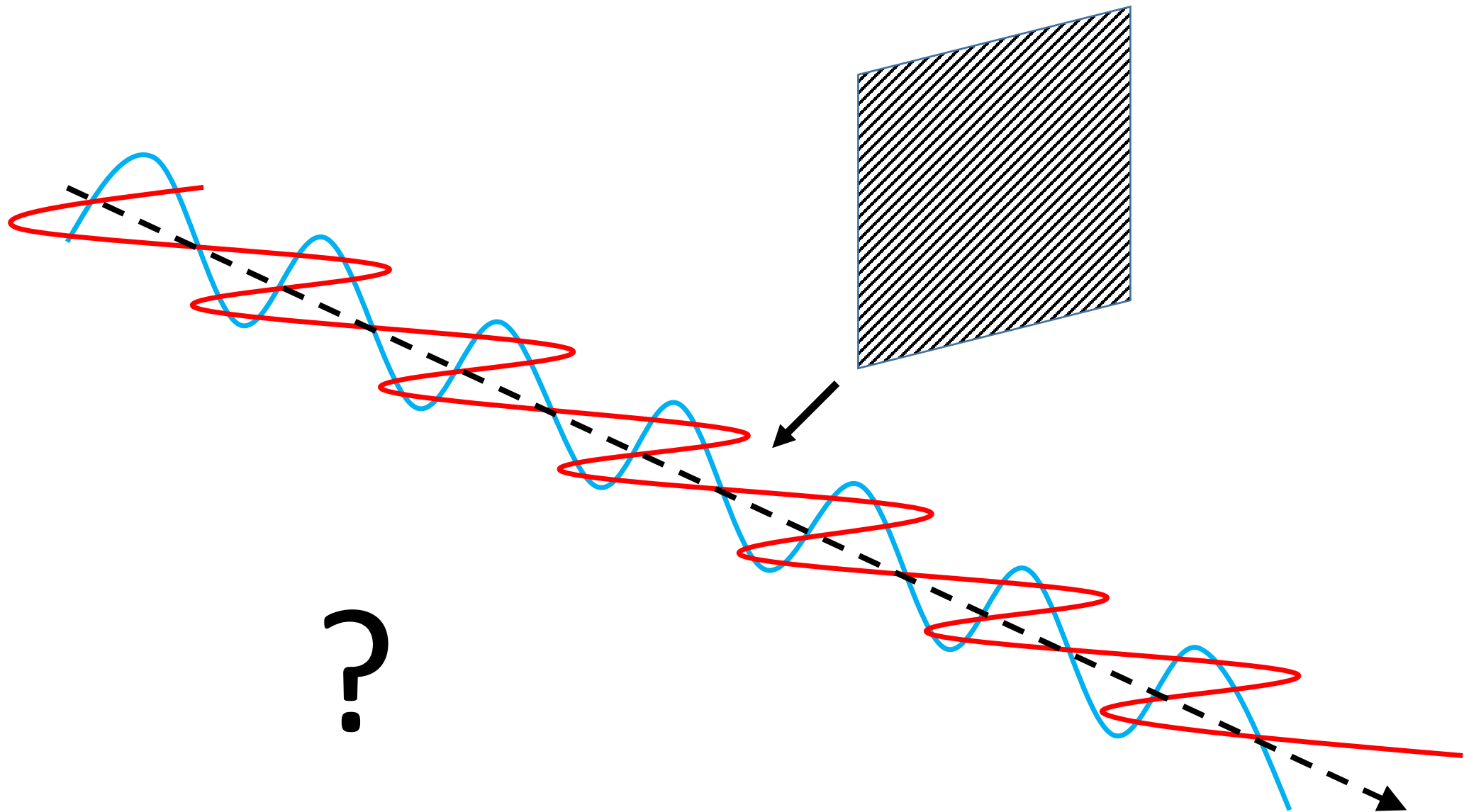


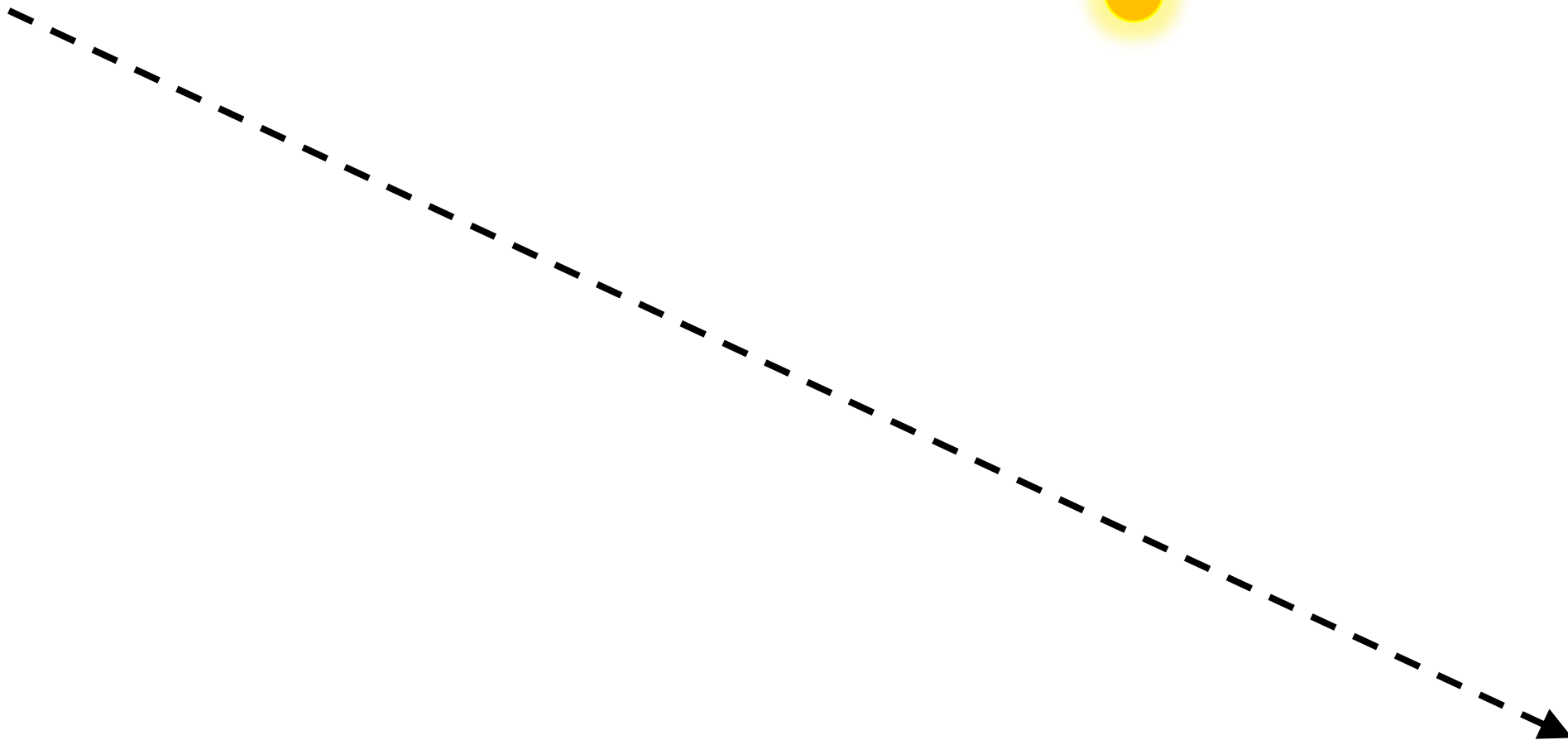
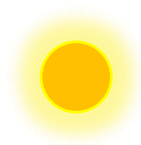


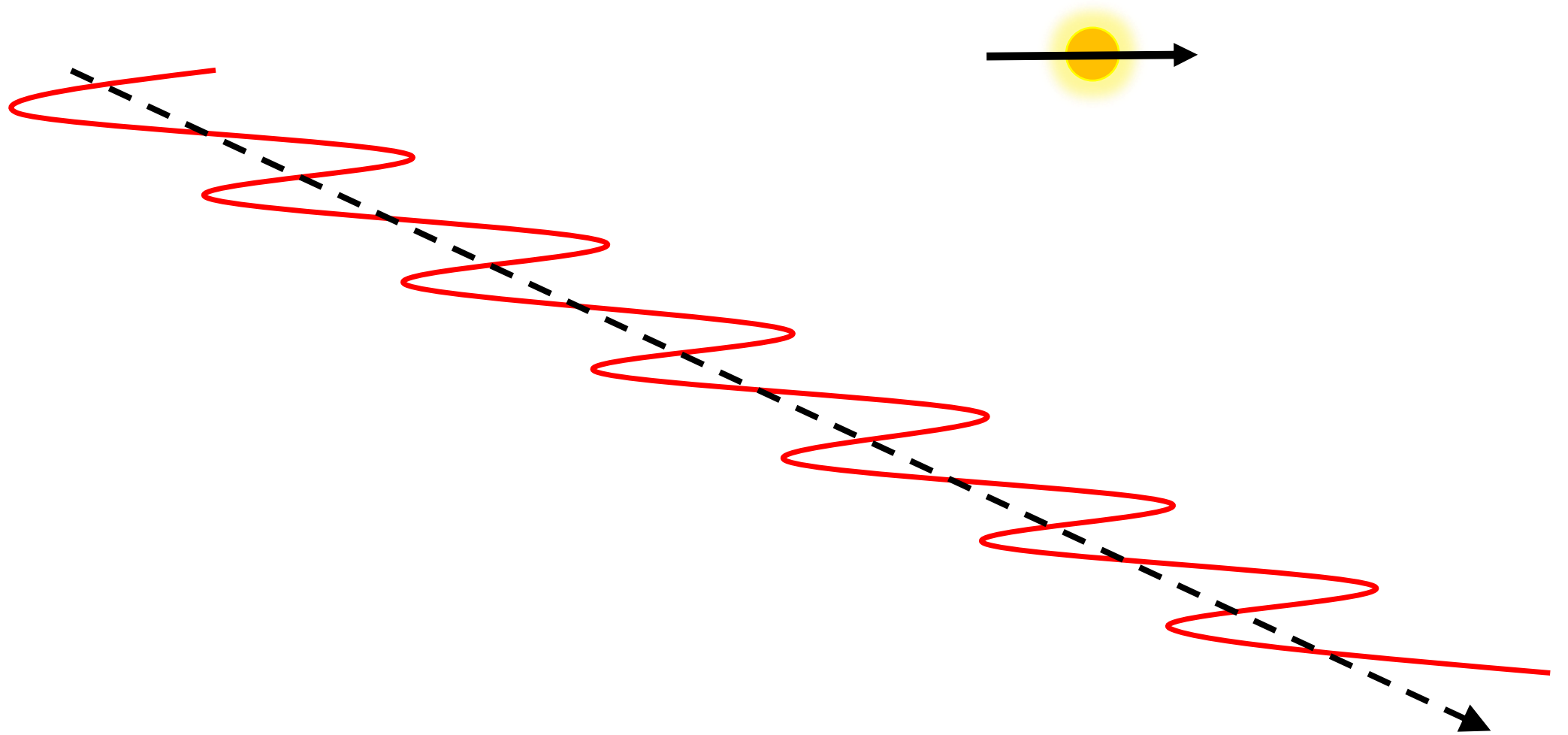


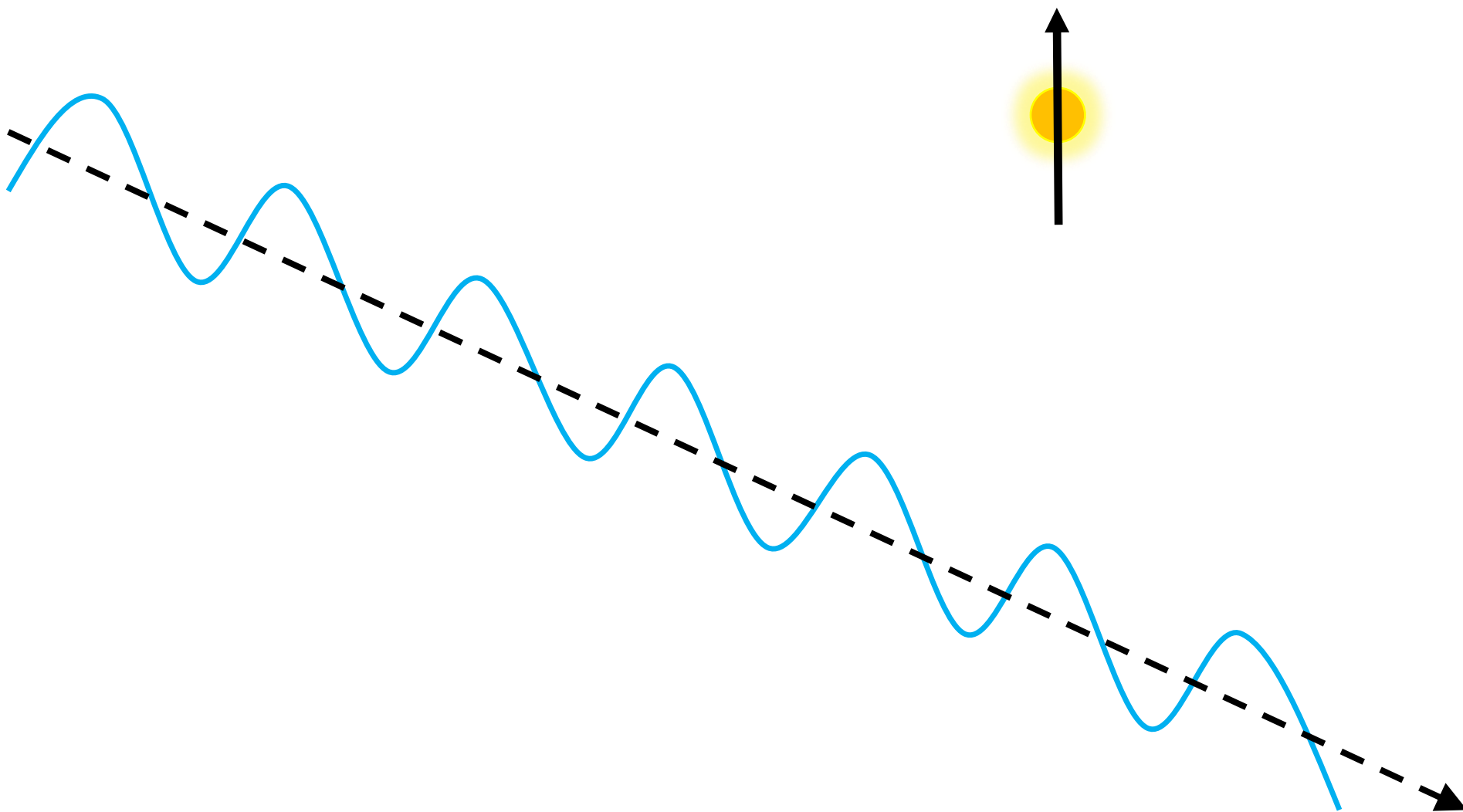


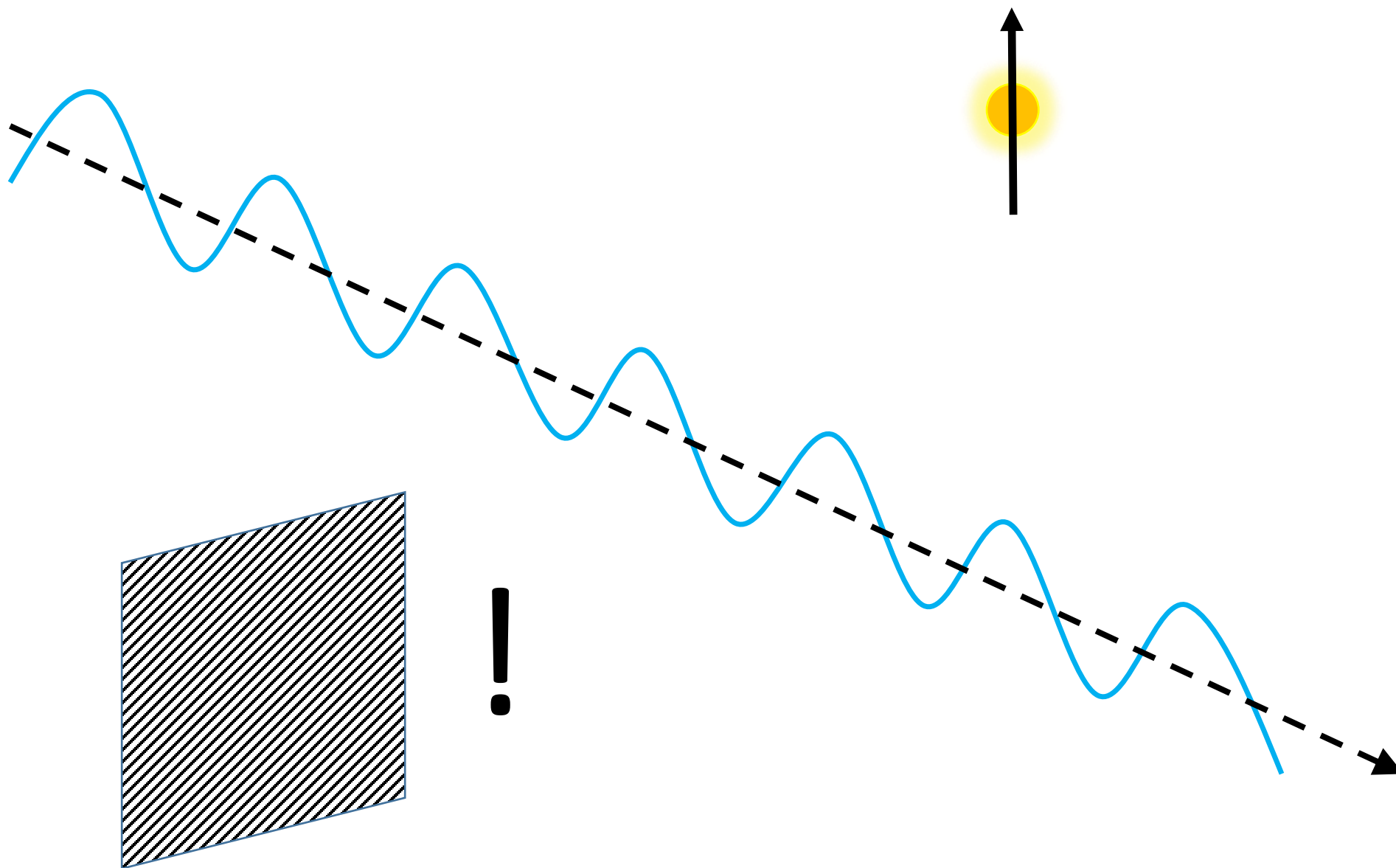


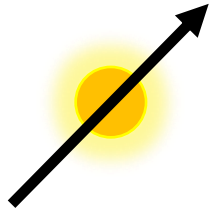
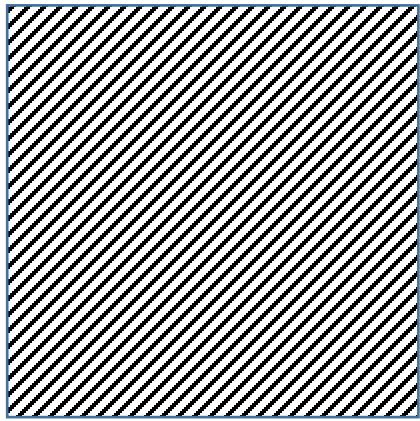


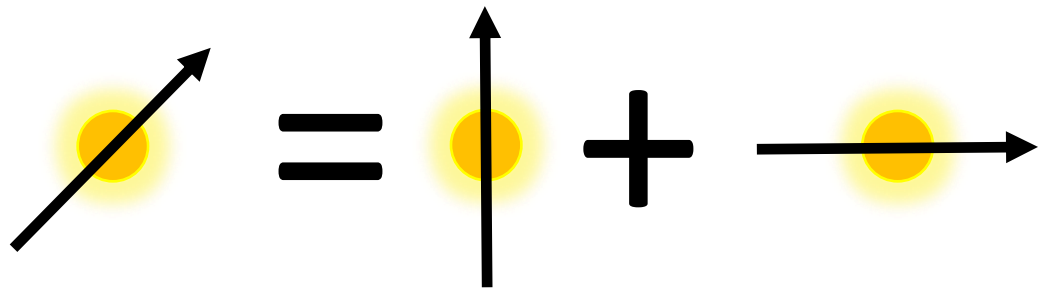
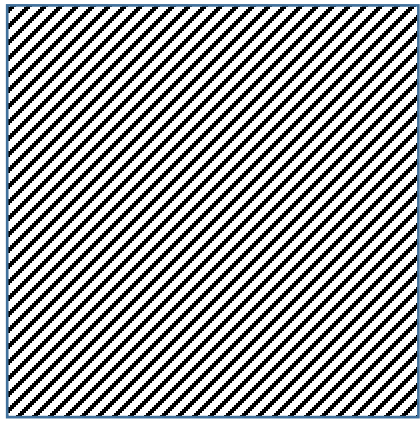


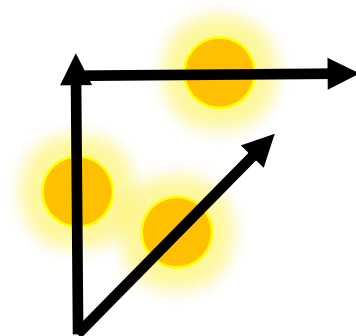


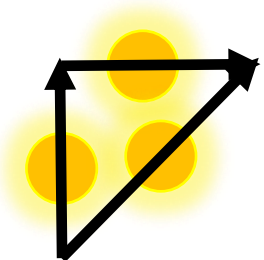


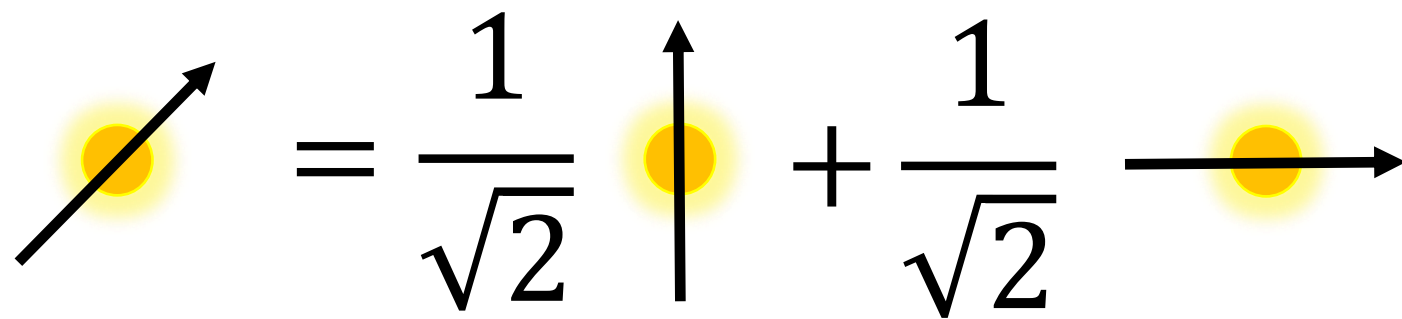












The diagram illustrates the decomposition of a vector into its components. On the left, a vector is shown as a black arrow pointing diagonally upwards and to the right, originating from a yellow circular dot with a soft glow. This vector is equal to the sum of two other vectors. The first vector is a vertical black arrow pointing upwards, also originating from a yellow circular dot with a soft glow, and is scaled by the fraction $\frac{1}{\sqrt{2}}$. The second vector is a horizontal black arrow pointing to the right, originating from a yellow circular dot with a soft glow, and is scaled by the fraction $\frac{1}{\sqrt{2}}$. The entire equation is presented in a clean, black serif font on a white background.

$$\text{diagonal vector} = \frac{1}{\sqrt{2}} \text{vertical vector} + \frac{1}{\sqrt{2}} \text{horizontal vector}$$

It is in two states at once!

$$\nearrow = \frac{1}{\sqrt{2}} \uparrow + \frac{1}{\sqrt{2}} \rightarrow$$

It is in two states at once!

Wrong

$$\nearrow = \frac{1}{\sqrt{2}} \uparrow + \frac{1}{\sqrt{2}} \rightarrow$$

$$\nearrow = \frac{1}{\sqrt{2}} \uparrow + \frac{1}{\sqrt{2}} \rightarrow$$



$$\nearrow = \frac{1}{\sqrt{2}} \uparrow + \frac{1}{\sqrt{2}} \rightarrow$$



“The probability that, if we make a measurement of the polarisation of the state, we will measure it to be vertically polarised, is one half”

$$\nearrow = \frac{1}{\sqrt{2}} \uparrow + \frac{1}{\sqrt{2}} \rightarrow$$



“The probability that, if we make a measurement of the polarisation of the state, we will measure it to be vertically polarised, is one half”

“The probability that the polarisation state is vertical is one half”

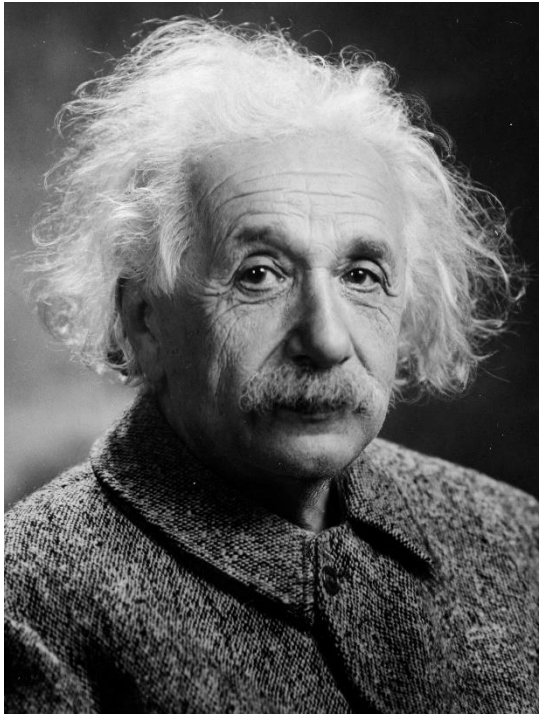
$$\nearrow = \frac{1}{\sqrt{2}} \uparrow + \frac{1}{\sqrt{2}} \rightarrow$$

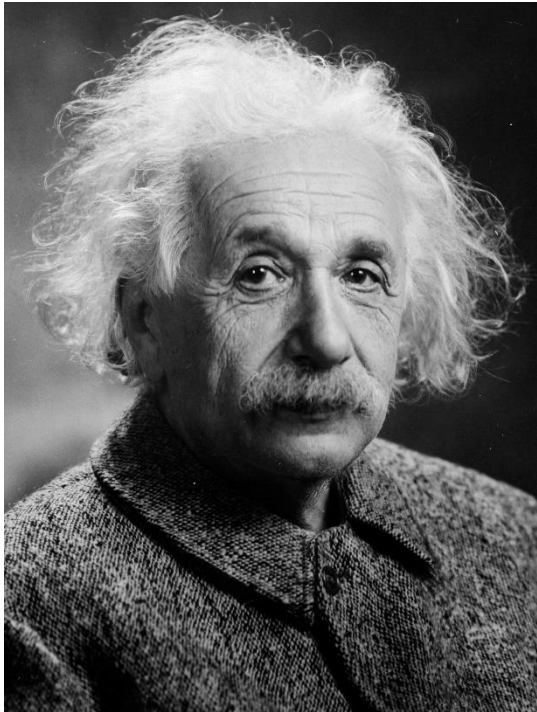


“The probability that, if we make a measurement of the polarisation of the state, we will measure it to be vertically polarised, is one half”

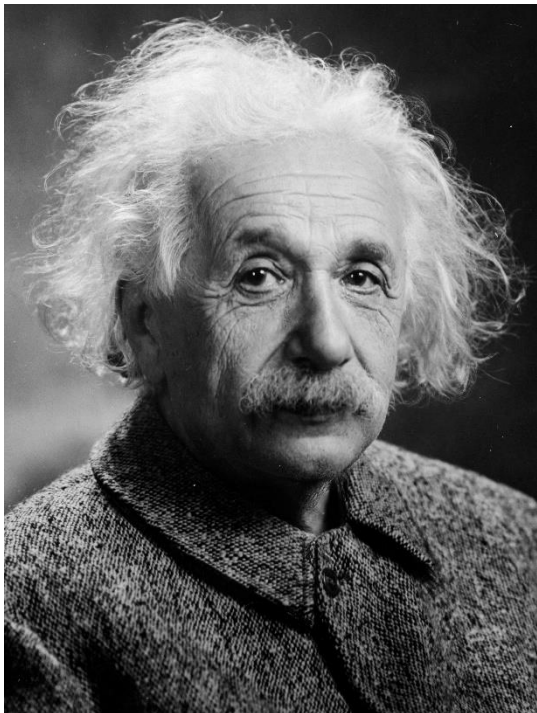
“The probability that the polarisation state is vertical is one half”

Wrong





“God does not play dice with the universe”



“God does not play dice with the universe”

Wrong

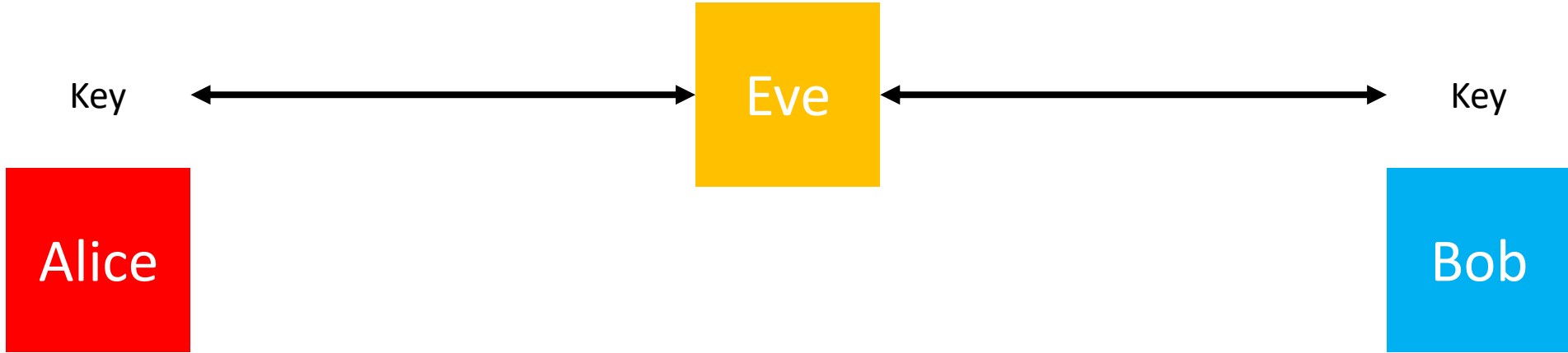
Quantum Key Distribution

Back off Eve

Alice

Bob



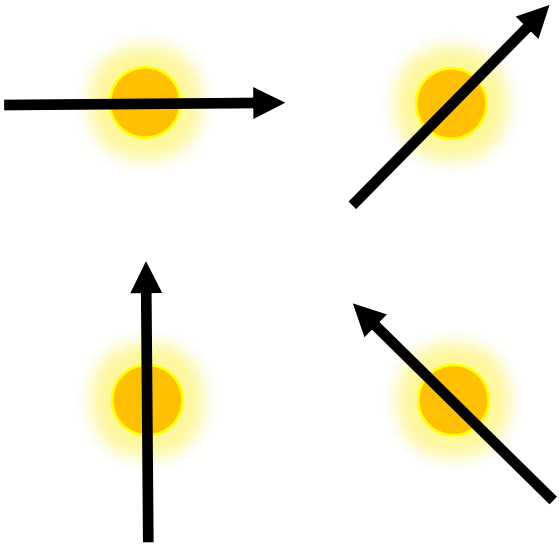


Alice

Bob

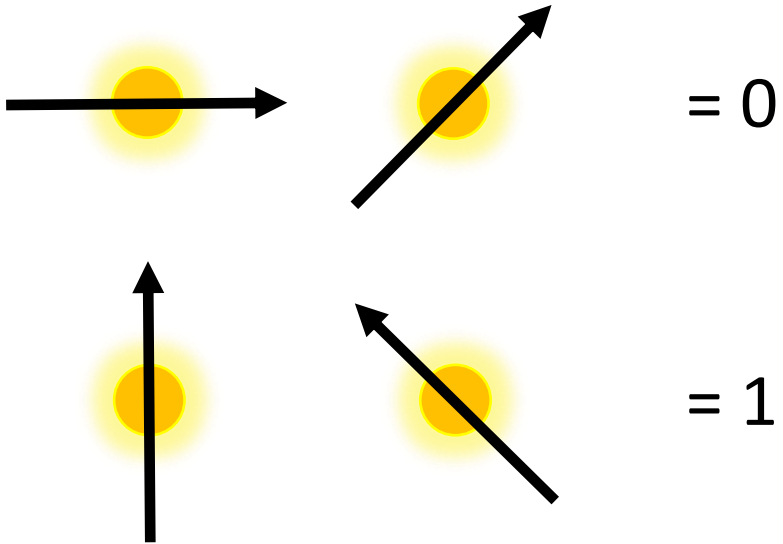
Alice

Bob

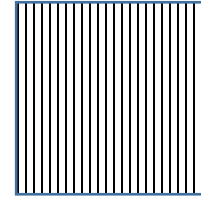


Alice

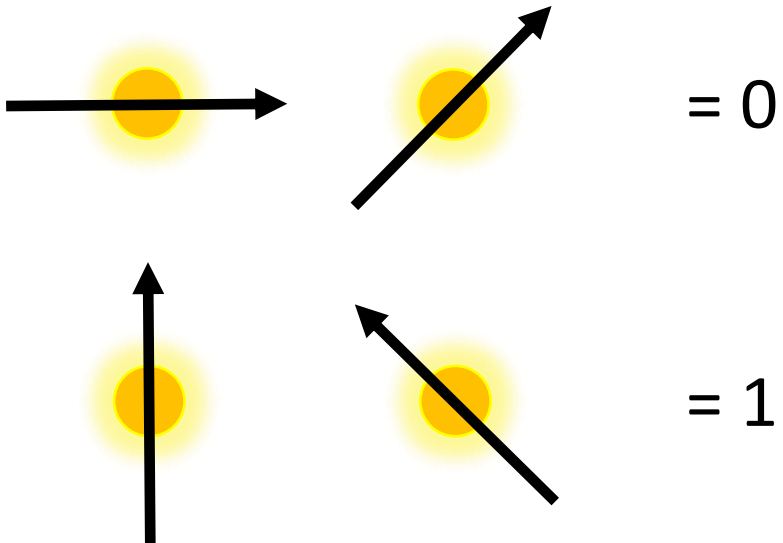
Bob



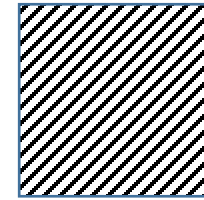
Alice



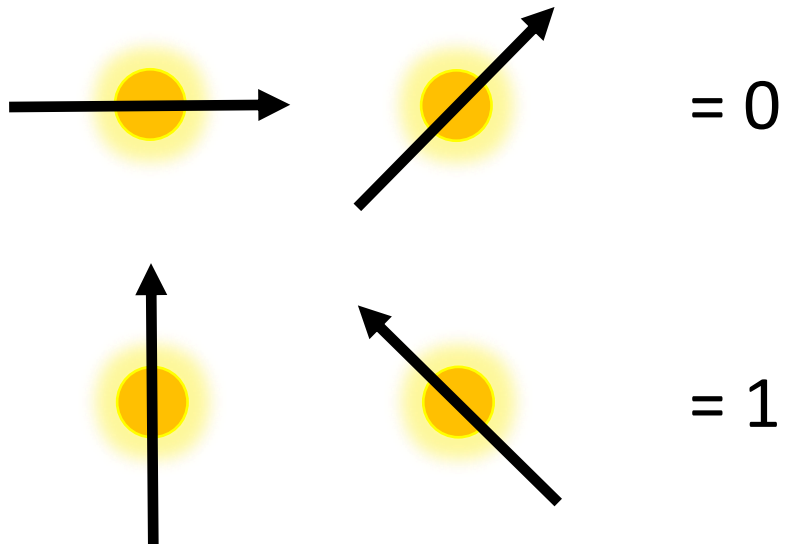
Bob



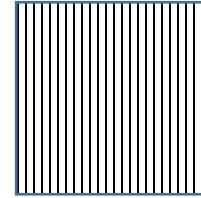
Alice



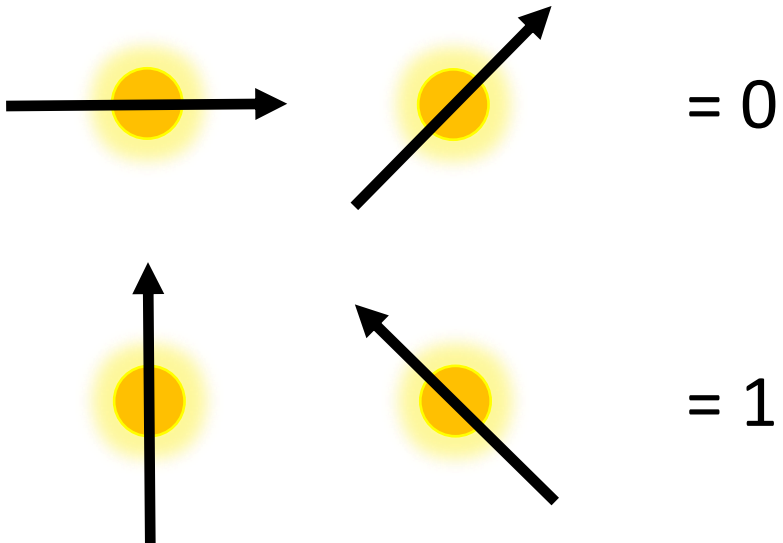
Bob



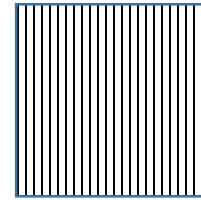
Alice



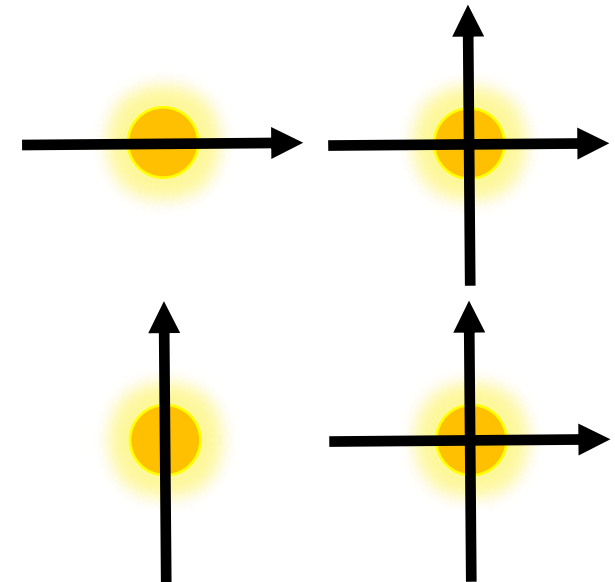
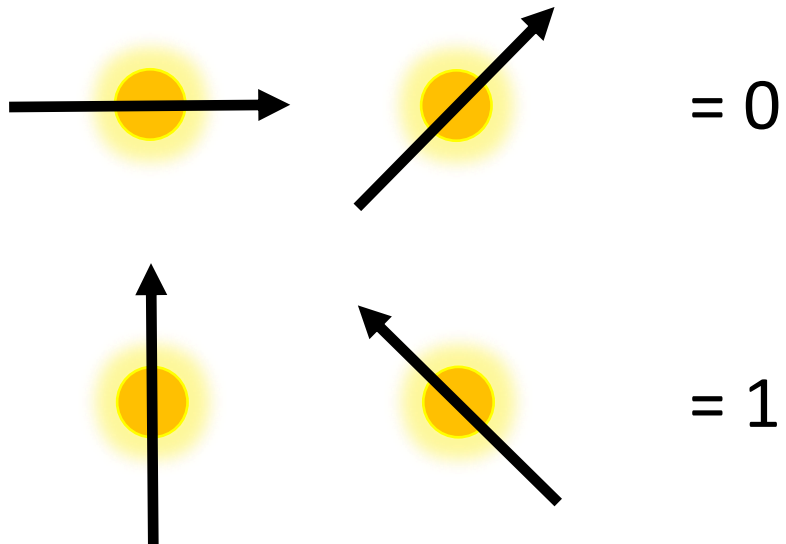
Bob



Alice



Bob

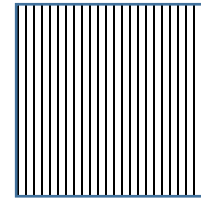


$$\nearrow = \frac{1}{\sqrt{2}} \uparrow + \frac{1}{\sqrt{2}} \rightarrow$$

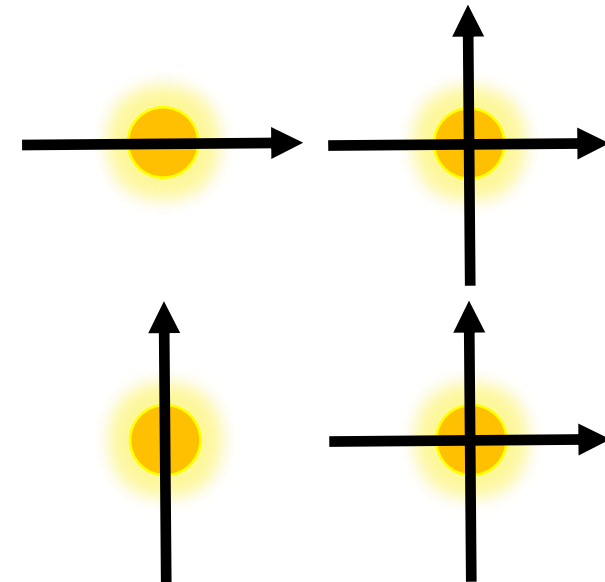
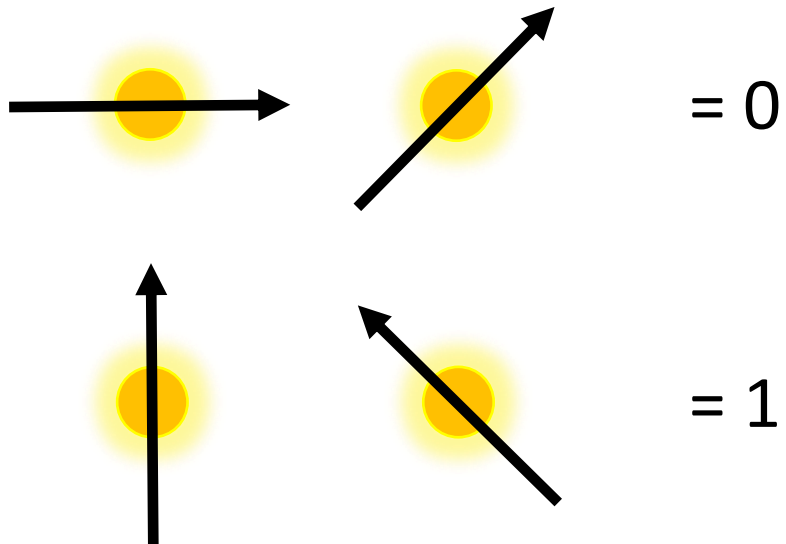


“The probability that, if we make a measurement of the polarisation of the state, we will measure it to be vertically polarised, is one half”

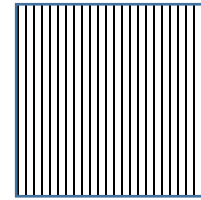
Alice



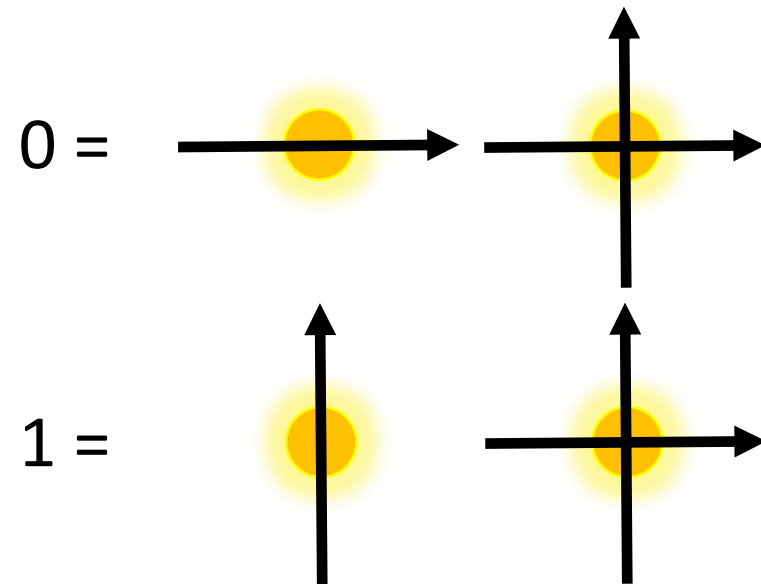
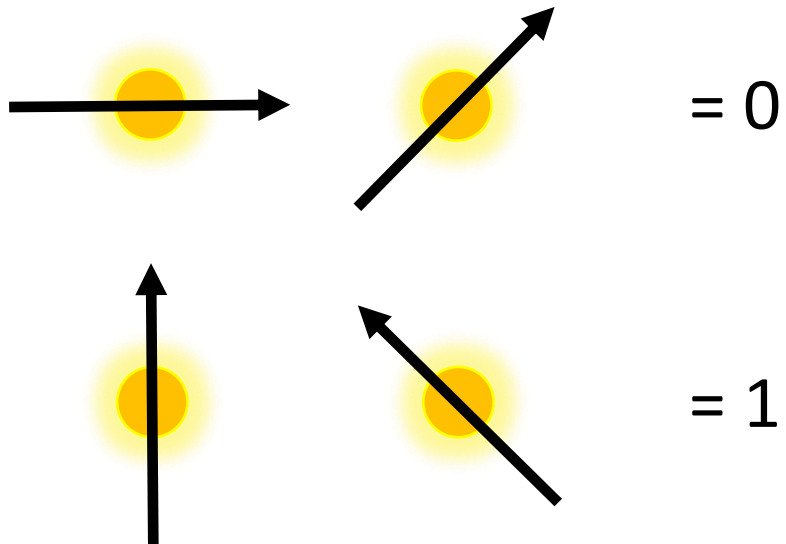
Bob



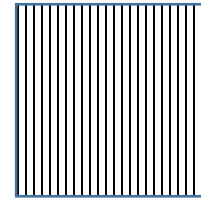
Alice



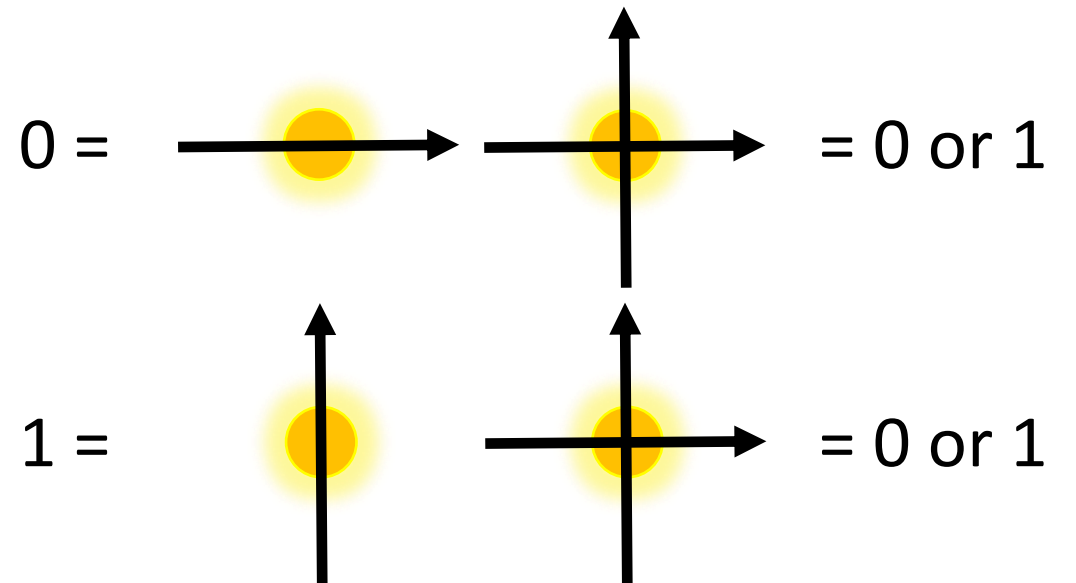
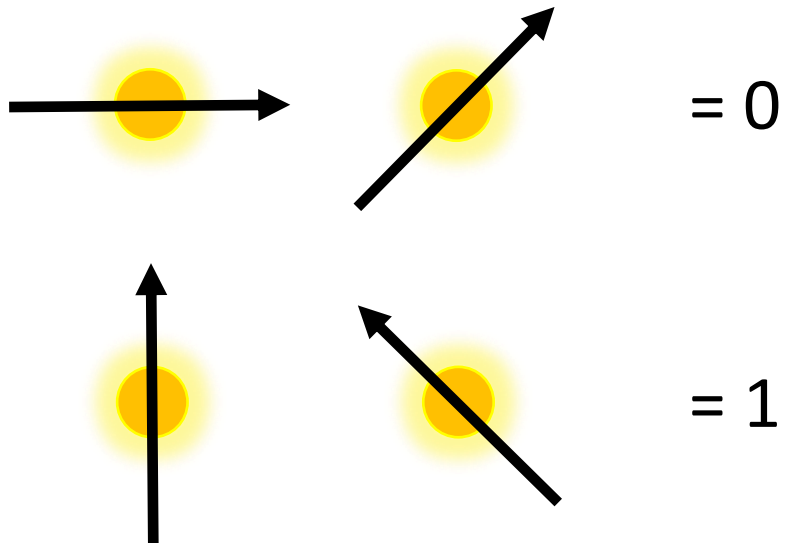
Bob



Alice

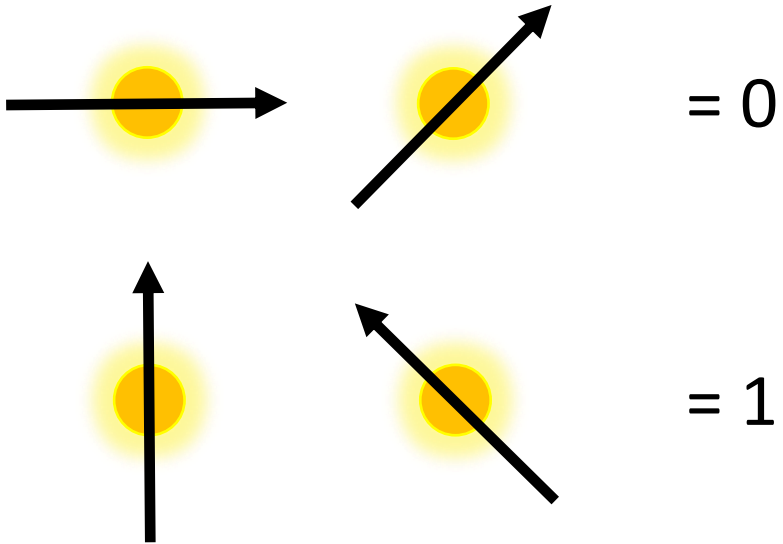


Bob

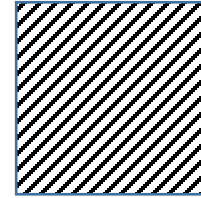


Alice

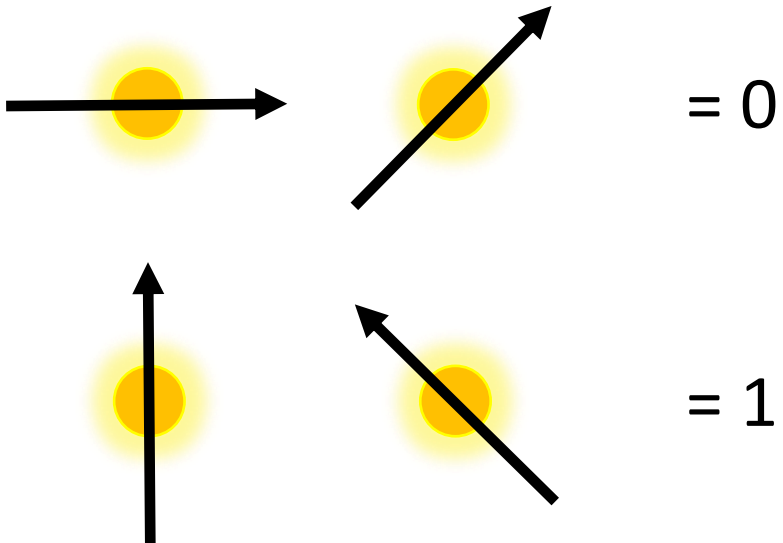
Bob



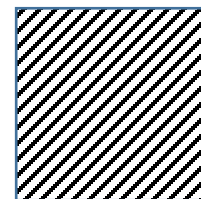
Alice



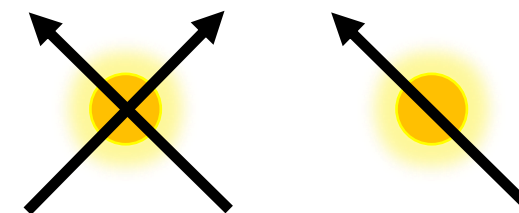
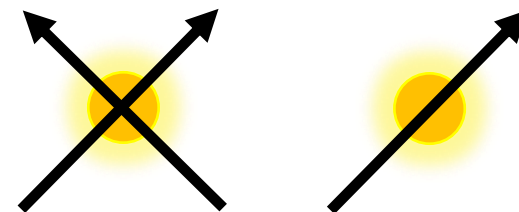
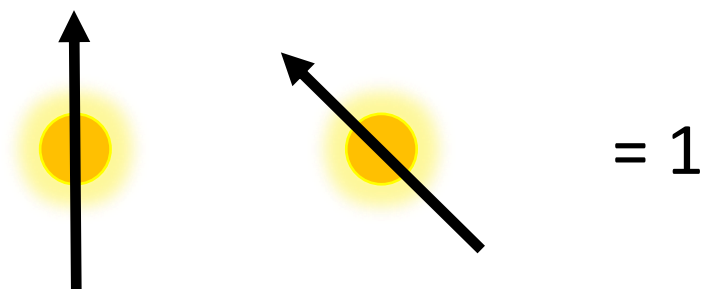
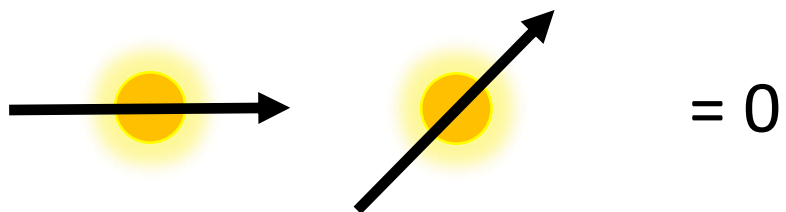
Bob

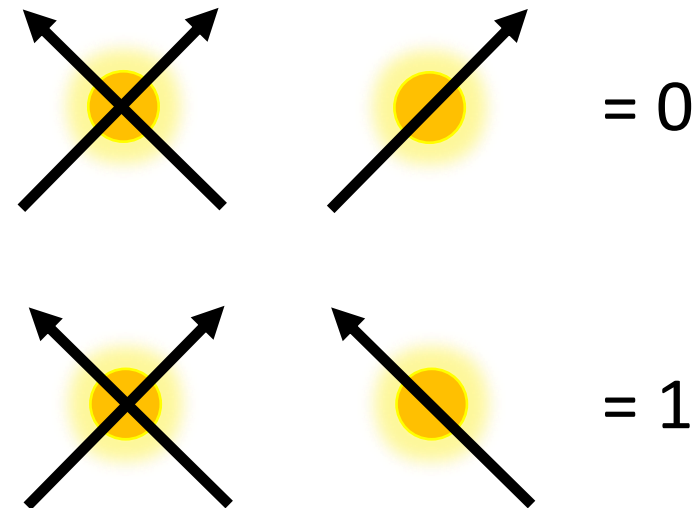
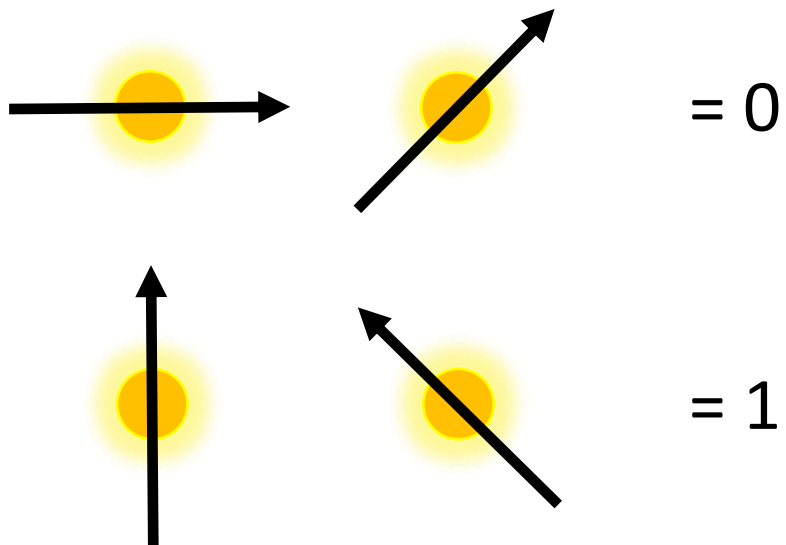
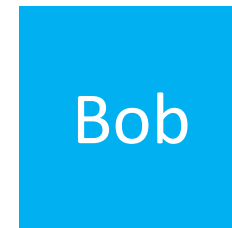
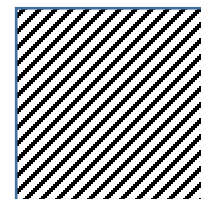


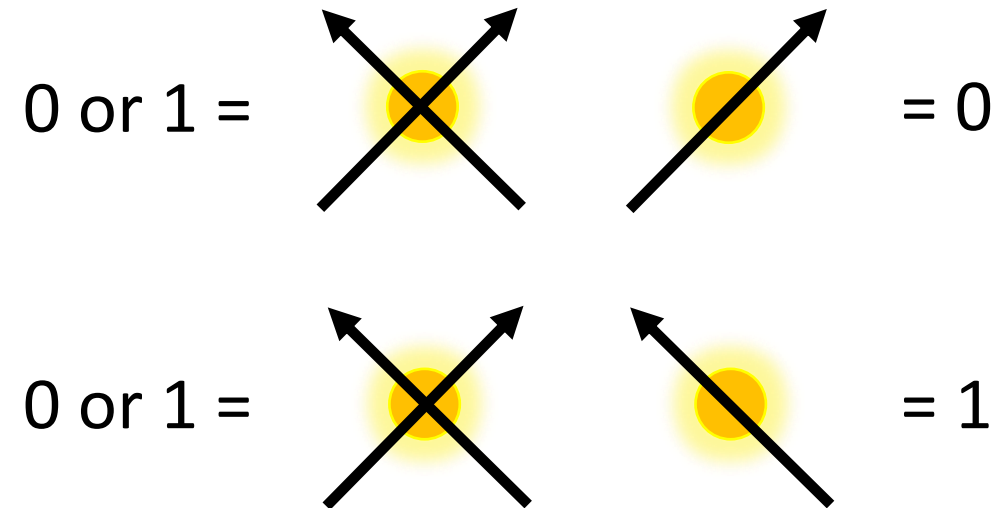
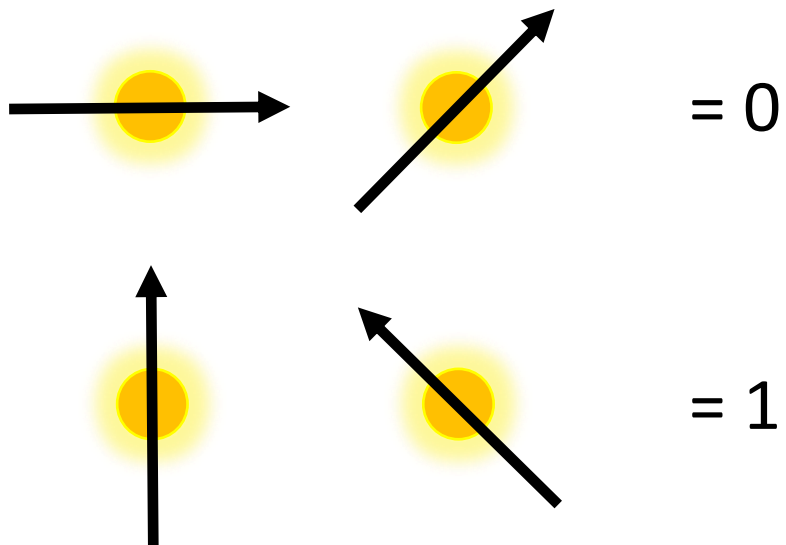
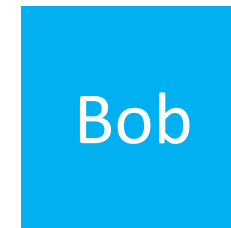
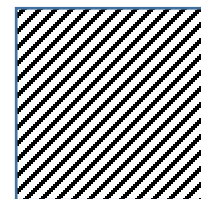
Alice



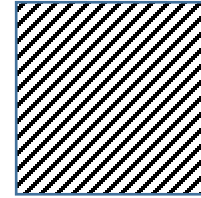
Bob



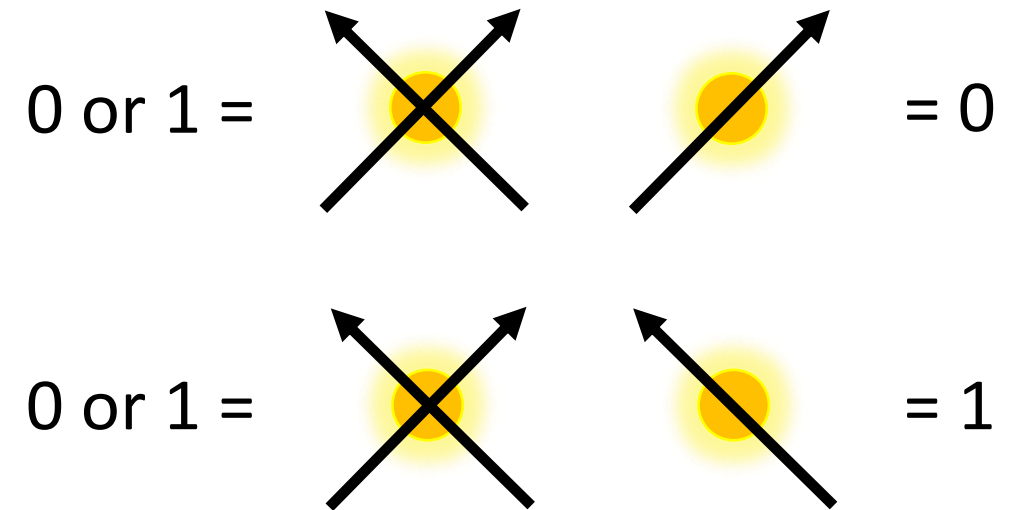
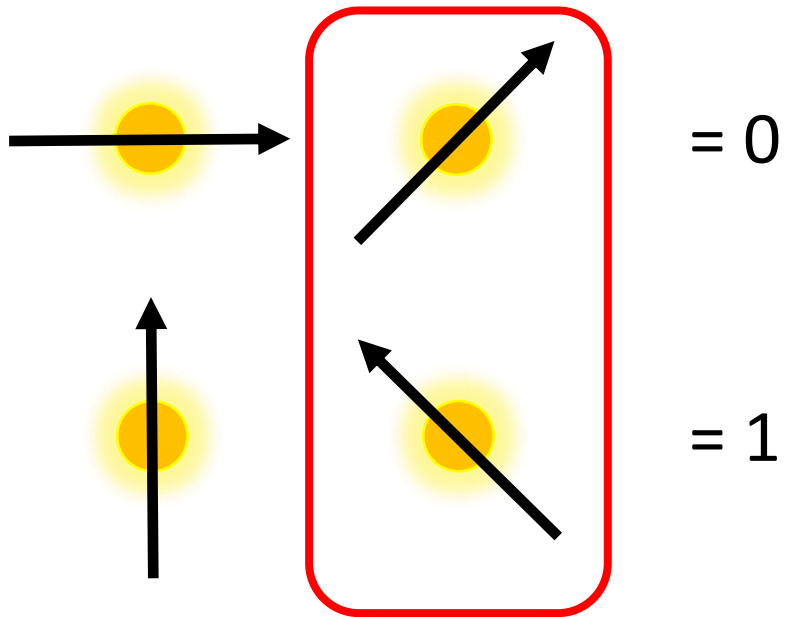




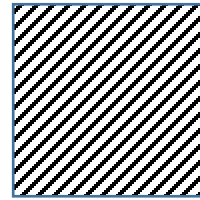
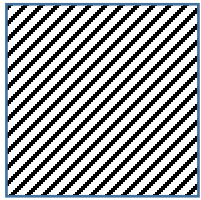
Alice



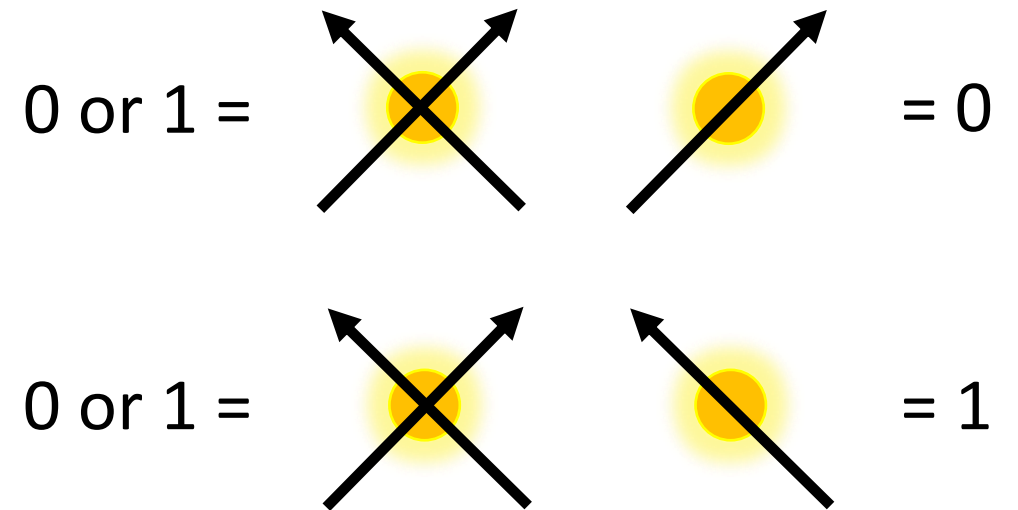
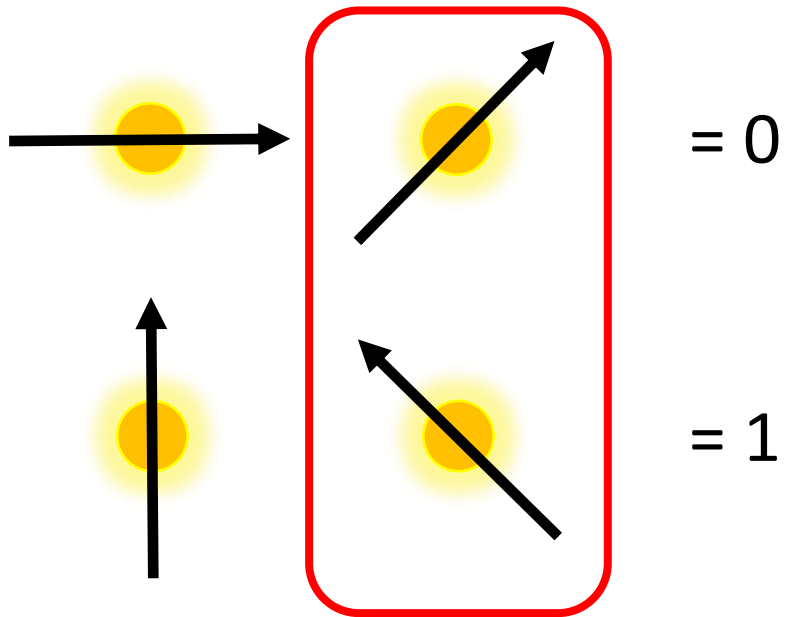
Bob



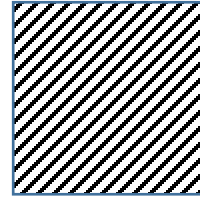
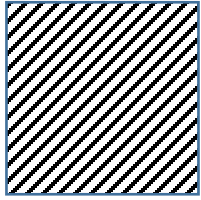
Alice



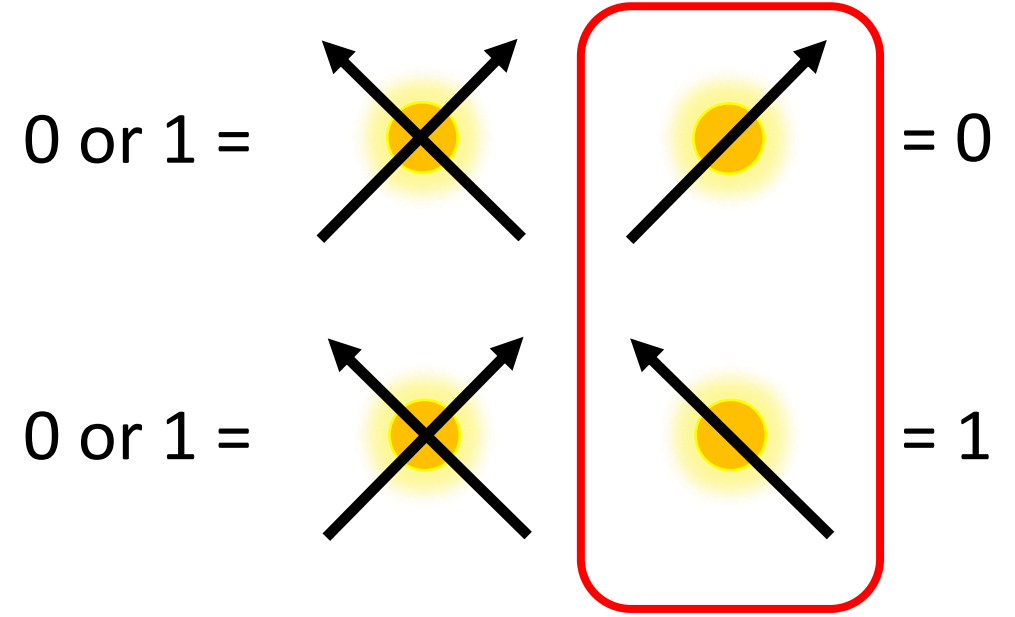
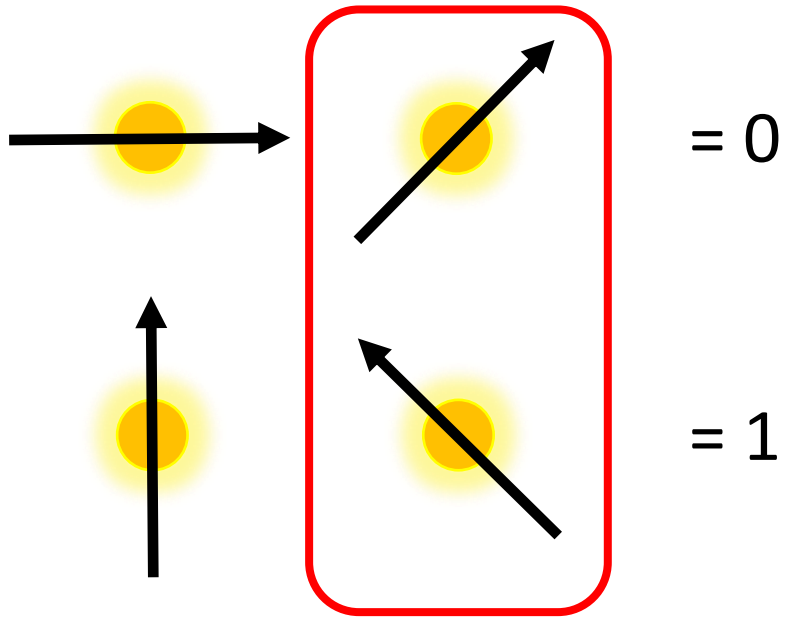
Bob

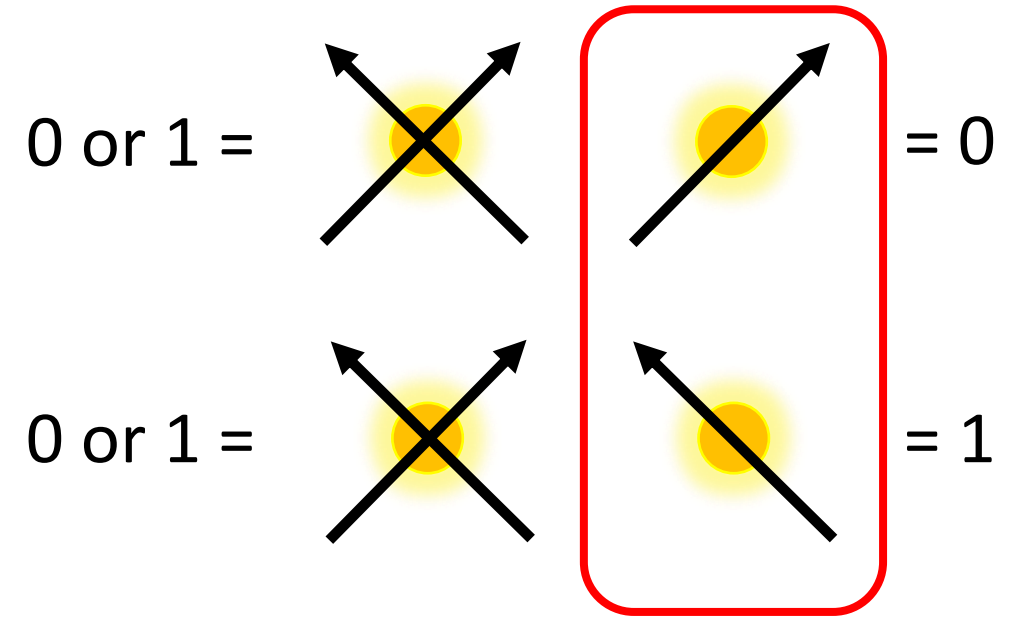
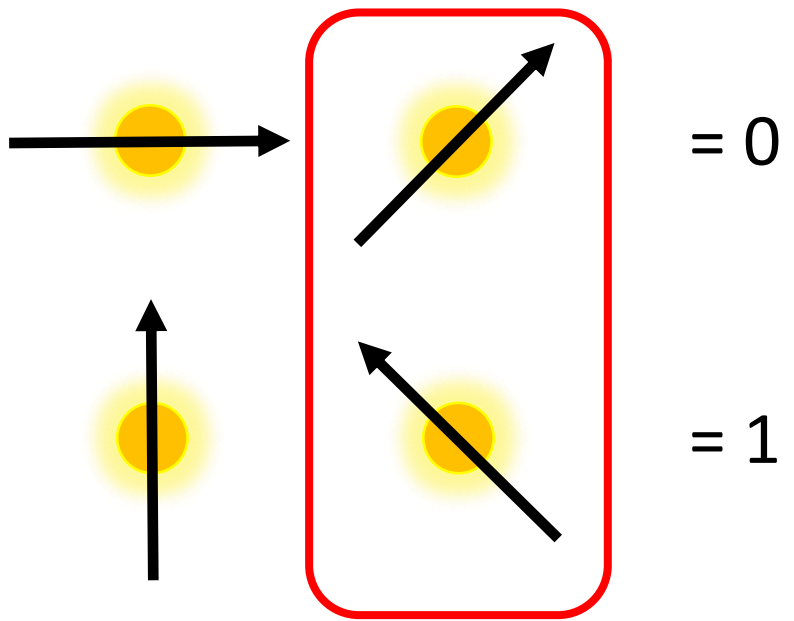
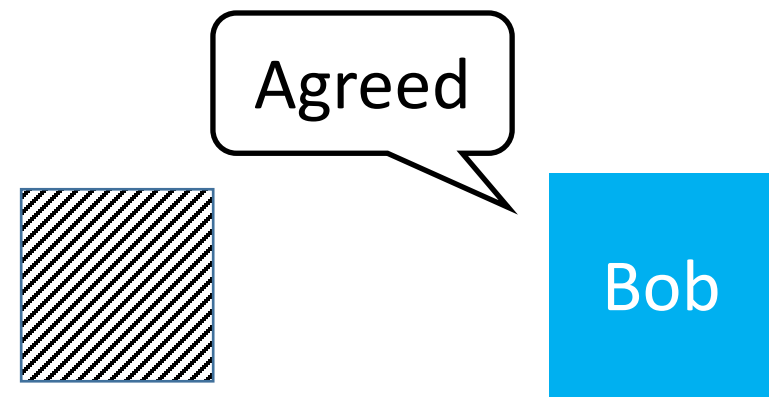
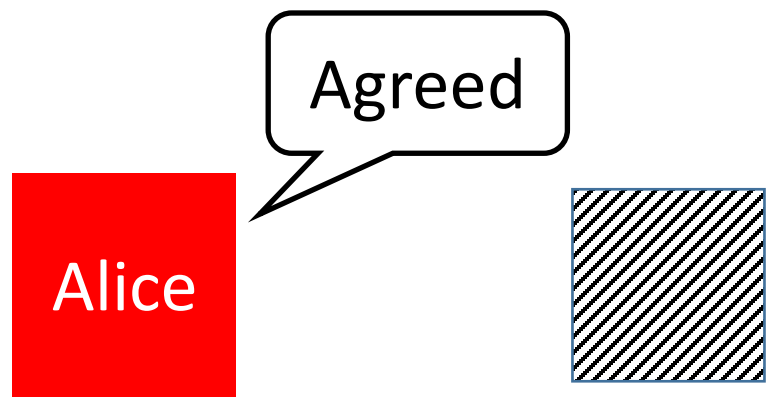


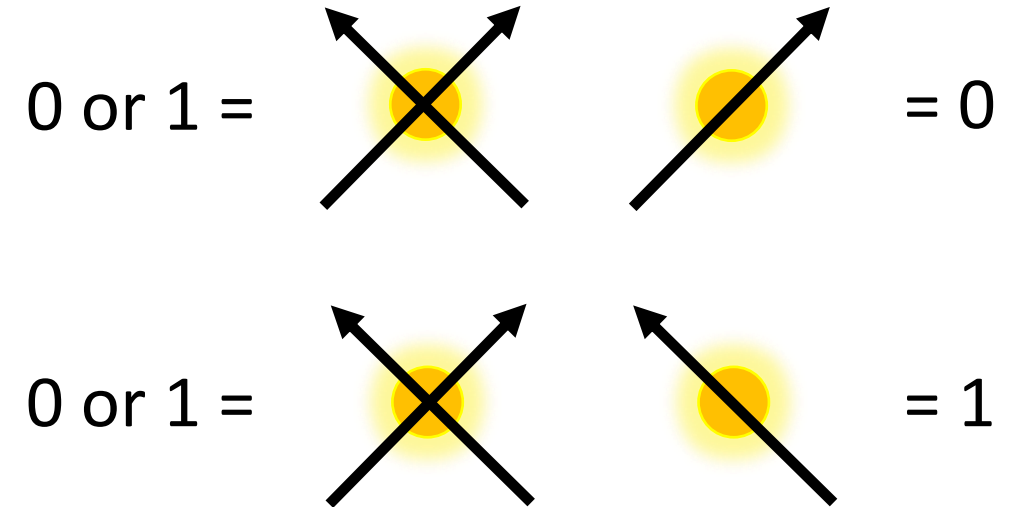
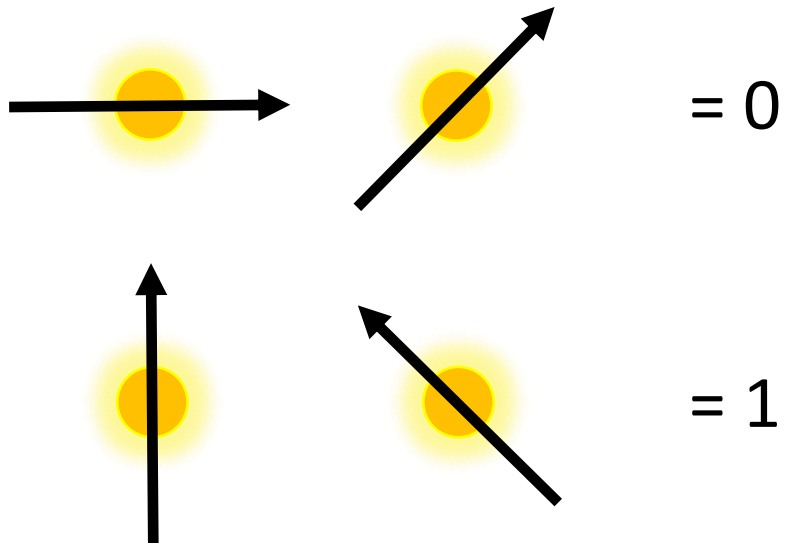
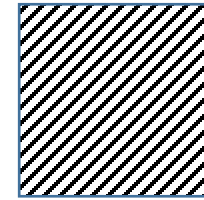
Alice



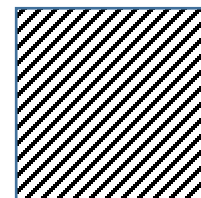
Bob



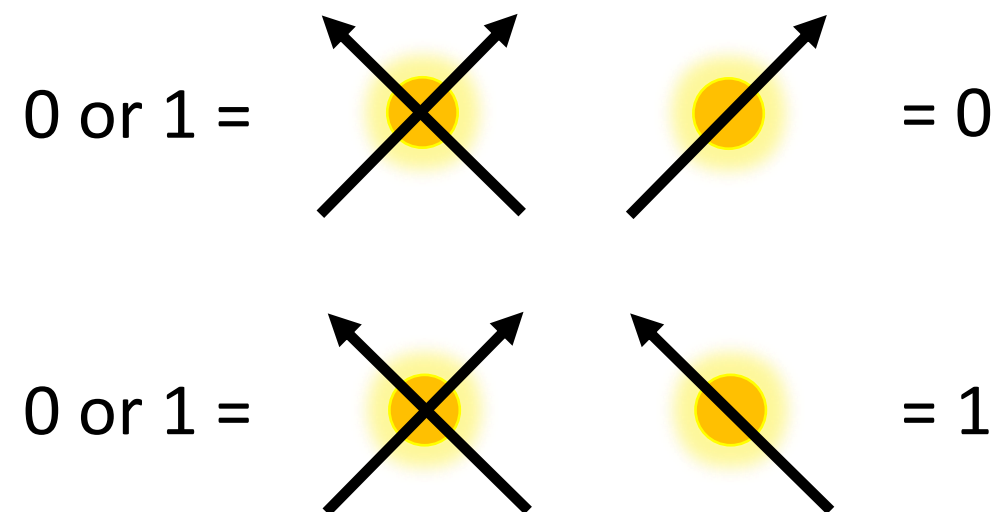
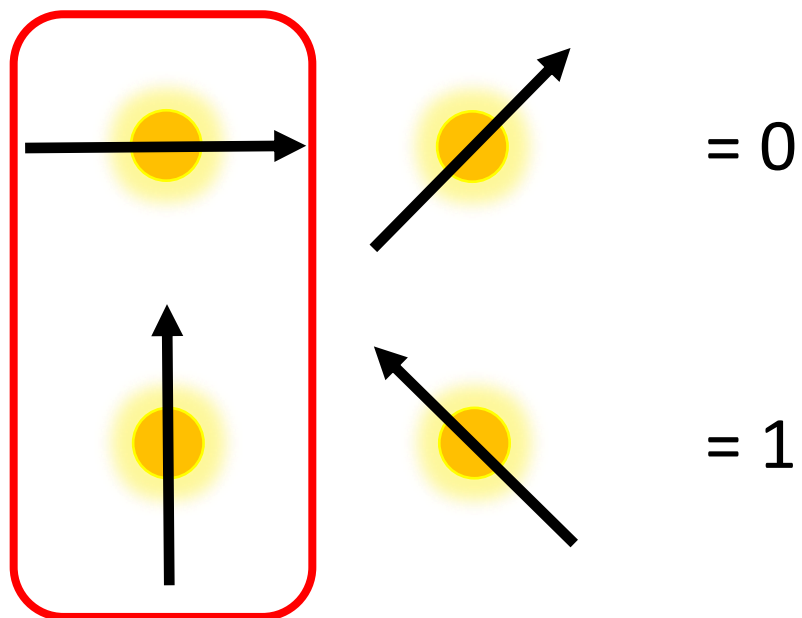




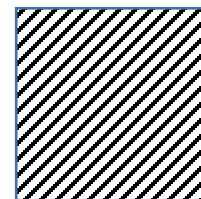
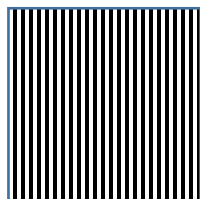
Alice



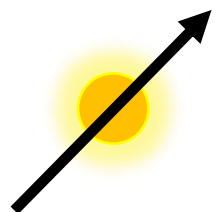
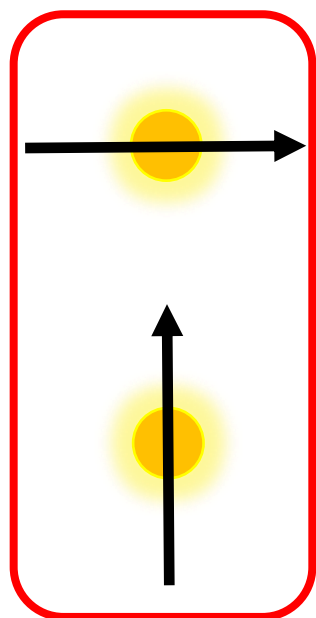
Bob



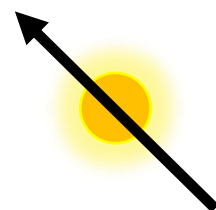
Alice



Bob

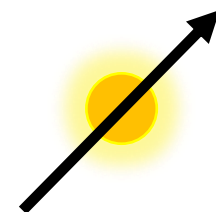
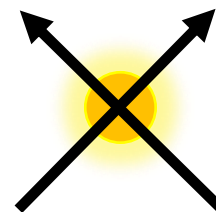


= 0



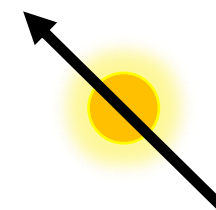
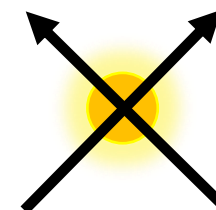
= 1

0 or 1 =



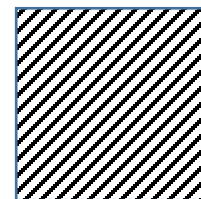
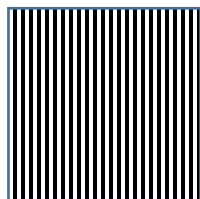
= 0

0 or 1 =

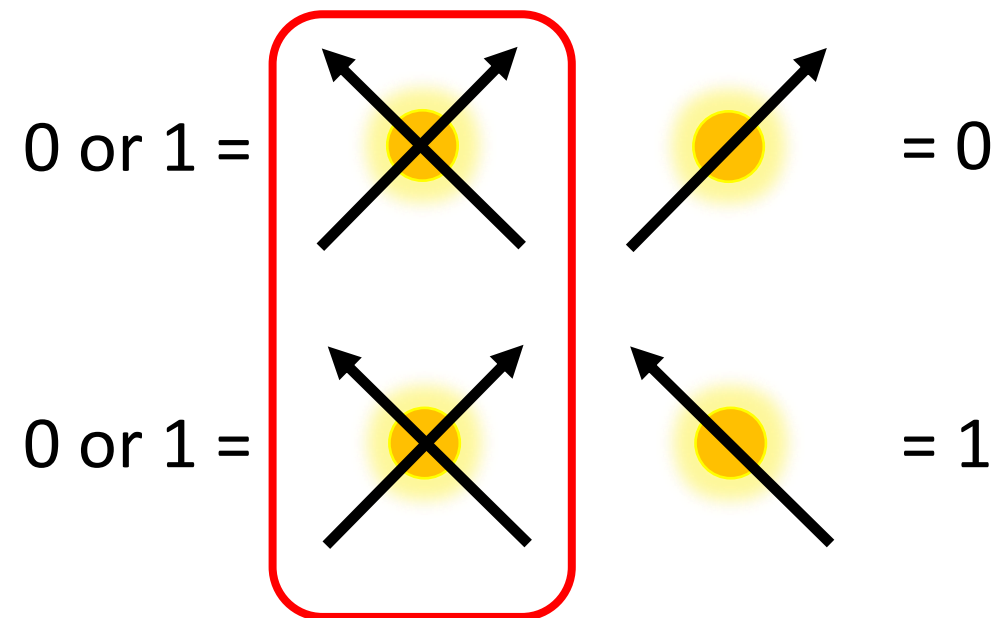
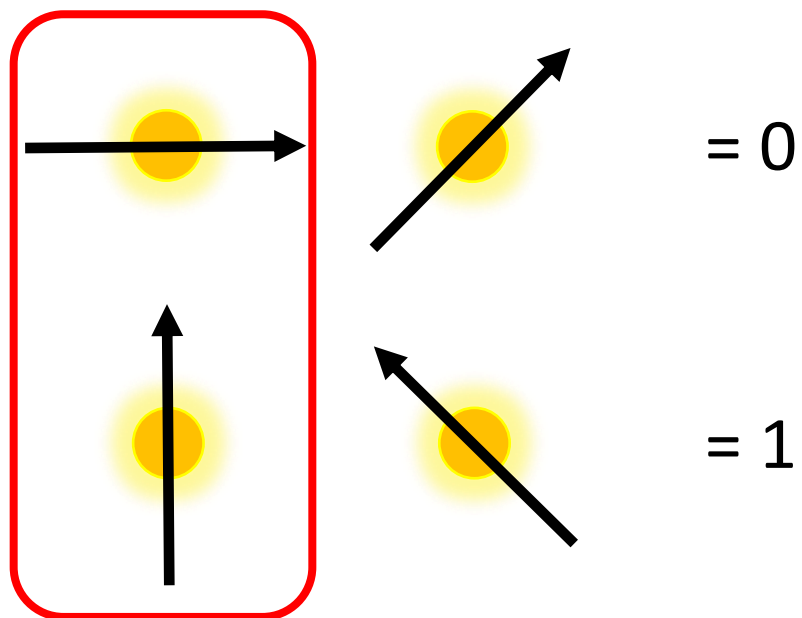


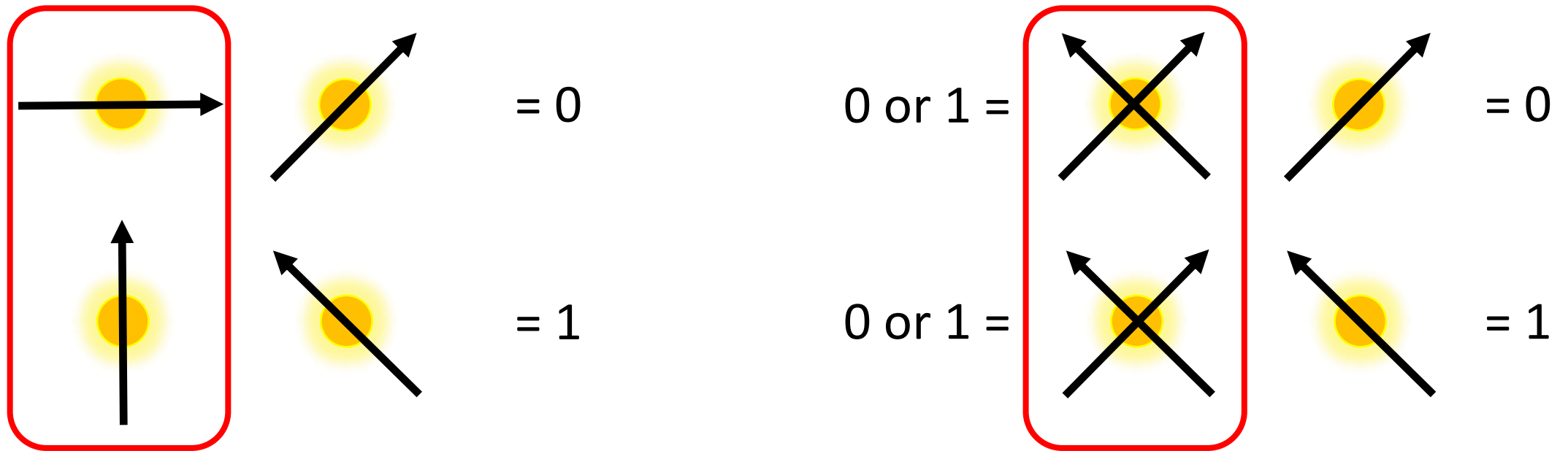
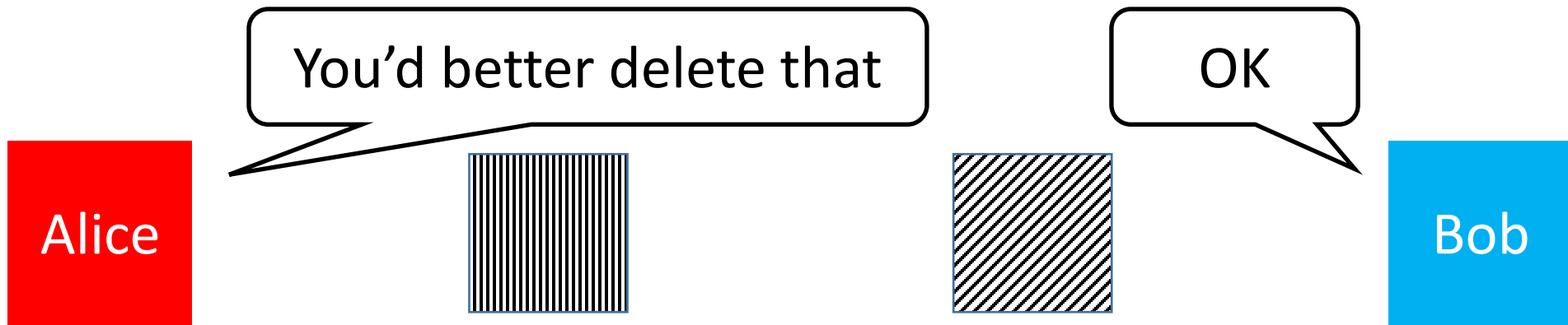
= 1

Alice



Bob





... 0 0 1 1 1 0 1 0 1 1 0 1 0 1 1 0 0 1 0 0 0 ...

... 0 0 1 0 1 0 1 1 1 1 0 0 0 0 1 0 0 1 0 1 0 ...

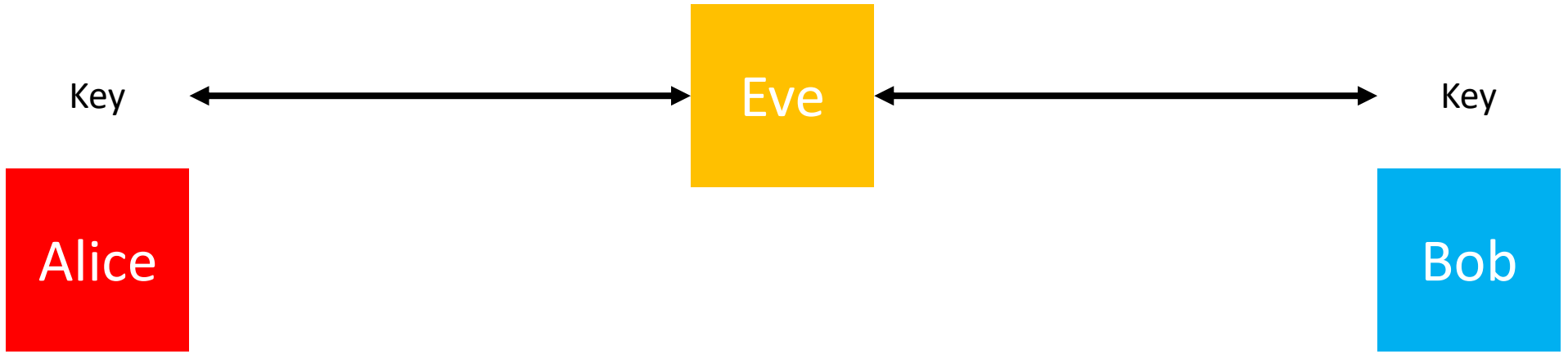
... 0 0 1 1 1 0 1 0 1 1 0 1 0 1 1 0 0 1 0 0 0 ...
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
... 0 0 1 0 1 0 1 1 1 1 0 0 0 0 1 0 0 1 0 1 0 ...

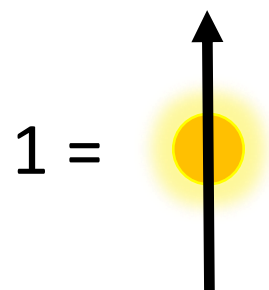
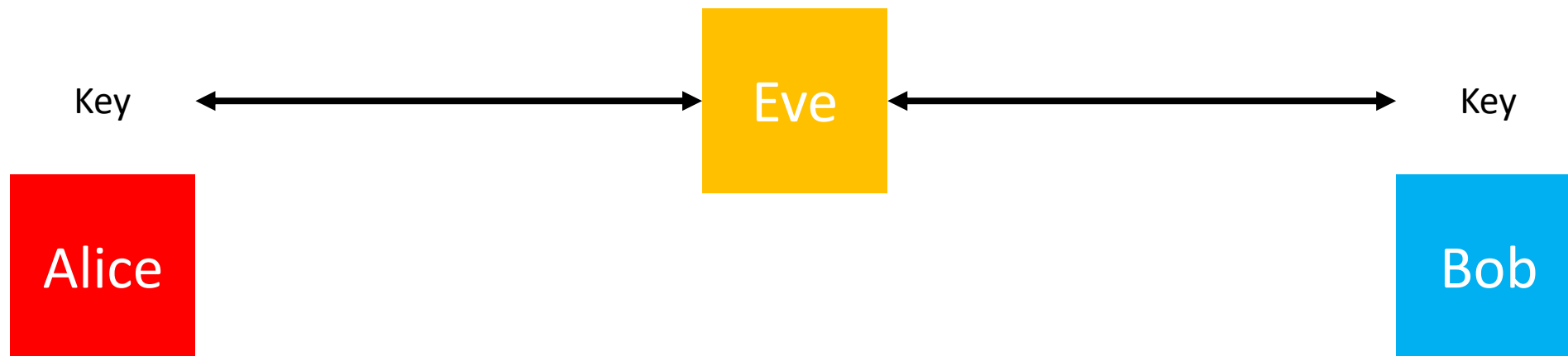
... 0 0 1 1 1 0 1 0 1 1 0 1 0 1 1 0 0 1 0 0 0 ...
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
 ... 0 0 1 0 1 0 1 1 1 1 0 0 0 0 1 0 0 1 0 1 0 ...

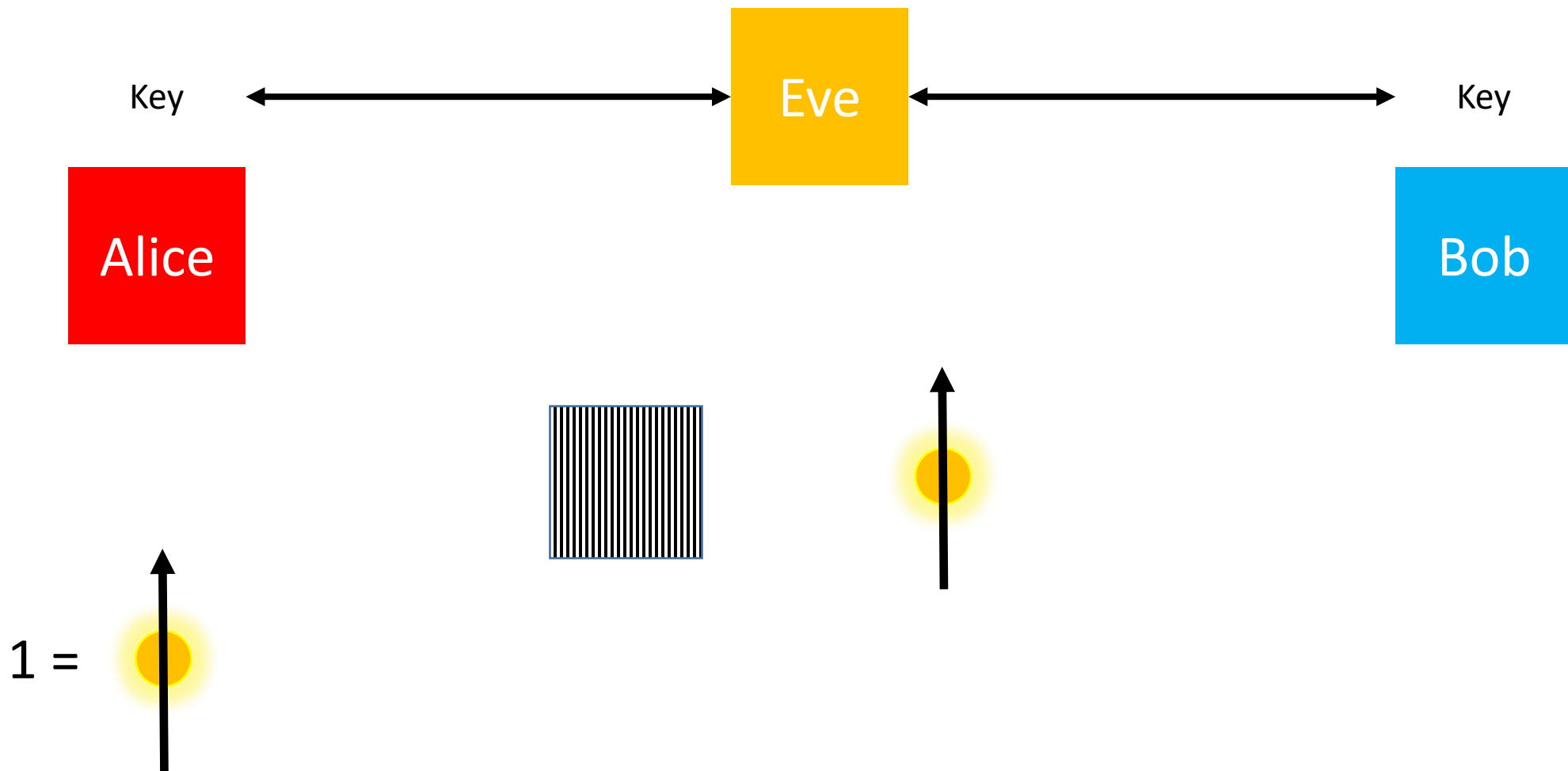
... 0 1 0 1 1 1 0 1 0 1 0 0 ...

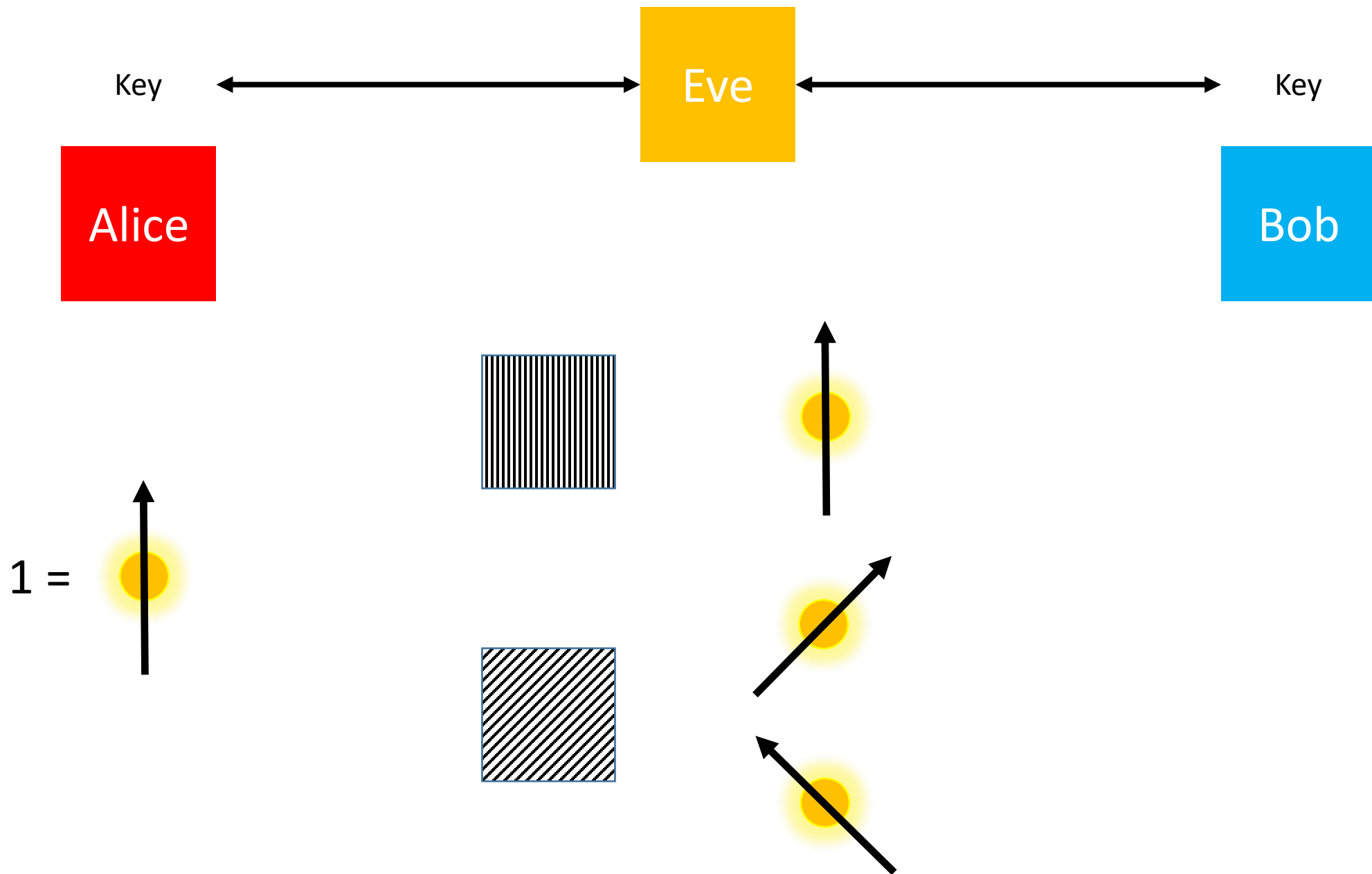
... 0 1 0 1 1 1 0 1 0 1 0 0 ...

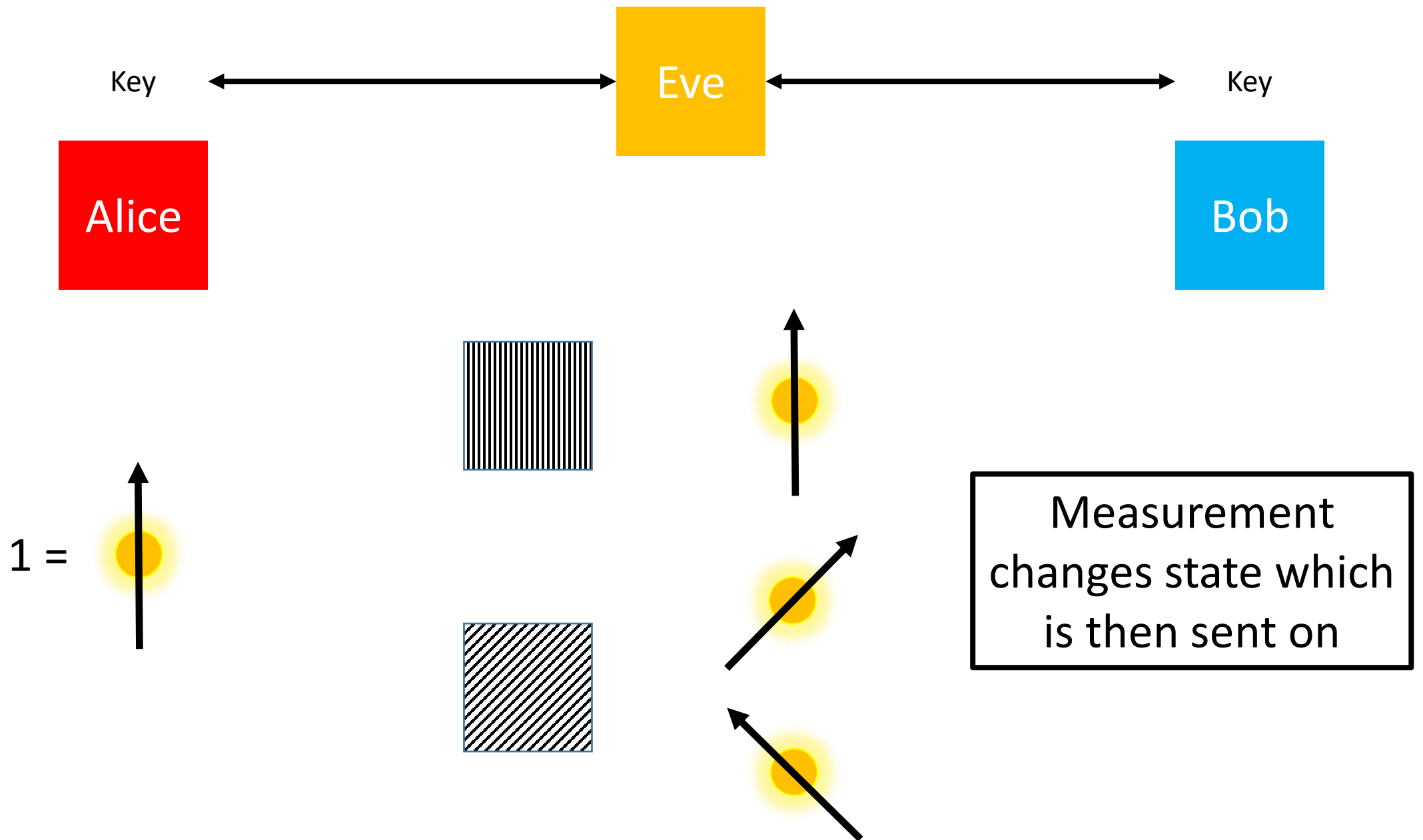


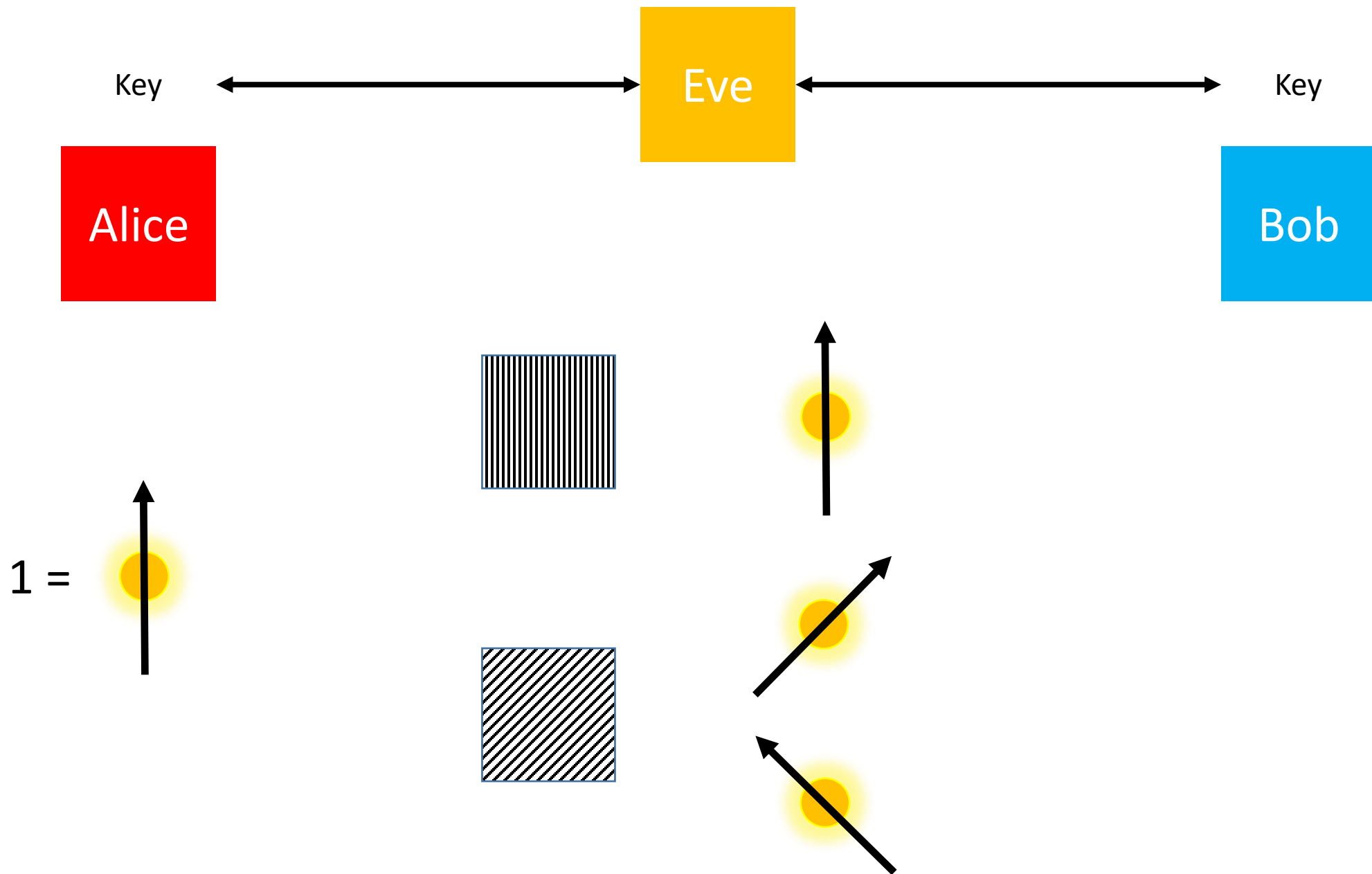


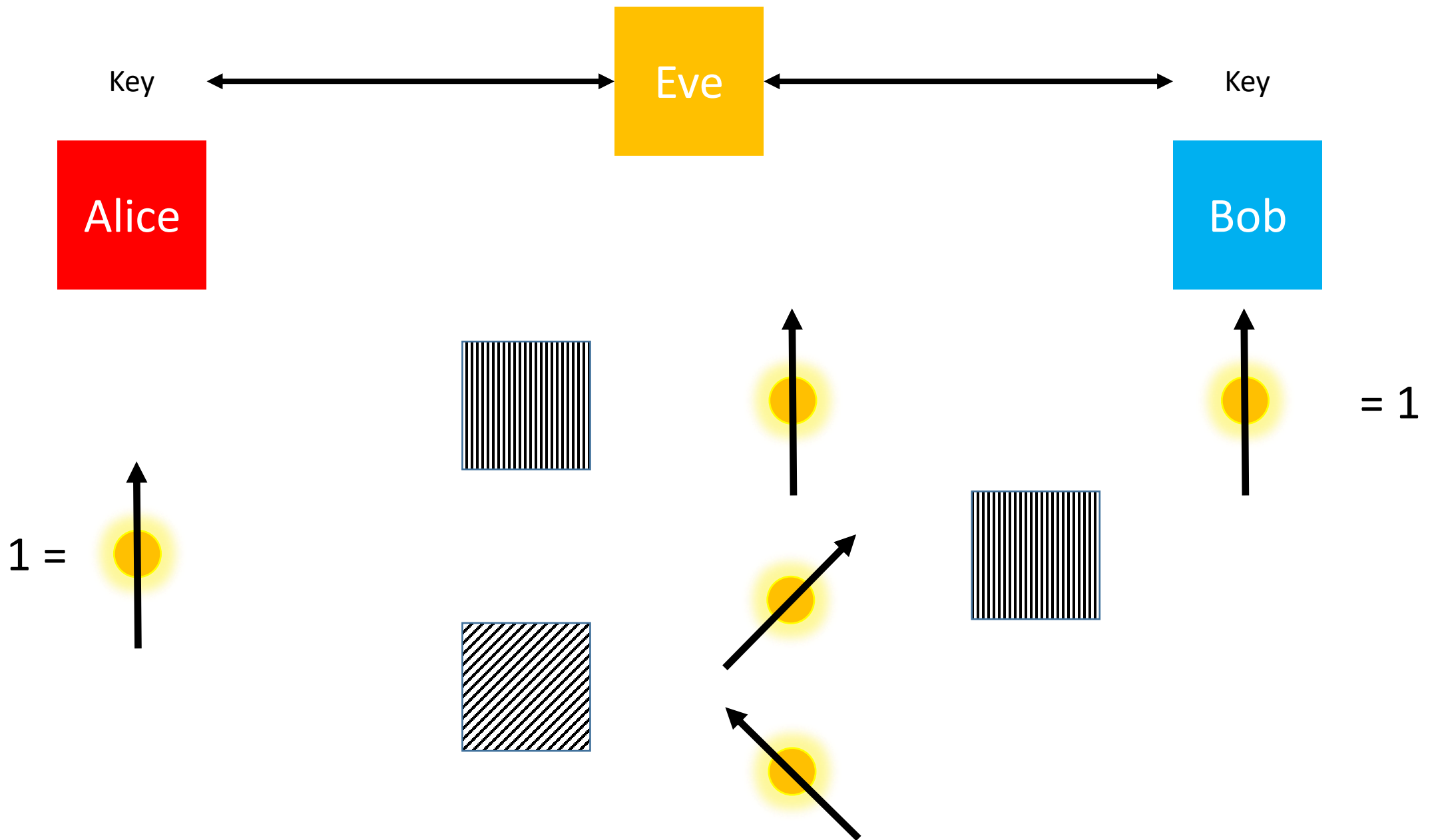


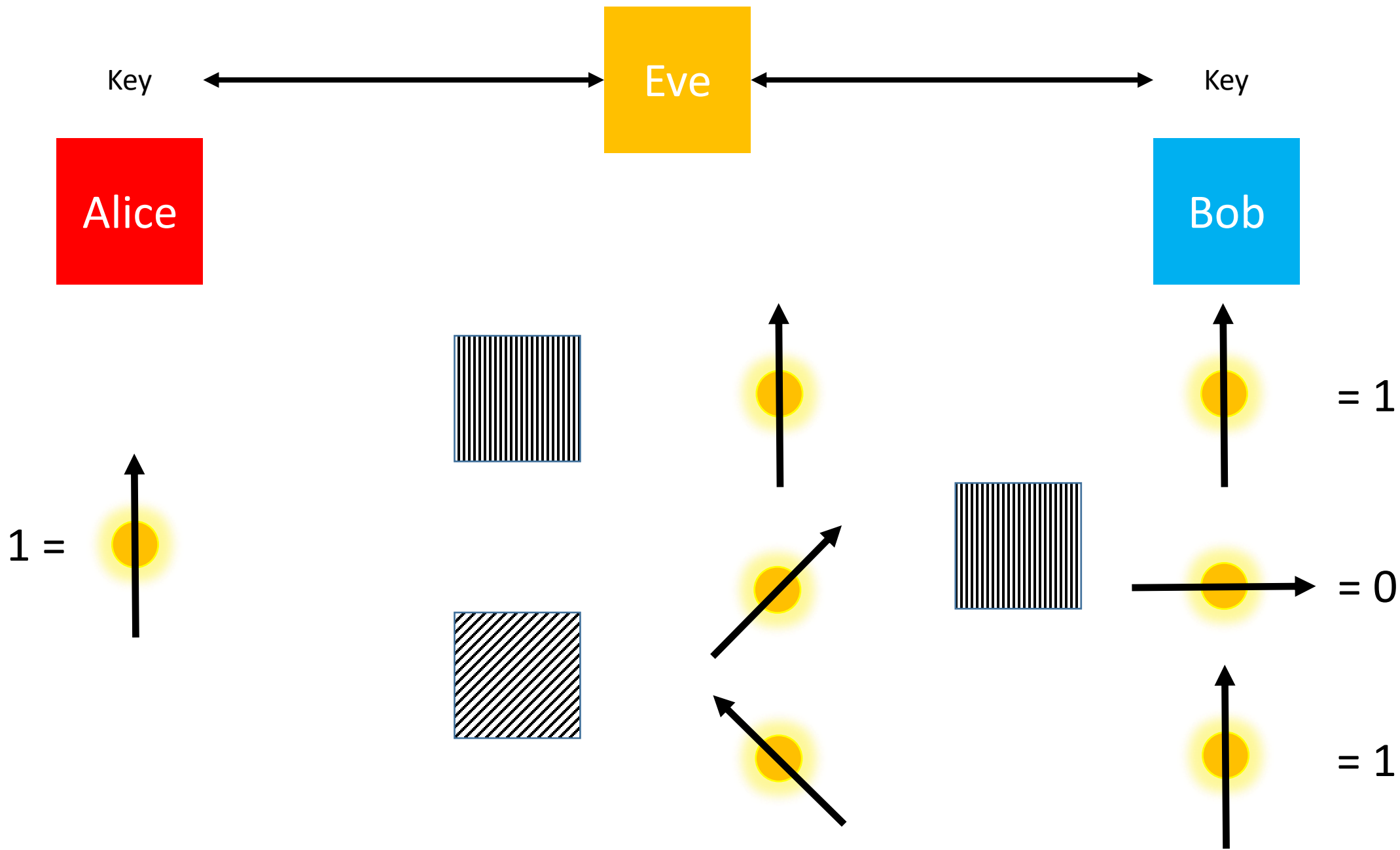












... 0 0 1 1 1 0 1 0 1 1 0 1 0 1 1 0 0 1 0 0 0 ...

... 0 0 1 0 1 0 1 1 1 0 0 0 0 0 1 1 0 1 0 1 0 ...

... 0 0 1 1 1 0 1 0 1 1 0 1 0 1 1 0 0 1 0 0 0 ...
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
... 0 0 1 0 1 0 1 1 1 0 0 0 0 0 1 1 0 1 0 1 0 ...

...	0	0	1	1	1	0	1	0	1	1	0	1	0	1	1	0	0	1	0	0	0	...
	↑			↑	↑		↑			↑	↑	↑		↑			↑		↑			
...	0	0	1	0	1	0	1	1	1	0	0	0	0	0	1	1	0	1	0	1	0	...

... 0 1 0 1 1 1 0 1 0 1 0 0 ...

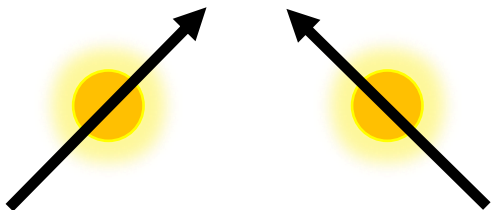
... 0 1 0 1 1 0 0 1 1 1 0 0 ...

...	0	0	1	1	1	0	1	0	1	1	0	1	0	1	1	0	0	1	0	0	0	...	
	↑			↑	↑		↑				↑	↑	↑				↑			↑			
...	0	0	1	0	1	0	1	1	1	0	0	0	0	0	0	1	1	0	1	0	1	0	...

...	0	1	0	1	1	1	0	1	0	1	0	0	...
...	0	1	0	1	1	0	0	1	1	1	0	0	...

Two Particle Systems

Leaving the realm of classical



The diagram illustrates the multiplication of two Pauli matrices. On the left, two Pauli matrices are shown as yellow circles with black arrows. The first arrow points diagonally up and to the right, and the second arrow points diagonally up and to the left. These are followed by an equals sign. To the right of the equals sign, the first Pauli matrix is expanded into a sum of two terms: a vertical arrow pointing up and a horizontal arrow pointing right. This sum is enclosed in large parentheses. The second Pauli matrix is similarly expanded into a sum of two terms: a vertical arrow pointing up and a horizontal arrow pointing left. This sum is also enclosed in large parentheses. The entire expression represents the distributive property of matrix multiplication.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right) \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right)$$

Diagrammatic equation showing the expansion of a two-particle interaction into a sum of four terms.

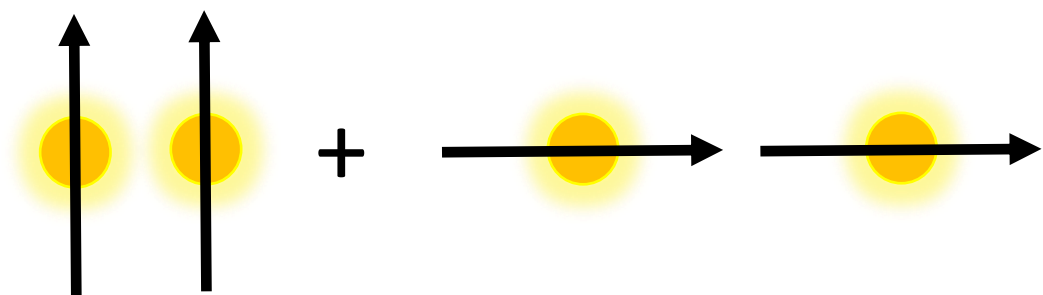
The first row shows the initial state (two particles with diagonal arrows) equal to the product of two sums:

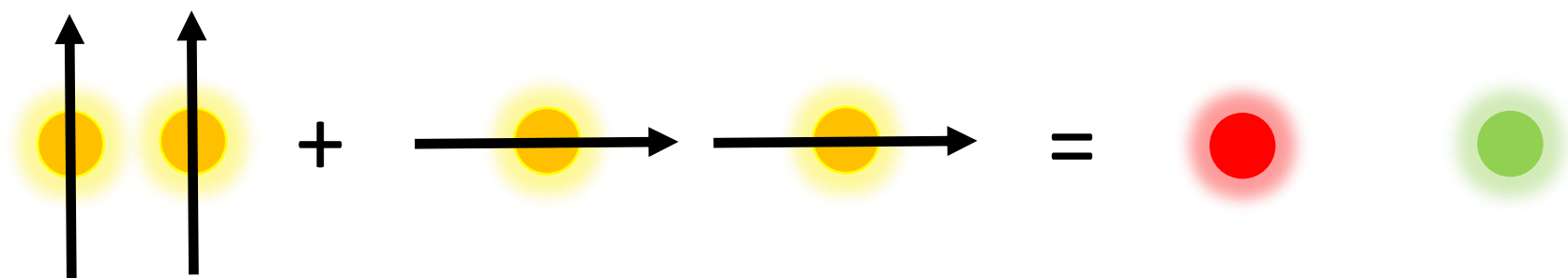
$$= \left(\begin{array}{c} \uparrow \\ \bullet \end{array} + \begin{array}{c} \rightarrow \\ \bullet \end{array} \right) \left(\begin{array}{c} \uparrow \\ \bullet \end{array} + \begin{array}{c} \leftarrow \\ \bullet \end{array} \right)$$

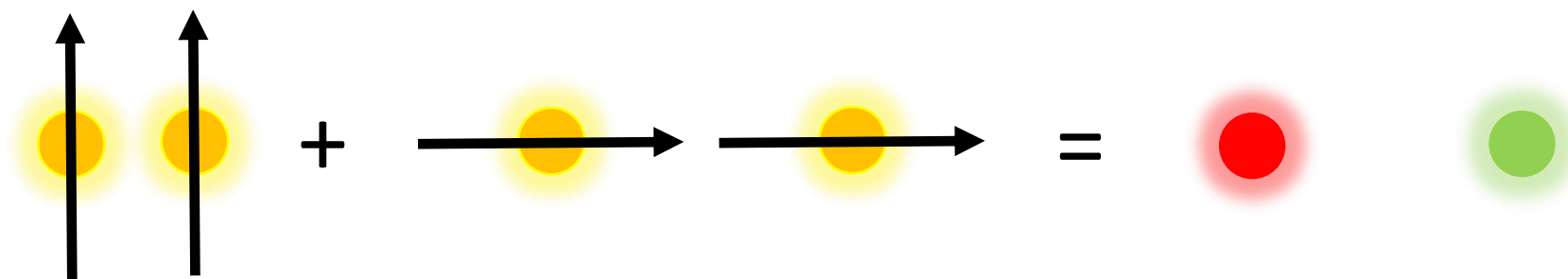
The second row shows the expansion of the product into four terms:

$$= \begin{array}{c} \uparrow \\ \bullet \end{array} \begin{array}{c} \uparrow \\ \bullet \end{array} + \begin{array}{c} \uparrow \\ \bullet \end{array} \begin{array}{c} \leftarrow \\ \bullet \end{array} + \begin{array}{c} \rightarrow \\ \bullet \end{array} \begin{array}{c} \uparrow \\ \bullet \end{array} + \begin{array}{c} \rightarrow \\ \bullet \end{array} \begin{array}{c} \leftarrow \\ \bullet \end{array}$$

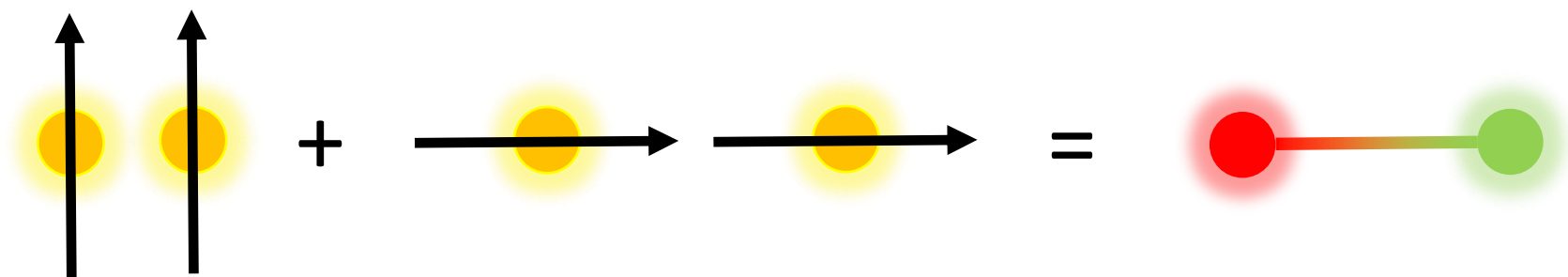
The diagram uses yellow circles with black outlines to represent particles, and black arrows to represent their states. The arrows are either vertical (up or down) or horizontal (left or right). The first row shows two particles with diagonal arrows. The second row shows four terms, each with two particles and vertical arrows. The third row shows two terms, each with two particles and horizontal arrows.

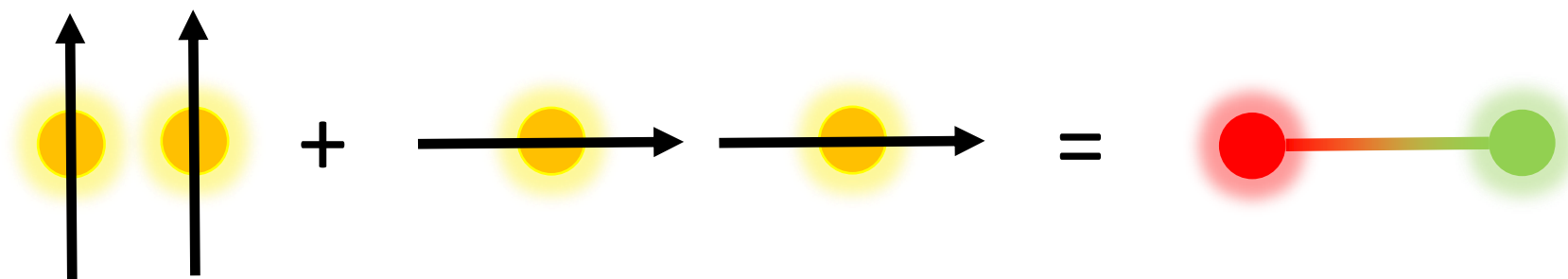




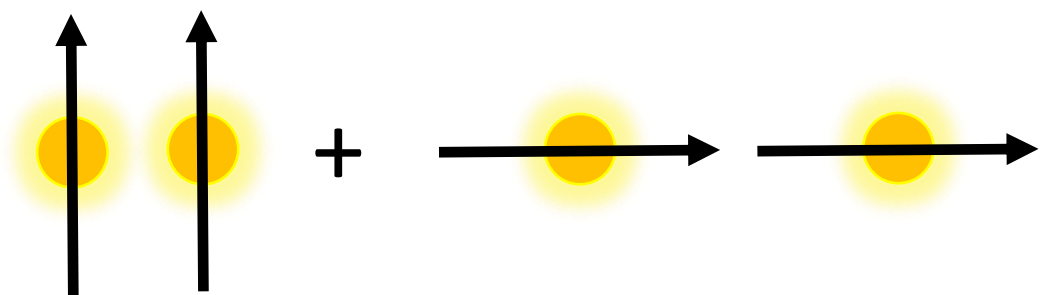


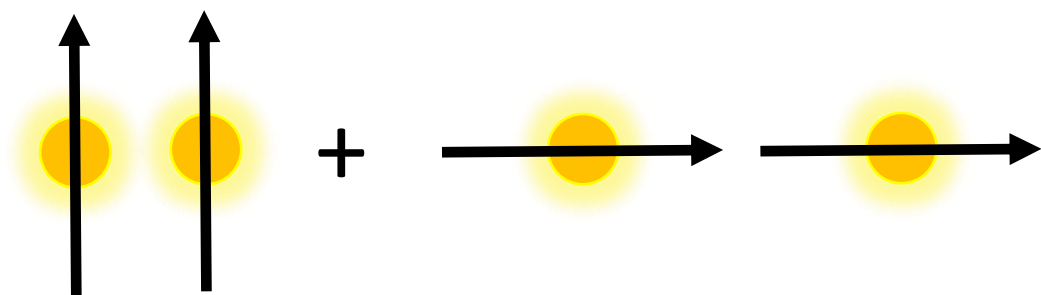
IMPOSSIBLE





ENTANGLEMENT





$$P(\uparrow\uparrow) = \frac{1}{2}$$

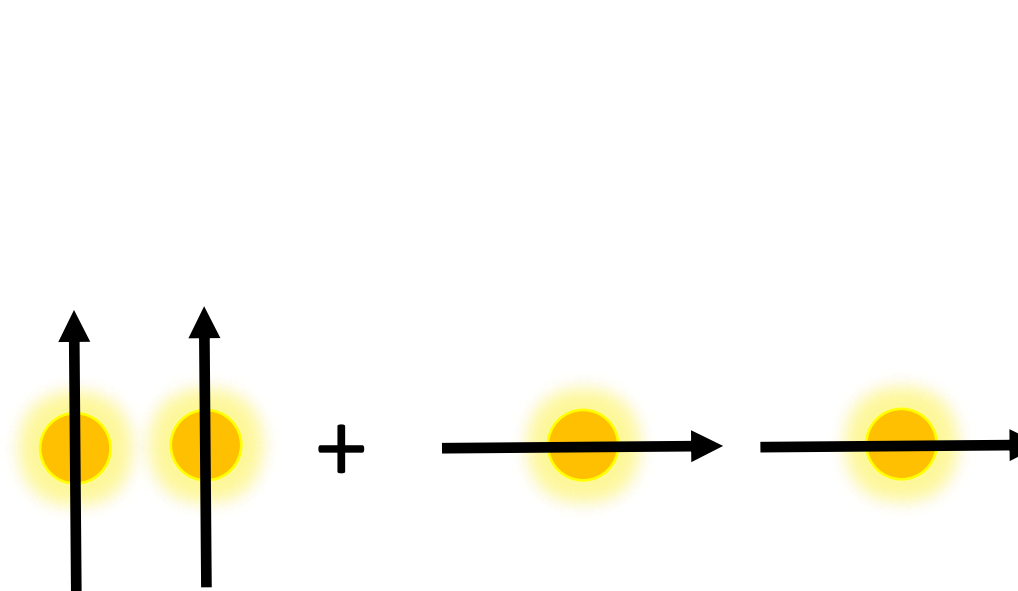


Diagram illustrating a quantum state or process. It shows two vertical arrows pointing up, followed by a plus sign, and then two horizontal arrows pointing right.

$$P(\uparrow \uparrow) = \frac{1}{2}$$

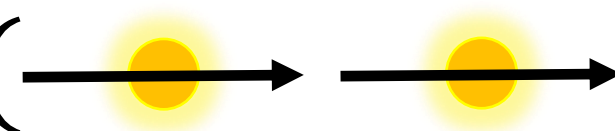
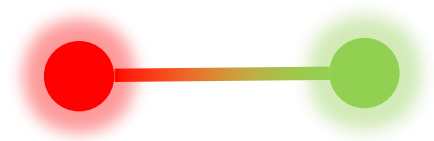
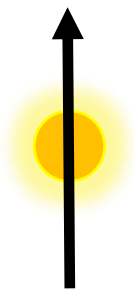


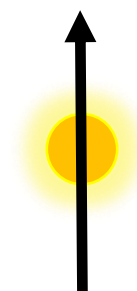
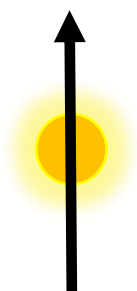
Diagram illustrating a quantum state or process. It shows two horizontal arrows pointing right.

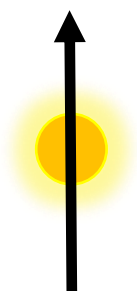
$$P(\rightarrow \rightarrow) = \frac{1}{2}$$



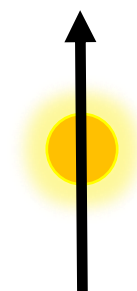


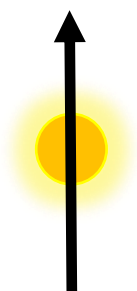






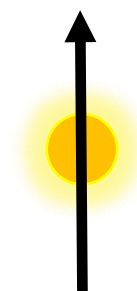
Faster than light communication!

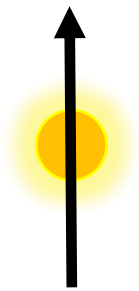




Faster than light communication!

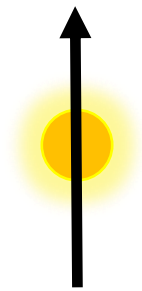
wrong





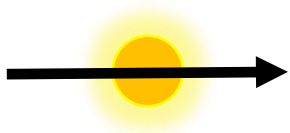
Faster than light communication!

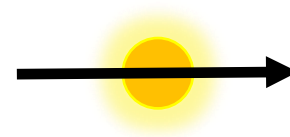
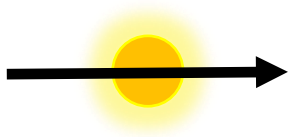
Wrong

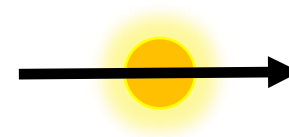
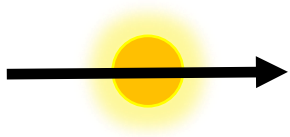


Non-local influences \neq information travels faster than the speed of light





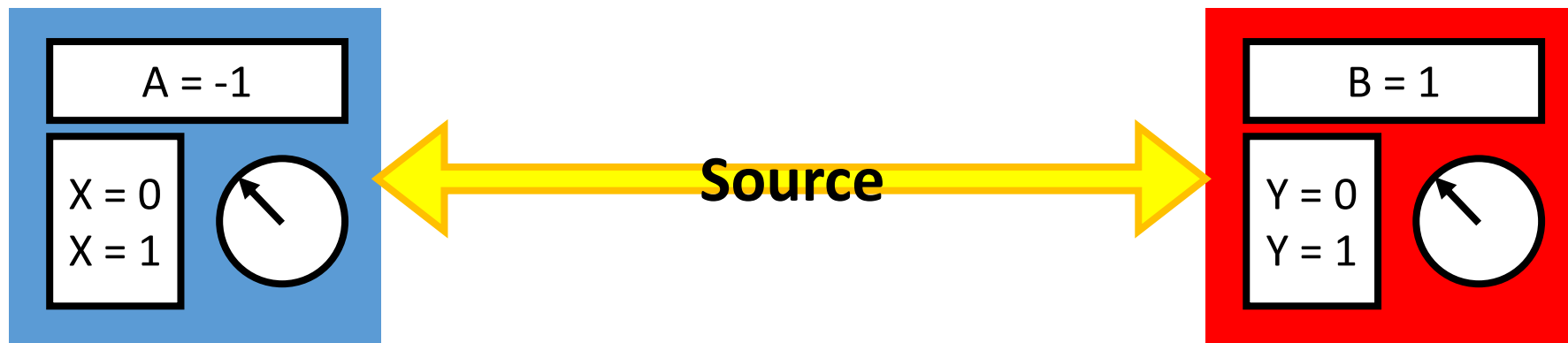


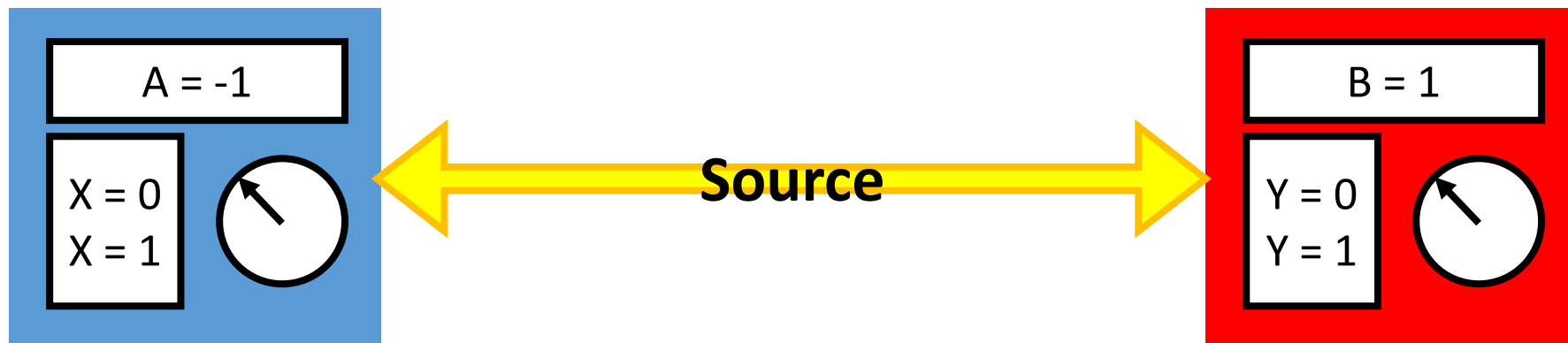


Bell's Test

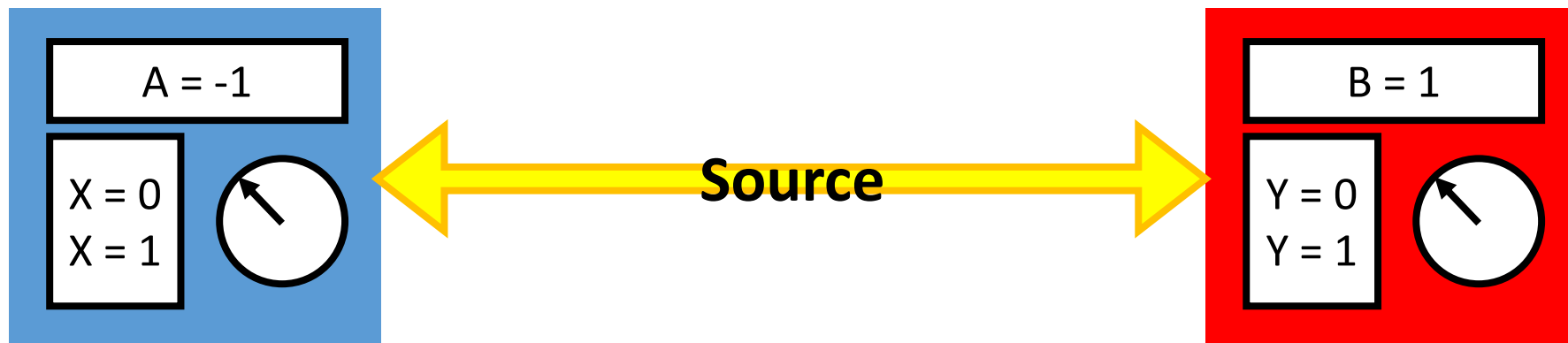
Bell's test

A test for weirdness



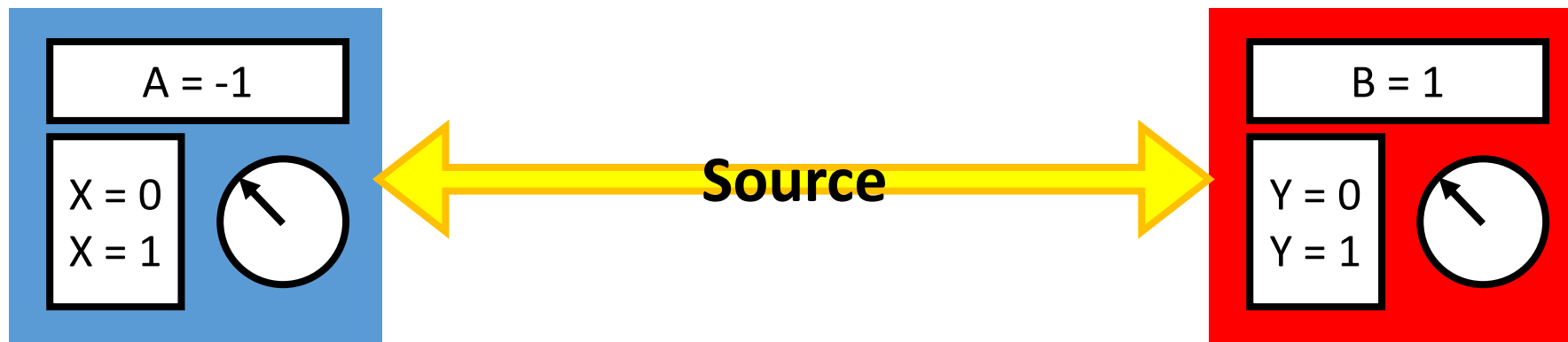


$$P_{XY}(A, B)$$



$$P_{XY}(A, B)$$

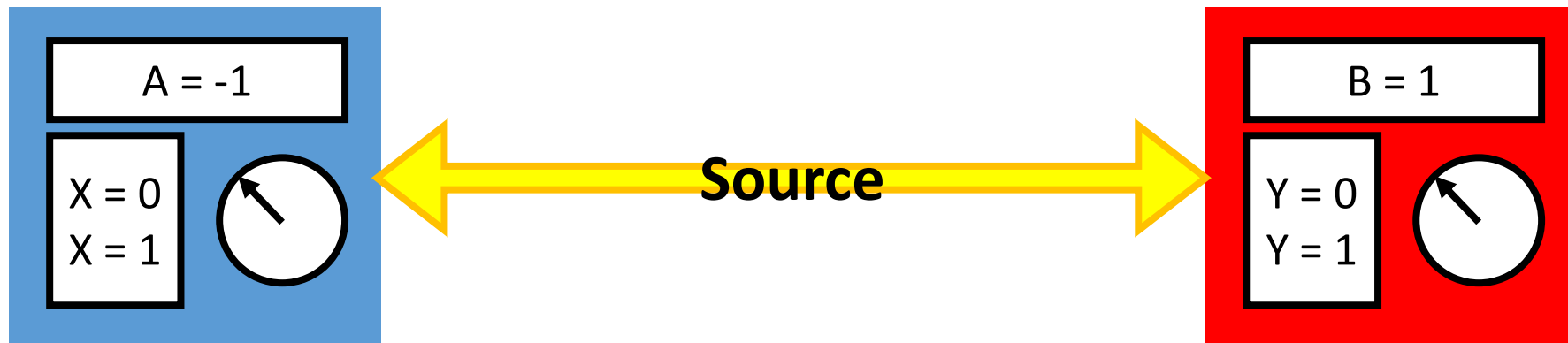
Property 1 means non-local



$$P_{XY}(A, B)$$

Property 1 means non-local

Property 2 means local

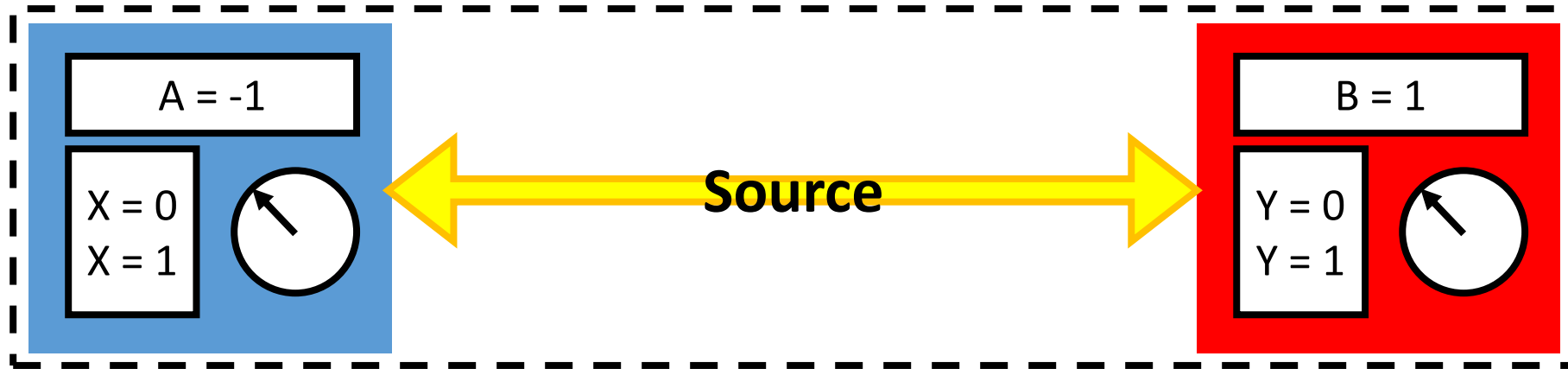


$$P_{XY}(A, B)$$

Property 1 means non-local

Property 2 means local

2015



$$P_{XY}(A, B)$$

Property 1 means non-local

Property 2 means local

My Dissertation

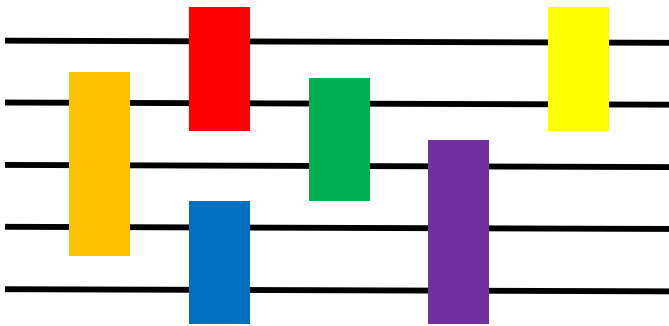
A new measure of weirdness

The Setting

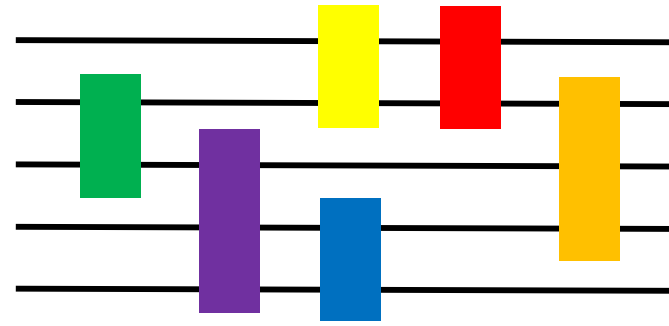
- **Restricted** models of quantum computers may appear **sooner**
- How do we **know** we have built one if we are only classical?
Hypothesis test!

Instantaneous Quantum Polytime Machine

- Uses **commuting** gates
 - Can be applied in any order
 - Can apply gates **instantaneously**



=



- Not classically simulable
- Easier to implement experimentally

A Hypothesis Test

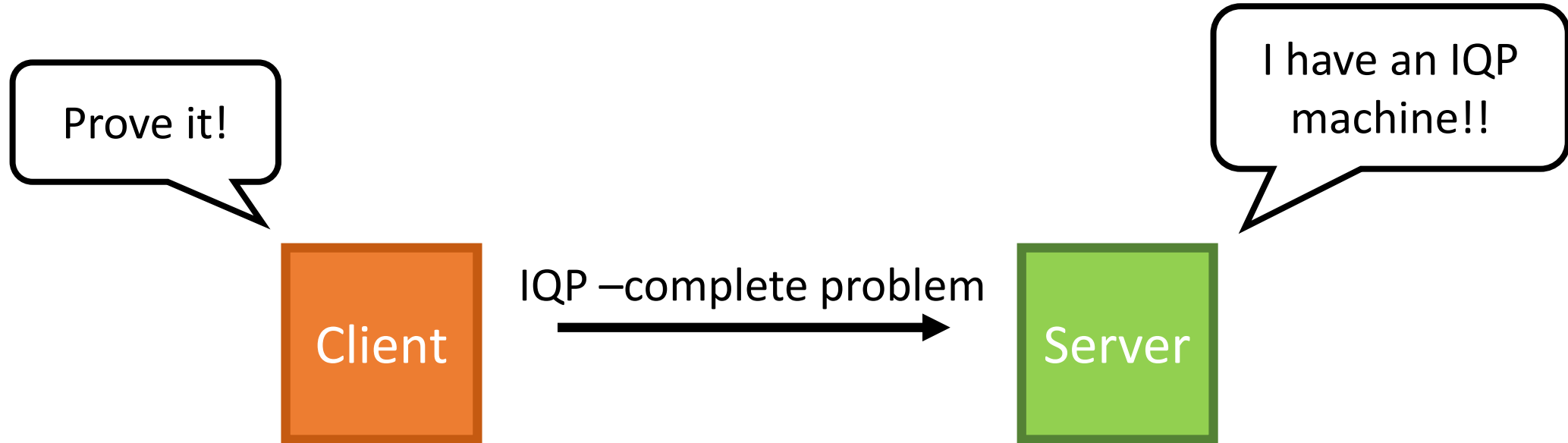
Prove it!

Client

I have an IQP
machine!!

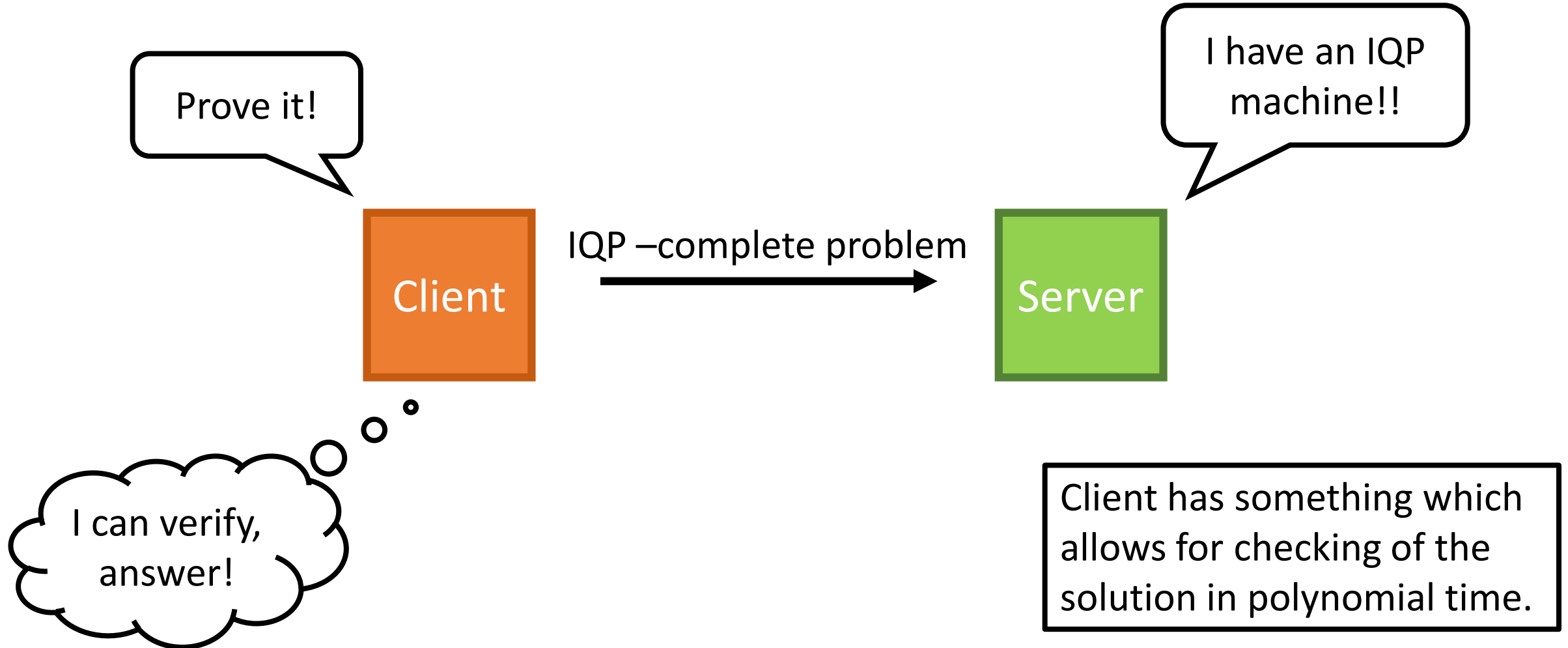
Server

A Hypothesis Test

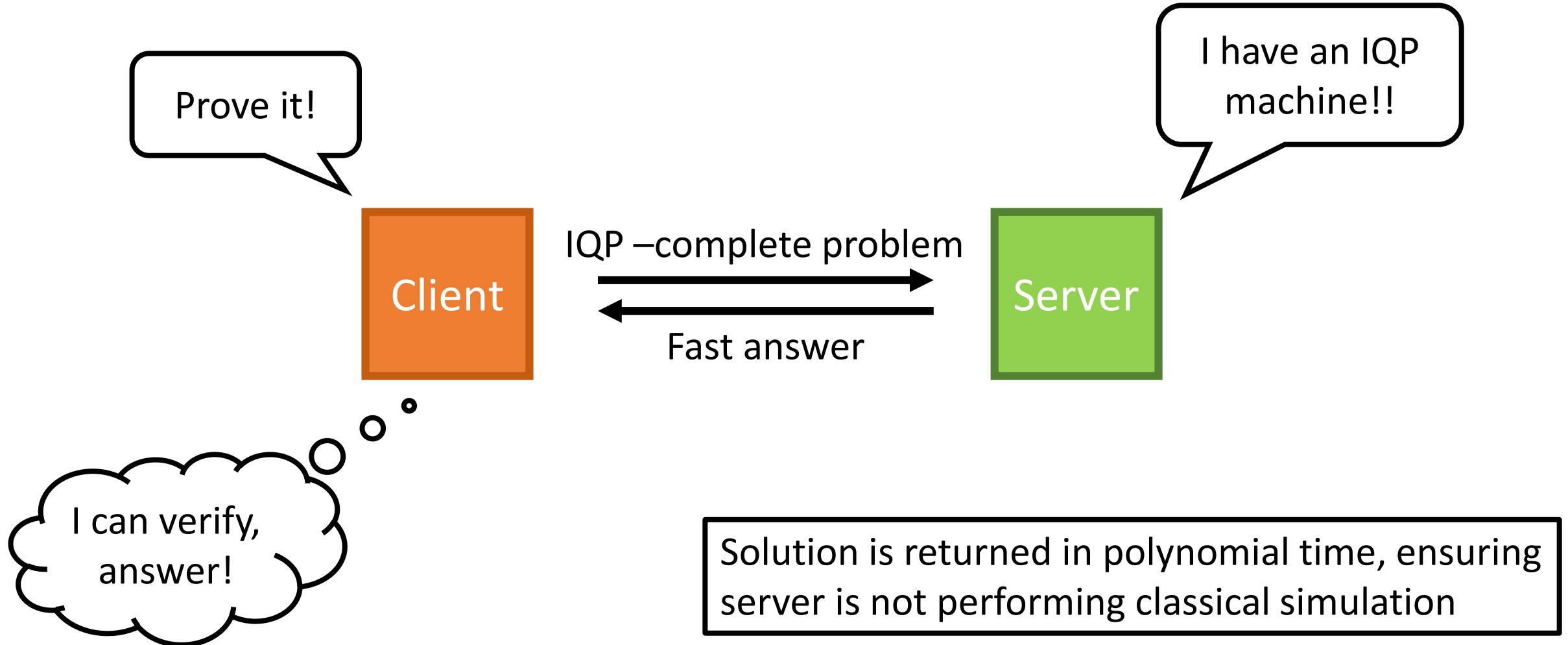


If IQP-sampling-complete problem is solved correctly then we know the server can perform all problems in the IQP sampling class.

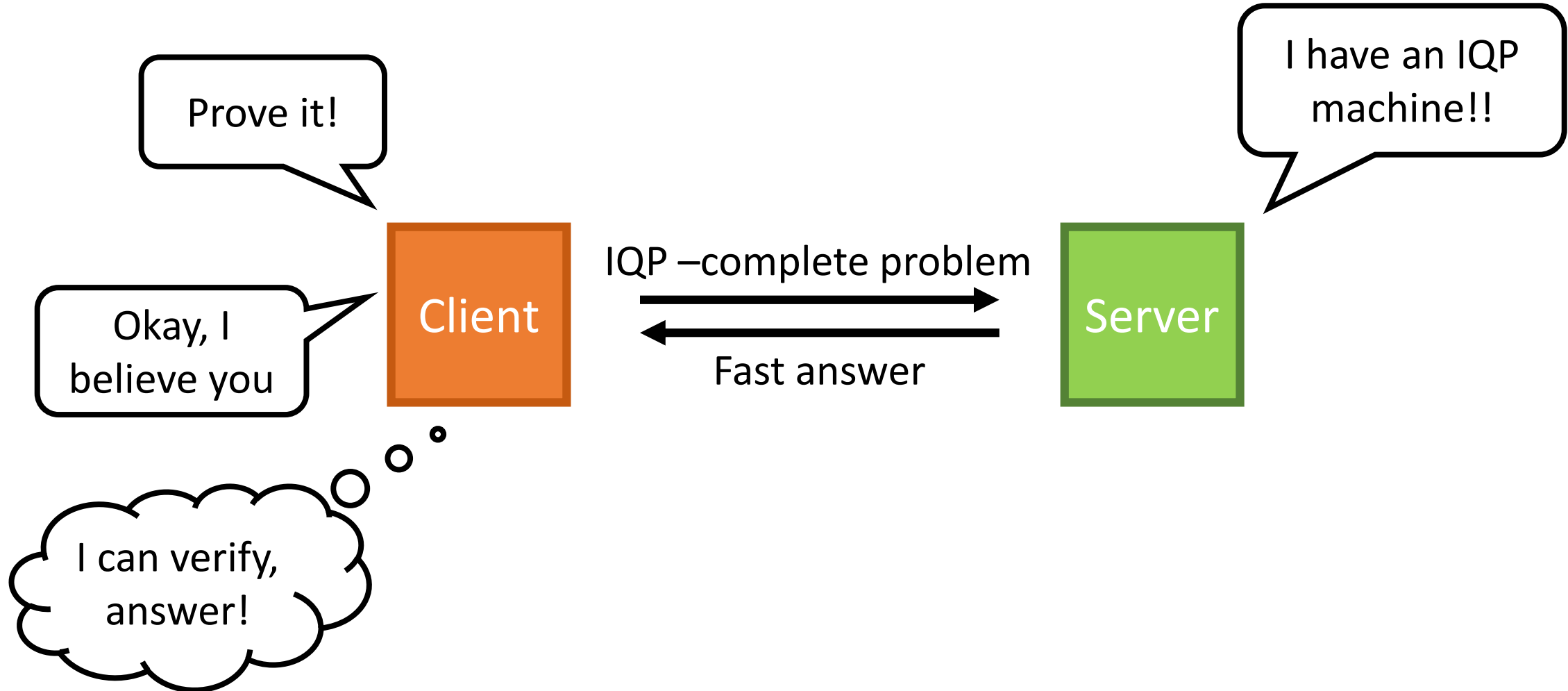
A Hypothesis Test



A Hypothesis Test



A Hypothesis Test



Three Building Blocks Of Hypothesis Test

1. Server solves **hard problem**
2. Client knows **something** allowing them to check server's solution
3. Server **must not use** this something to help solve problem

Three Building Blocks Of Hypothesis Test

Client **cannot complete**
computation if **limited to classical**



1. Server solves **hard problem**
2. Client knows **something** allowing them to check server's solution
3. Server **must not use** this something to help solve problem

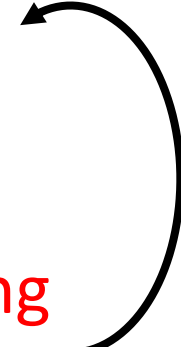
Three Building Blocks Of Hypothesis Test

Client **cannot complete**
computation if **limited to classical**



1. Server solves **hard problem**
2. Client knows **something** allowing them to check server's solution
3. Server **must not use** this something to help solve problem

Problem may have **structure** resulting
from 'something' known by the client.



Two Cases for the 'Something'

3. Server **must not use** this something to help solve problem

Two Cases for the 'Something'

Server **trusted** and you can
assume he does not use it



3. Server **must not use** this something to help solve problem

Two Cases for the 'Something'

Server **trusted** and you can
assume he does not use it



3. Server **must not use** this something to help solve problem

Server **not trusted**
and you must **hide** it



Three Building Blocks Of Hypothesis Test

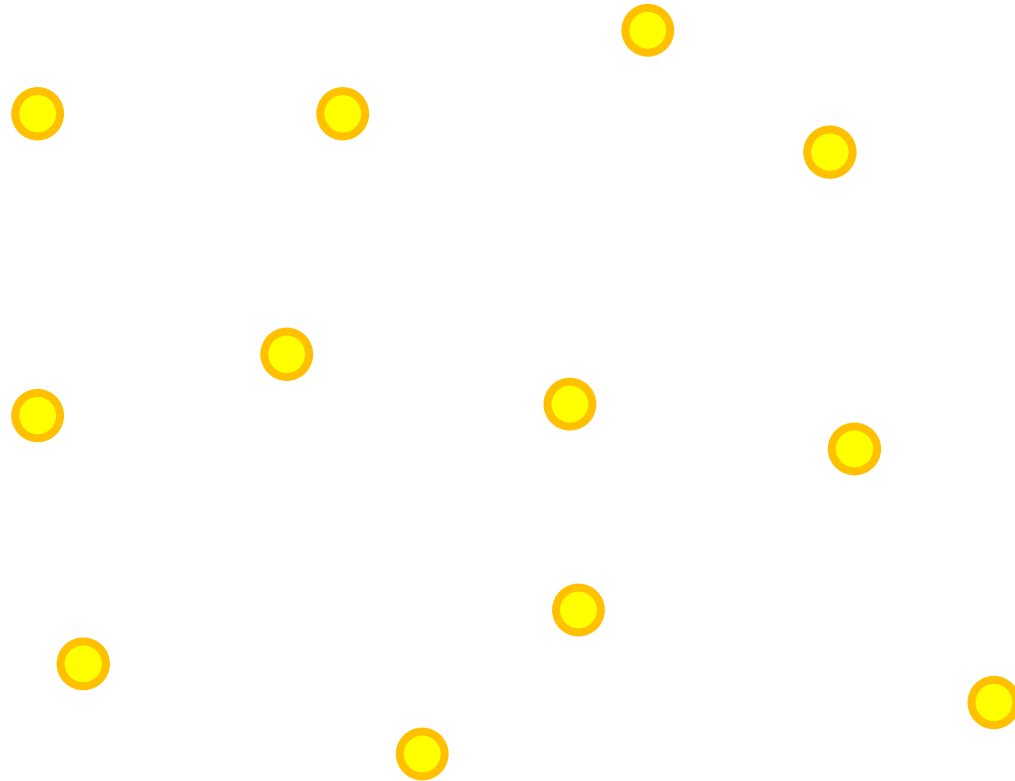
1. Server solves **hard problem**
2. Client knows **something** allowing them to check server's solution
3. Server **must not use** this something to help solve problem

Three Building Blocks Of Hypothesis Test

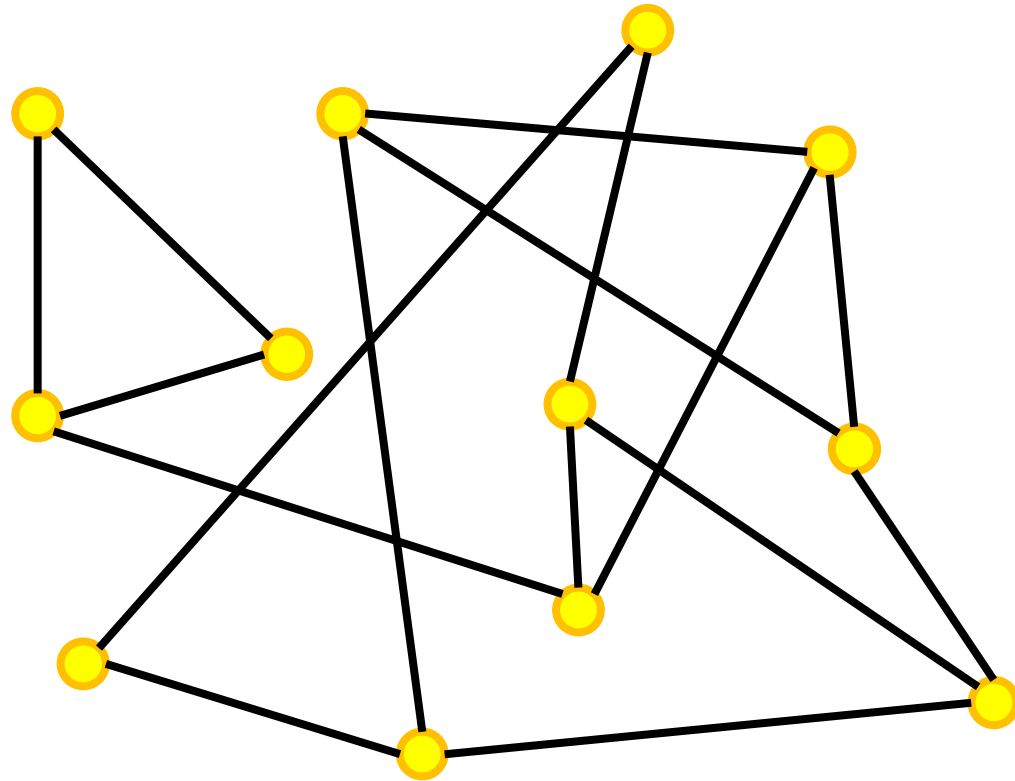
1. Server solves **hard problem**
2. Client knows **something** allowing them to check server's solution
3. Server **must not use** this something to help solve problem

Measurement Based Quantum Computing

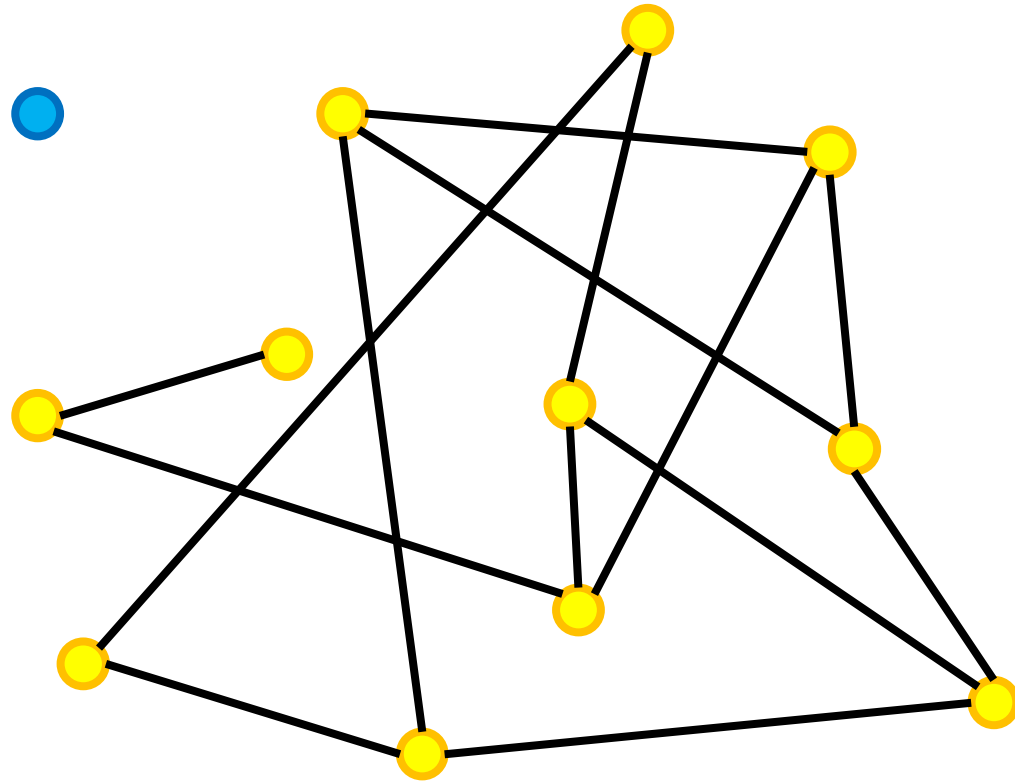
Measurement Based Quantum Computing



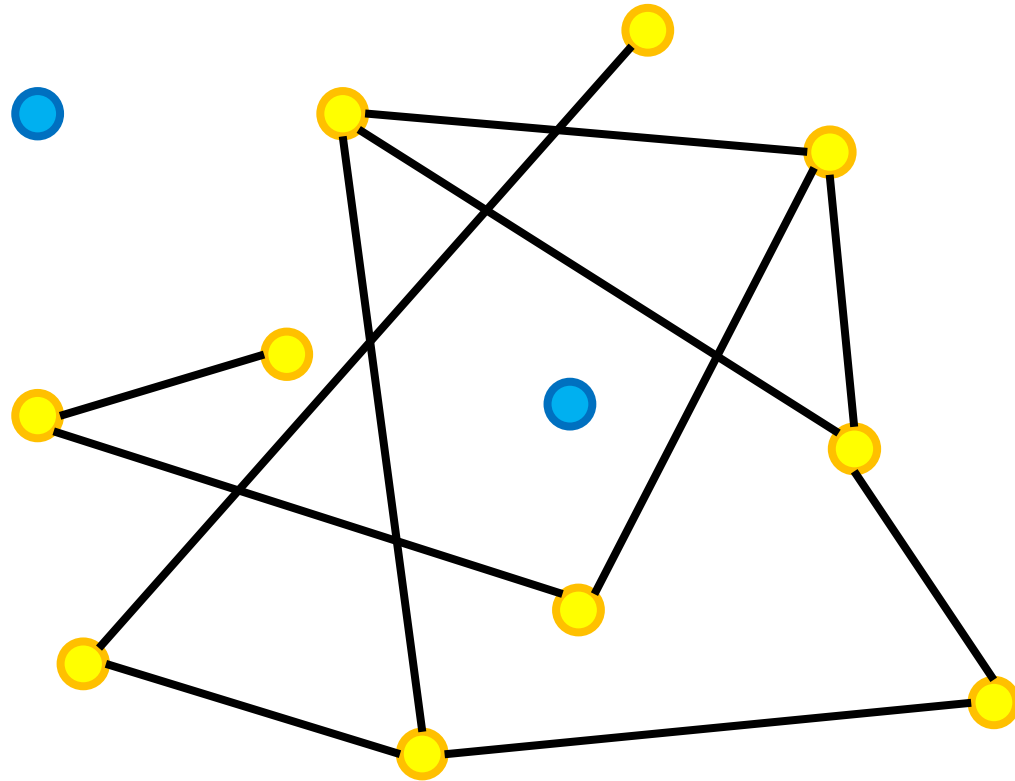
Measurement Based Quantum Computing



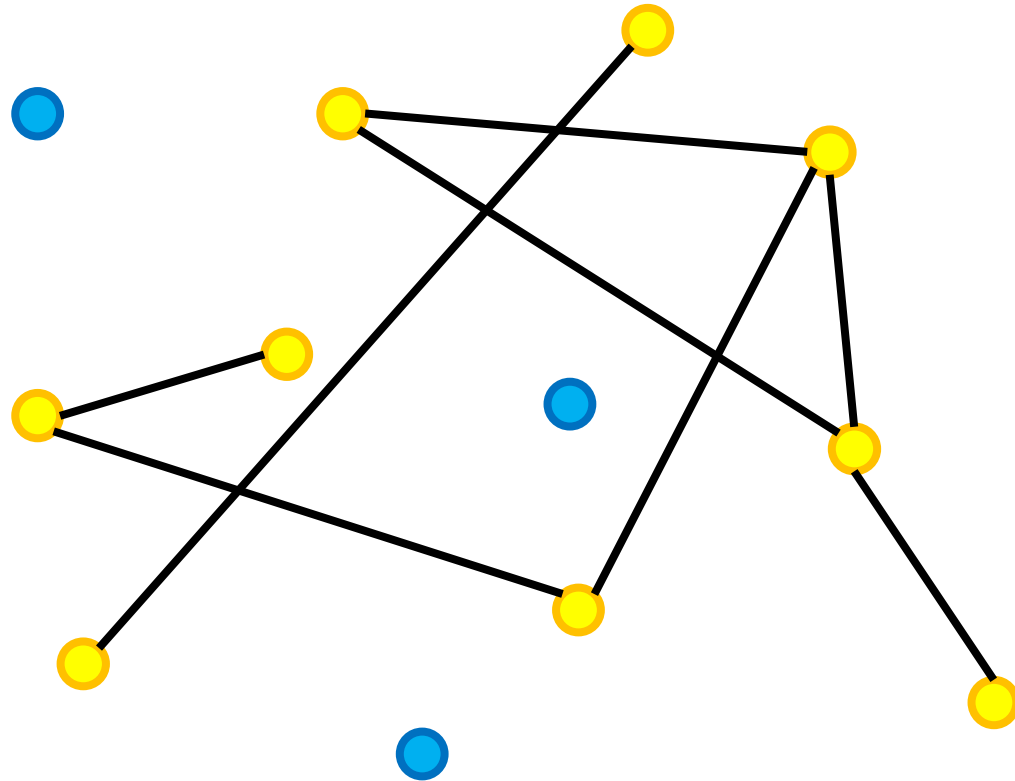
Measurement Based Quantum Computing



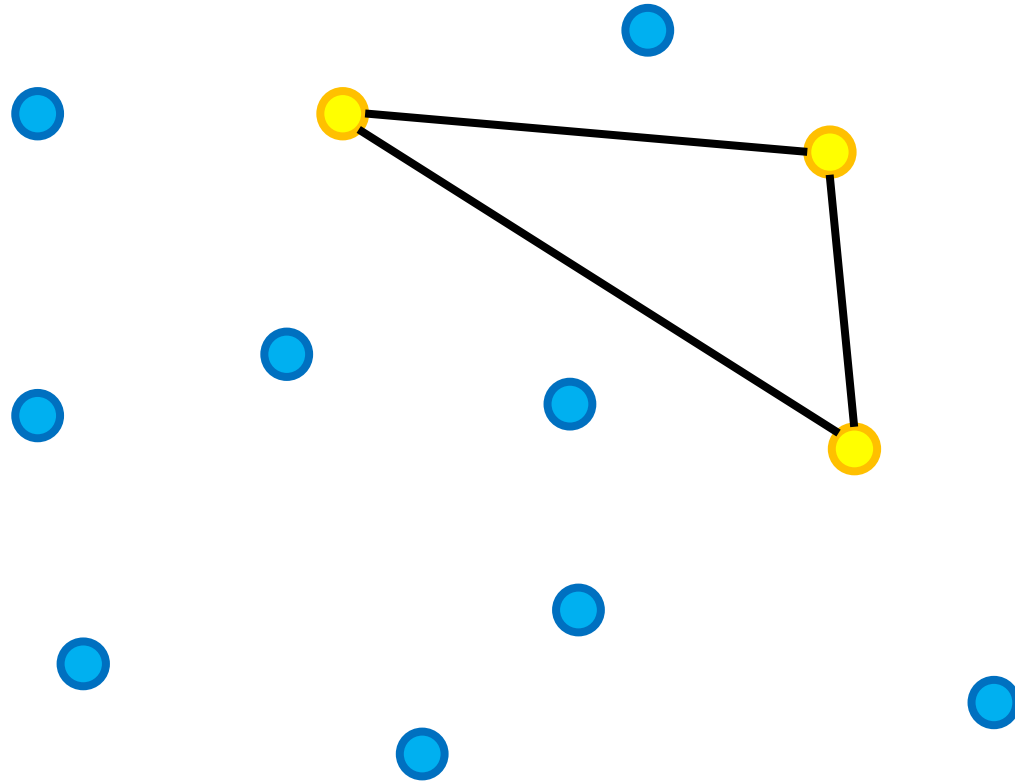
Measurement Based Quantum Computing



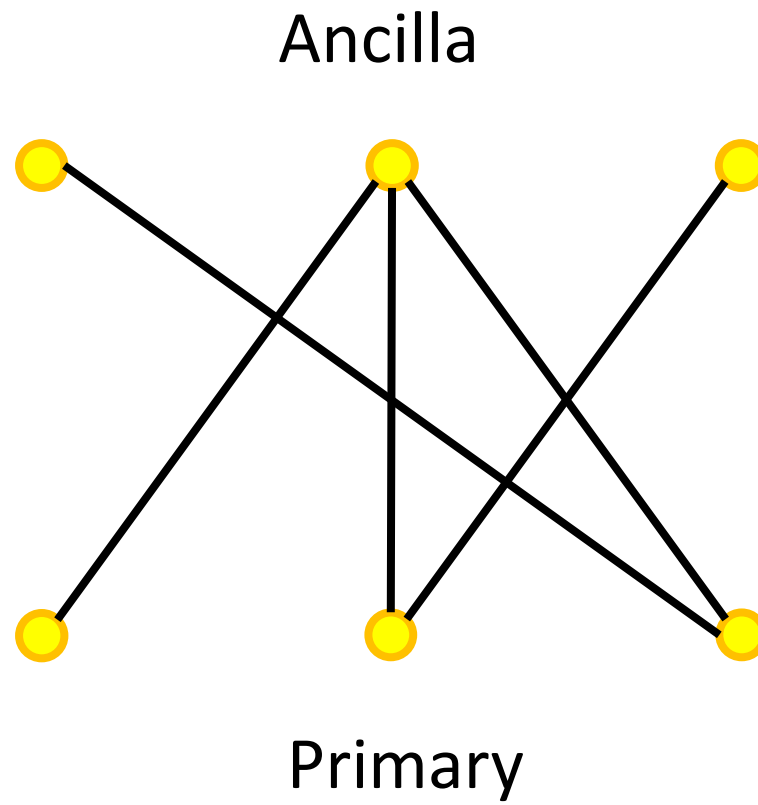
Measurement Based Quantum Computing



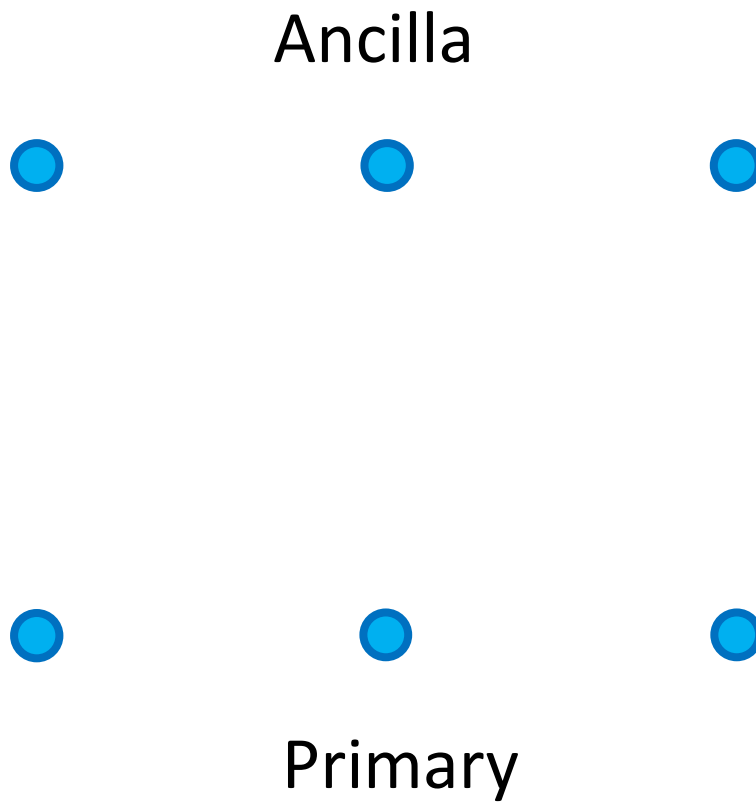
Measurement Based Quantum Computing



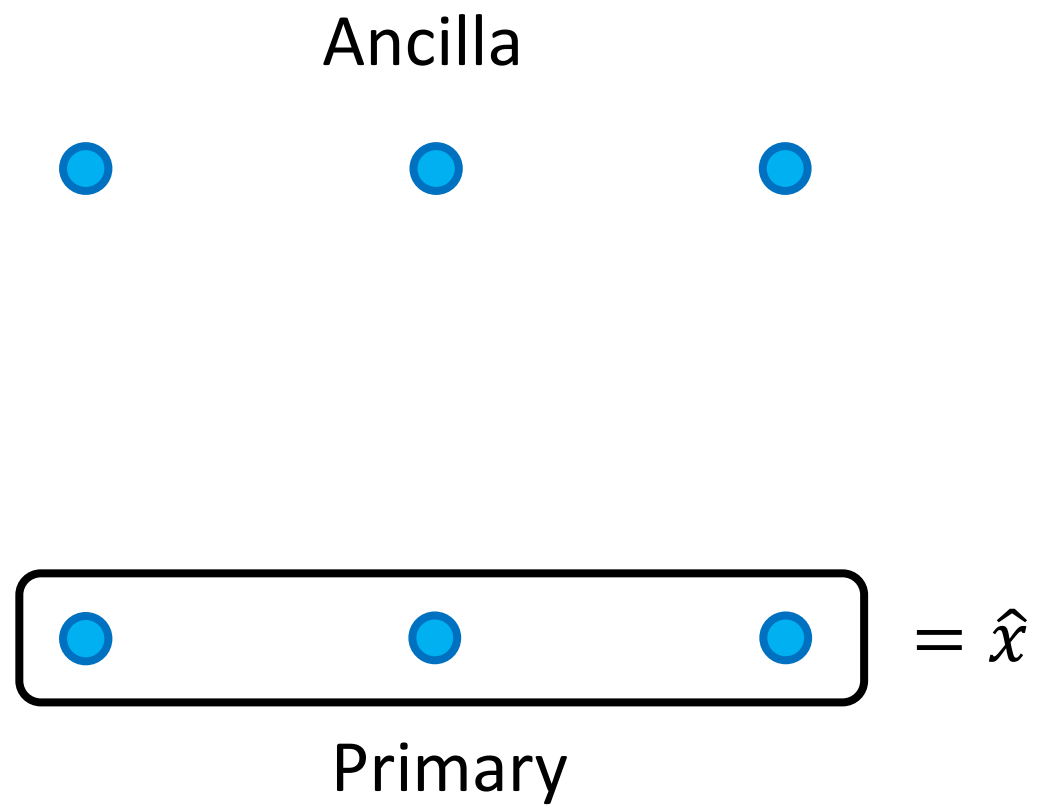
IQP In MBQC



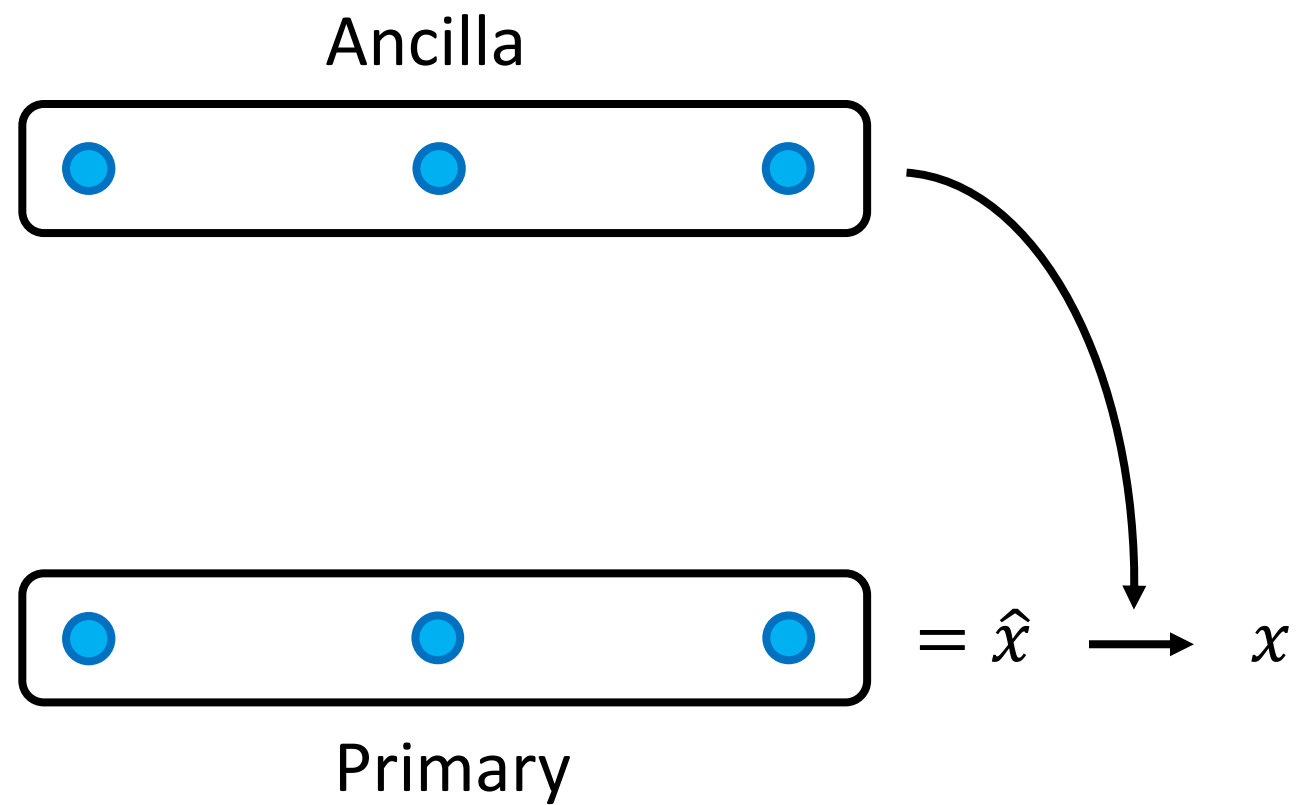
IQP In MBQC



IQP In MBQC



IQP In MBQC



Bridge and Break Operations

Break:

Bridge:

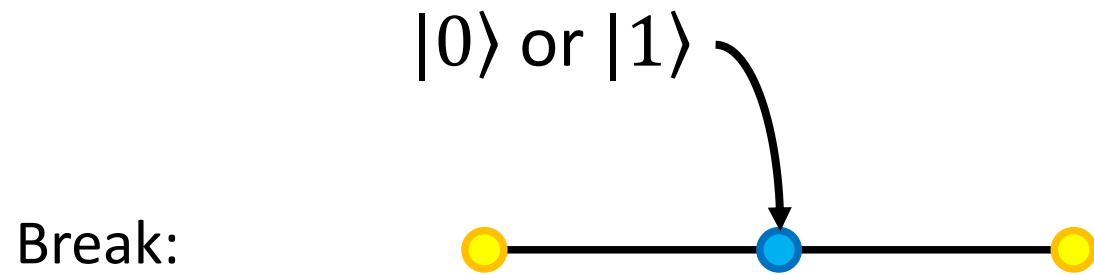
Bridge and Break Operations

Break:



Bridge:

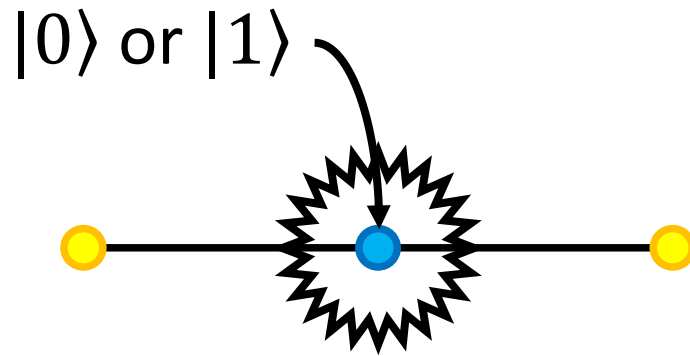
Bridge and Break Operations



Bridge:

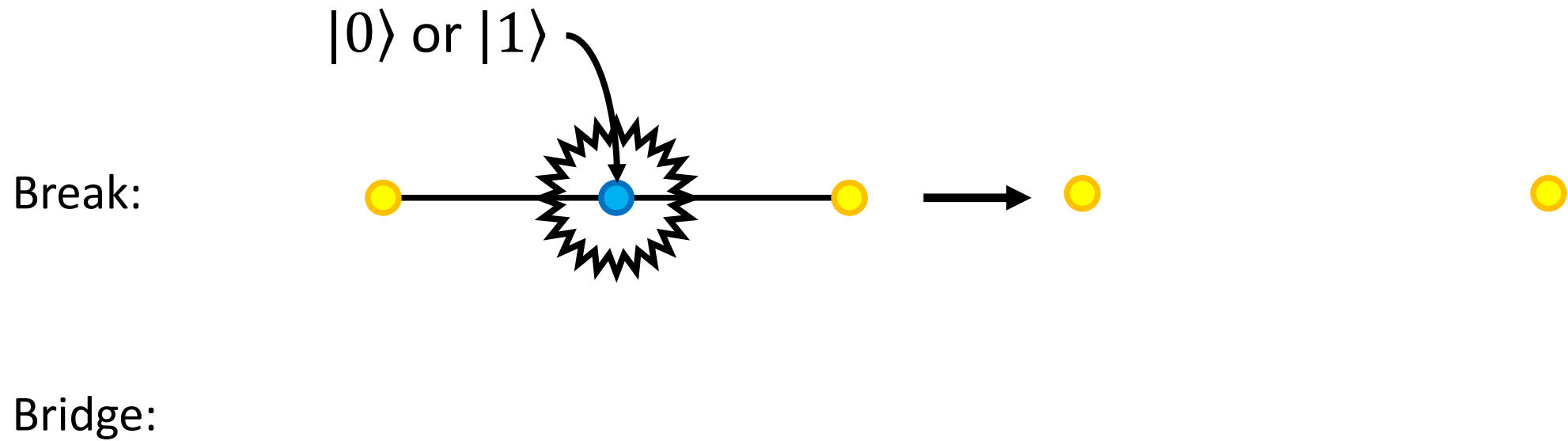
Bridge and Break Operations

Break:

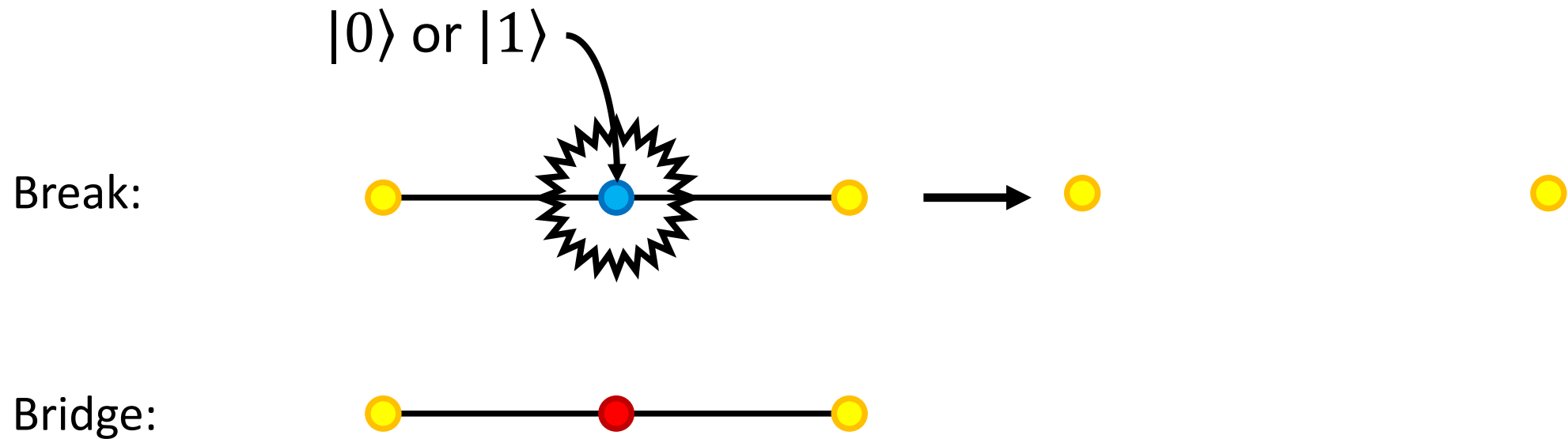


Bridge:

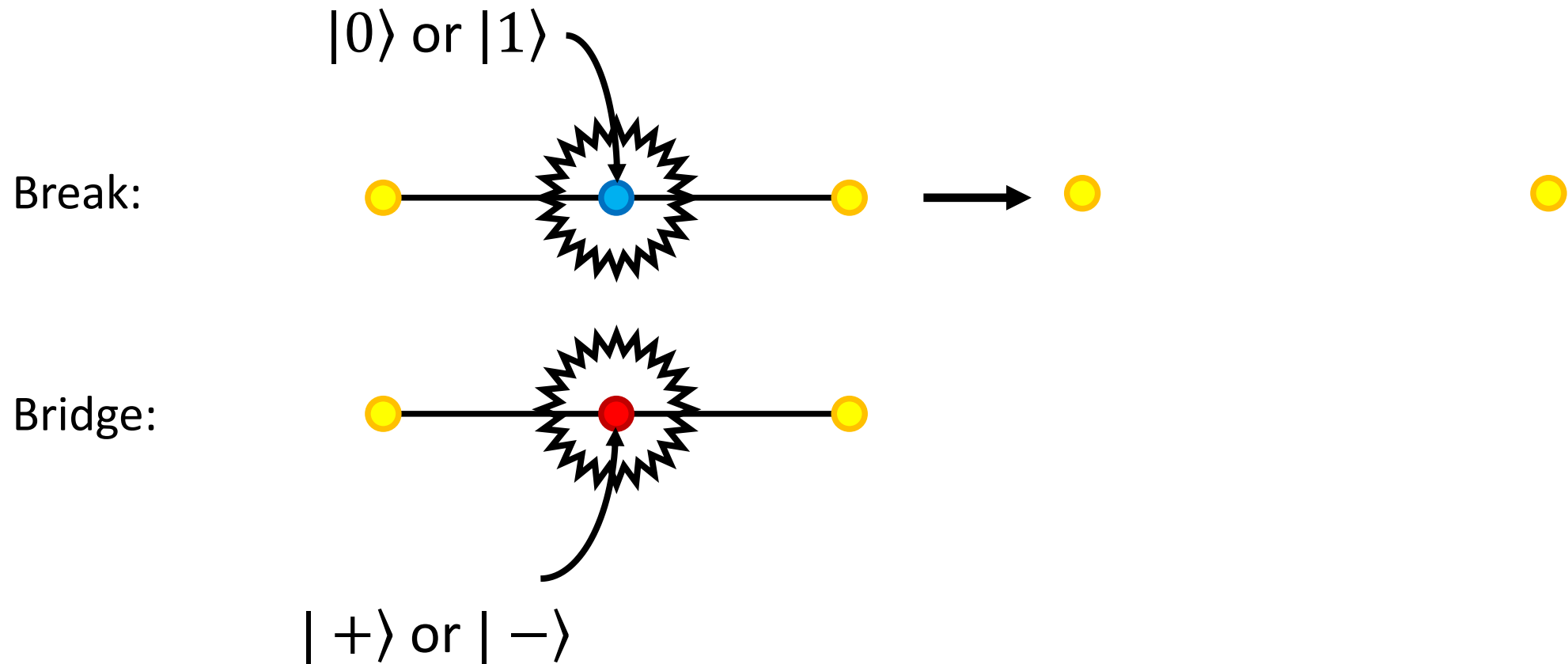
Bridge and Break Operations



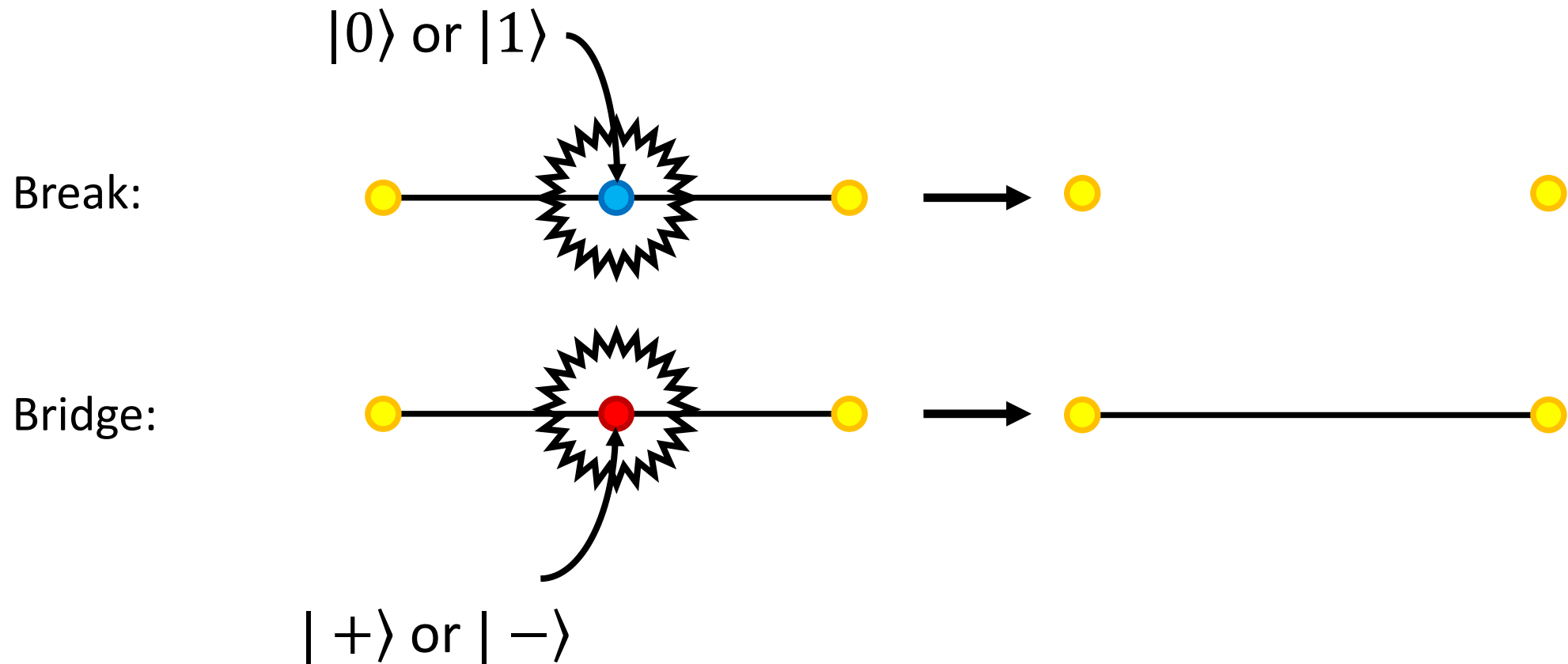
Bridge and Break Operations



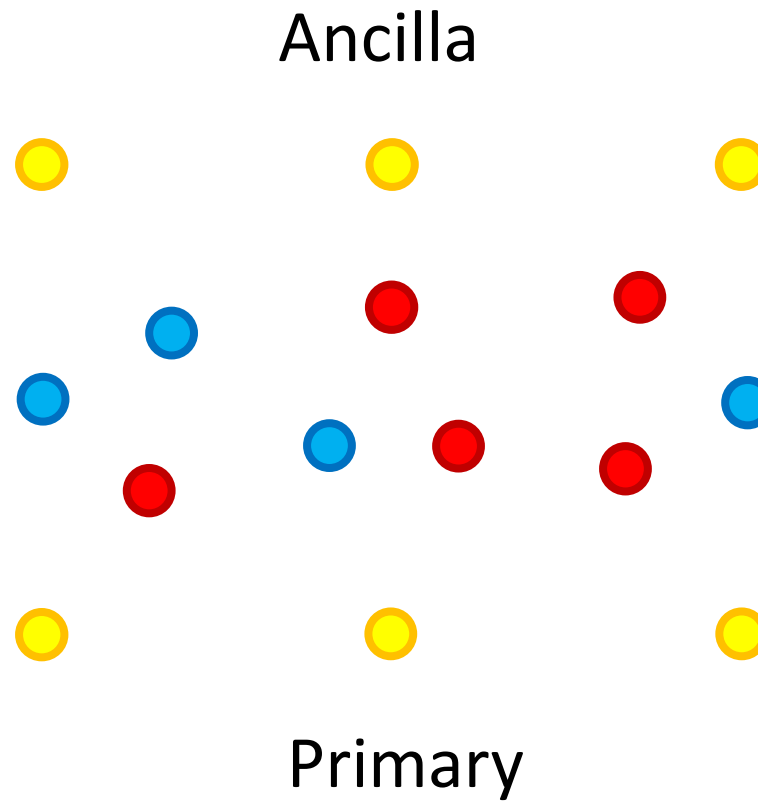
Bridge and Break Operations



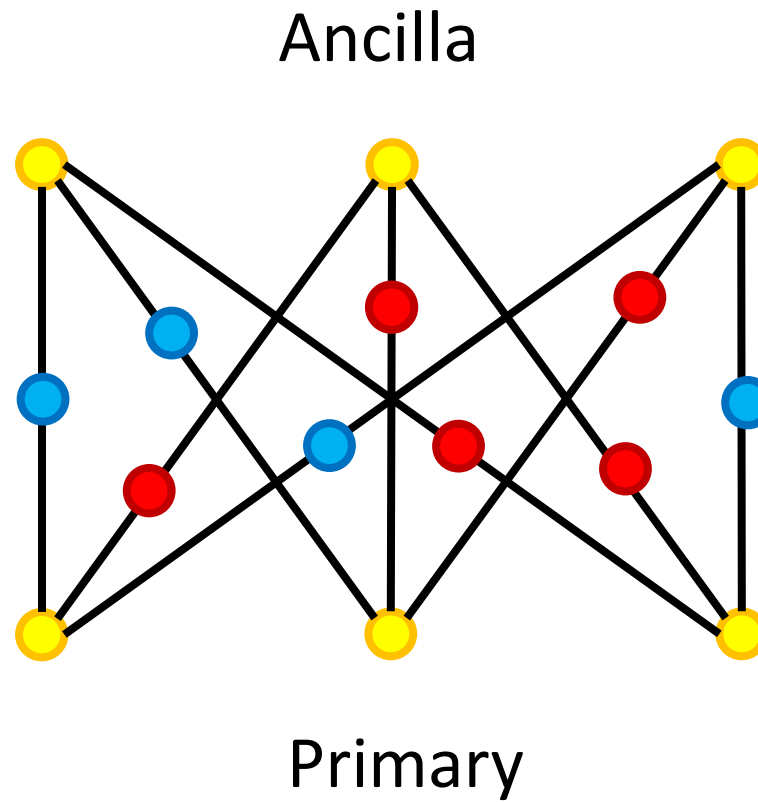
Bridge and Break Operations



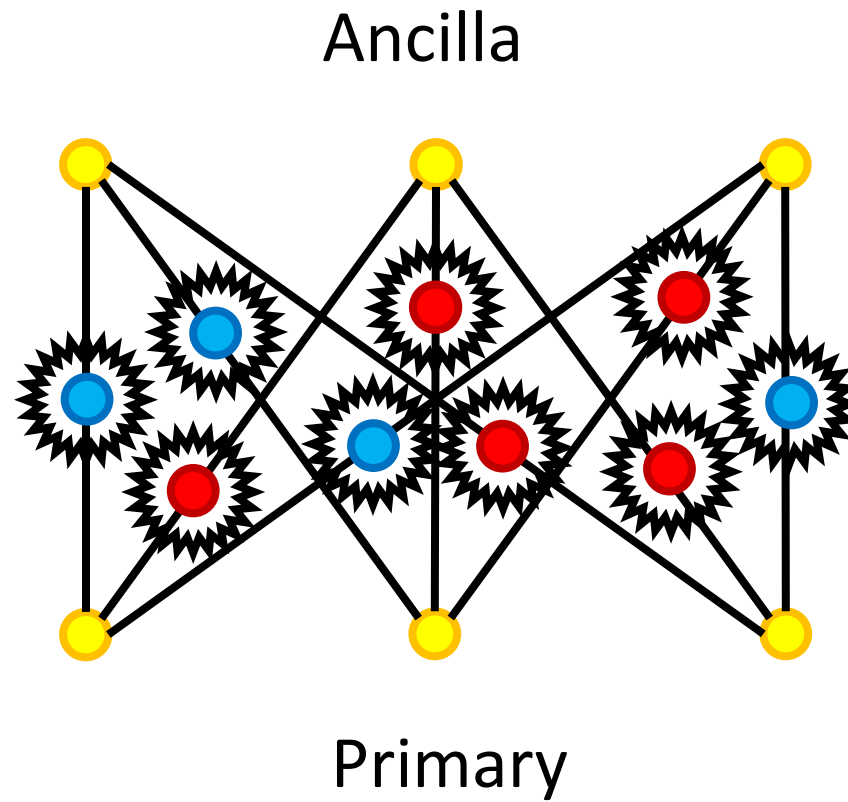
IQP MBQC Graph Generation



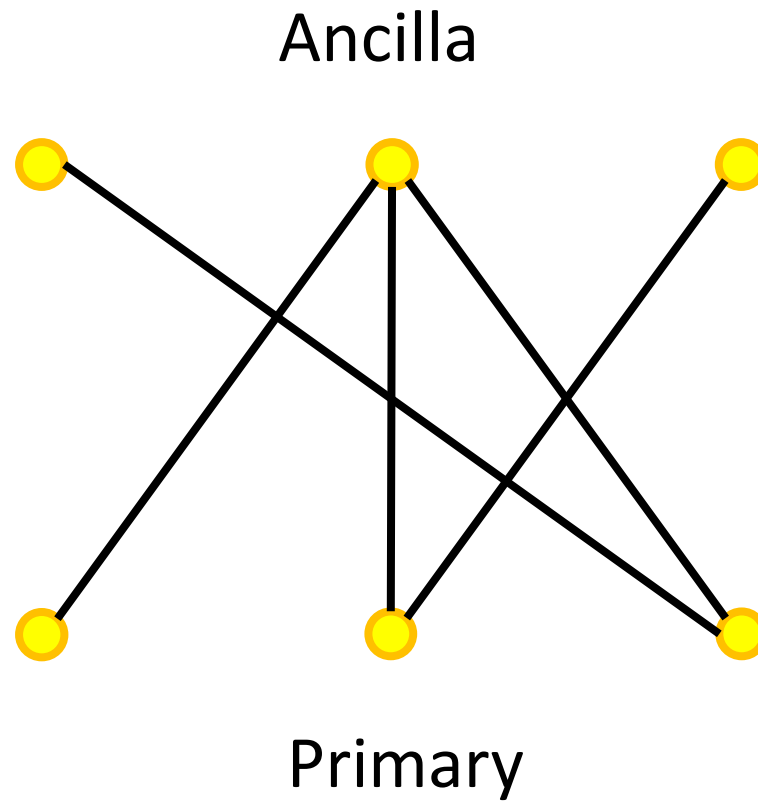
IQP MBQC Graph Generation



IQP MBQC Graph Generation

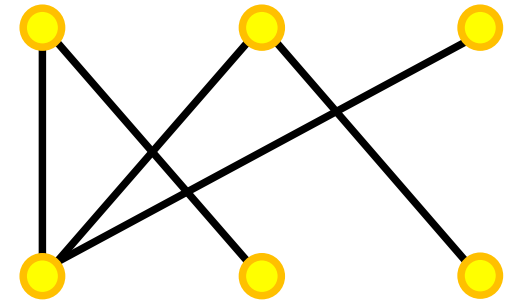


IQP MBQC Graph Generation



Blind IQP MBQC Graph Generation

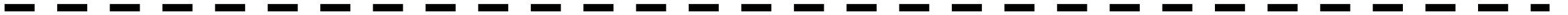
Client



Server

Blind IQP MBQC Graph Generation

Client

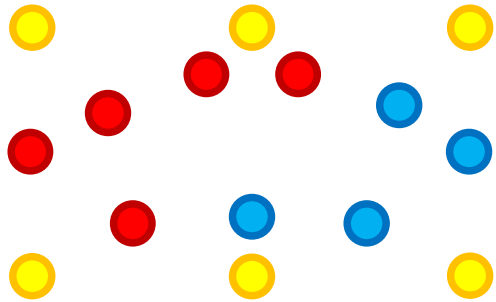


?

Server

Blind IQP MBQC Graph Generation

Client

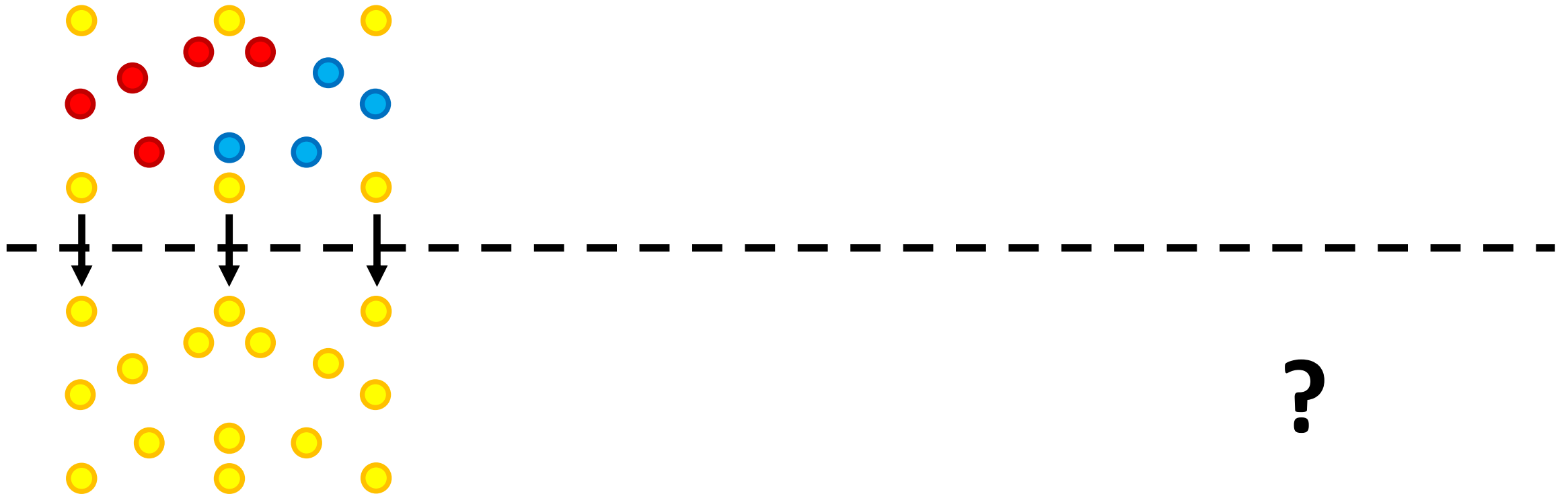


?

Server

Blind IQP MBQC Graph Generation

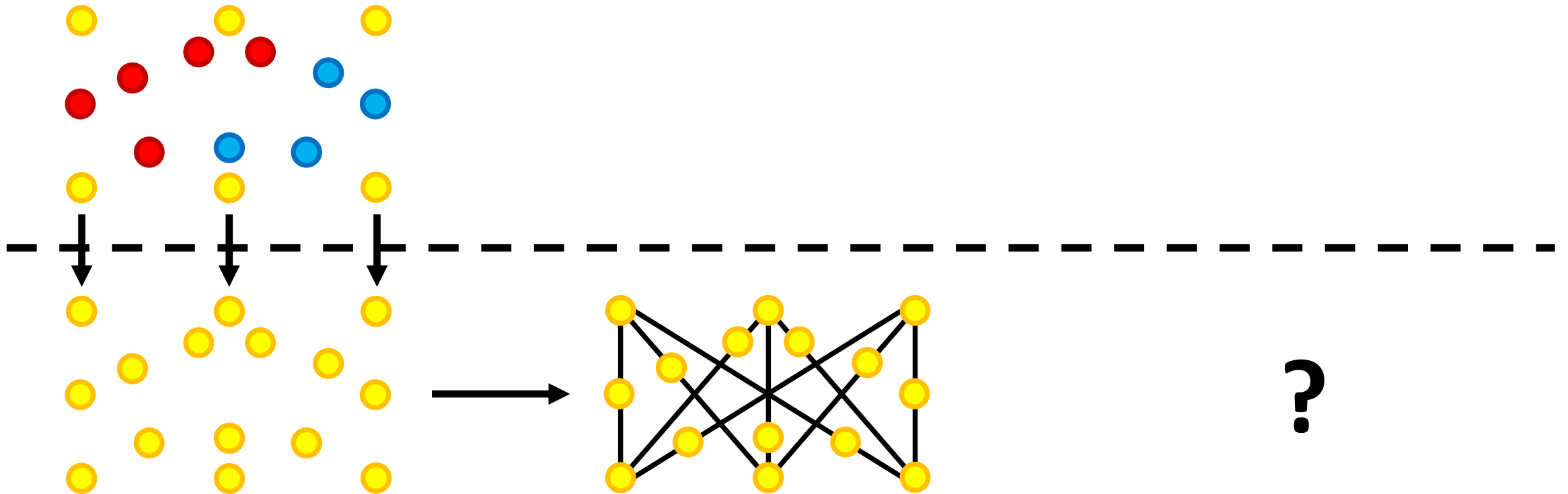
Client



Server

Blind IQP MBQC Graph Generation

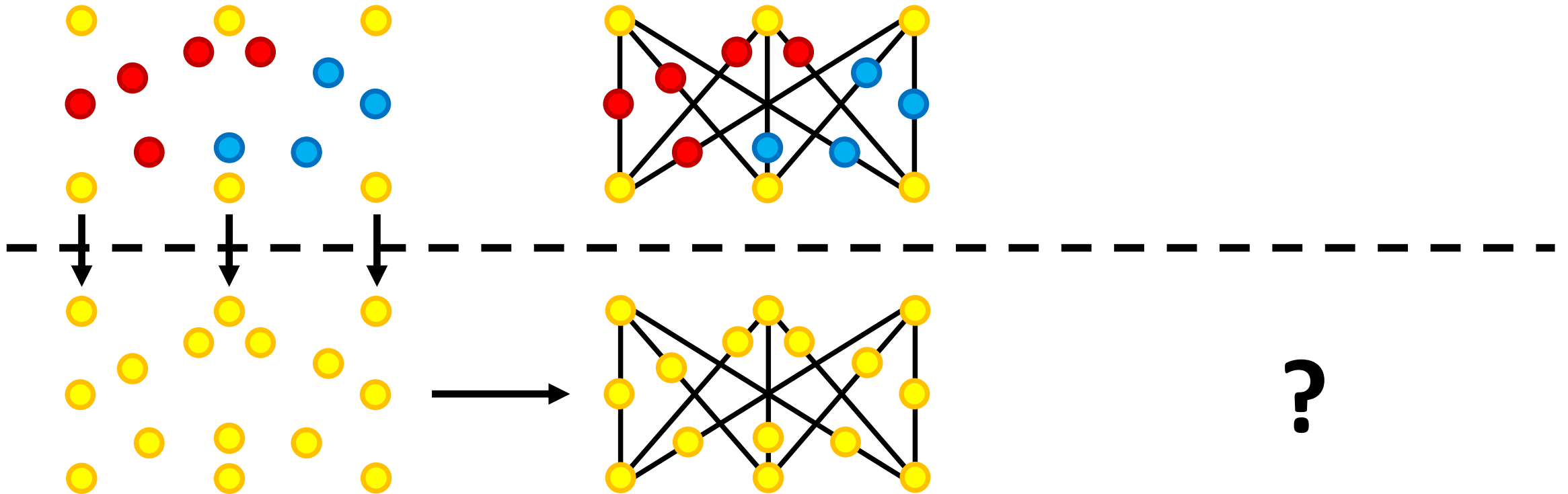
Client



Server

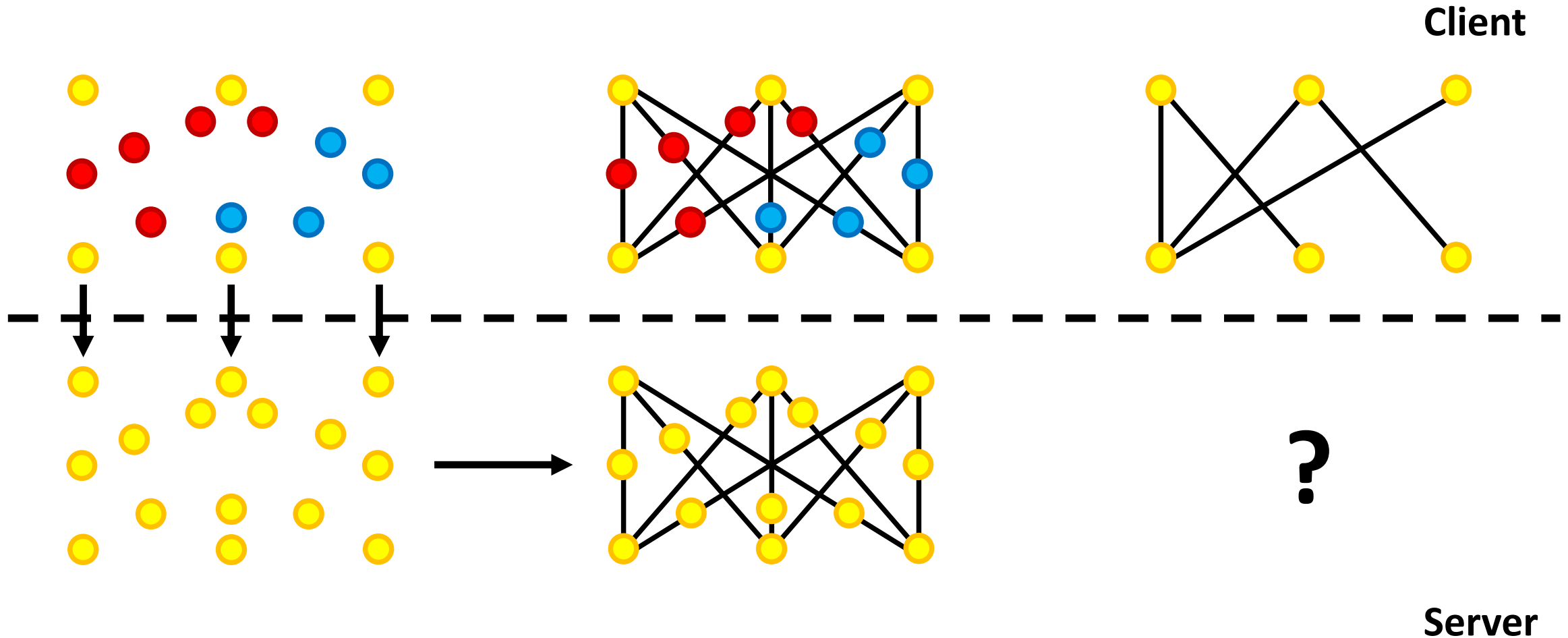
Blind IQP MBQC Graph Generation

Client

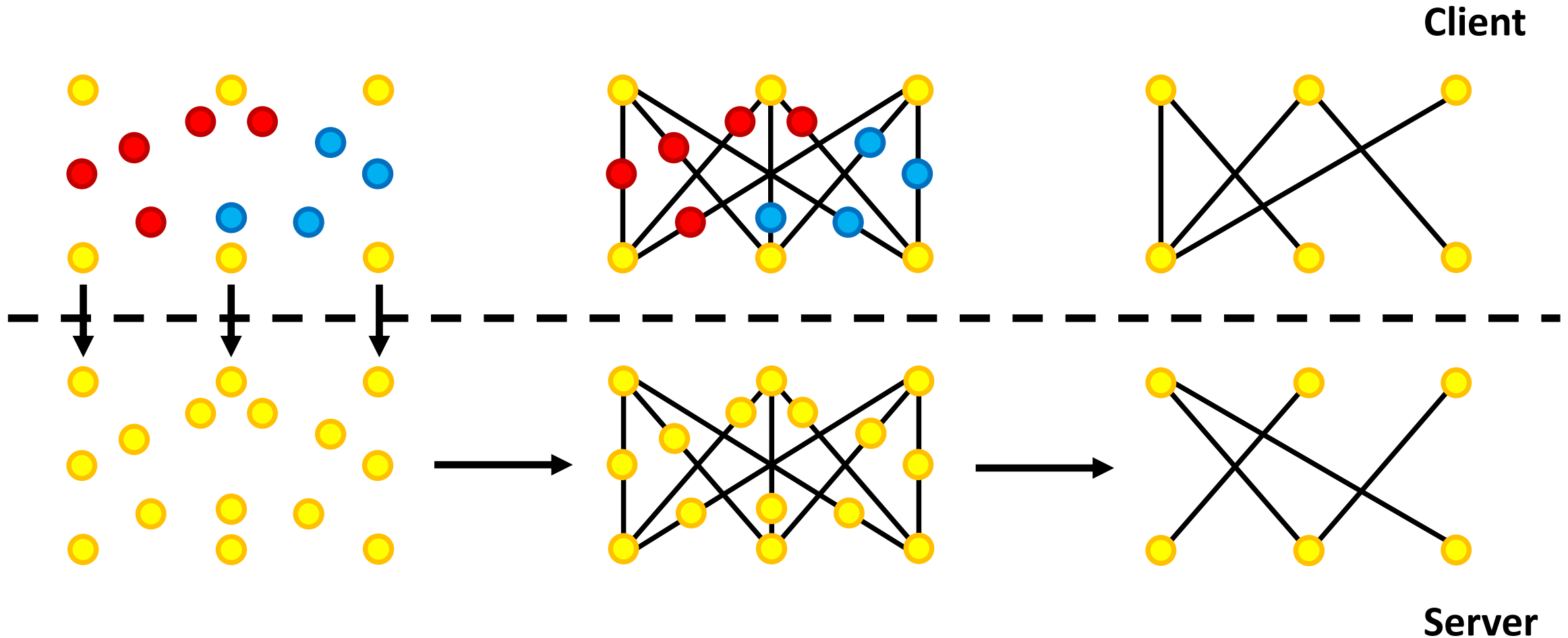


Server

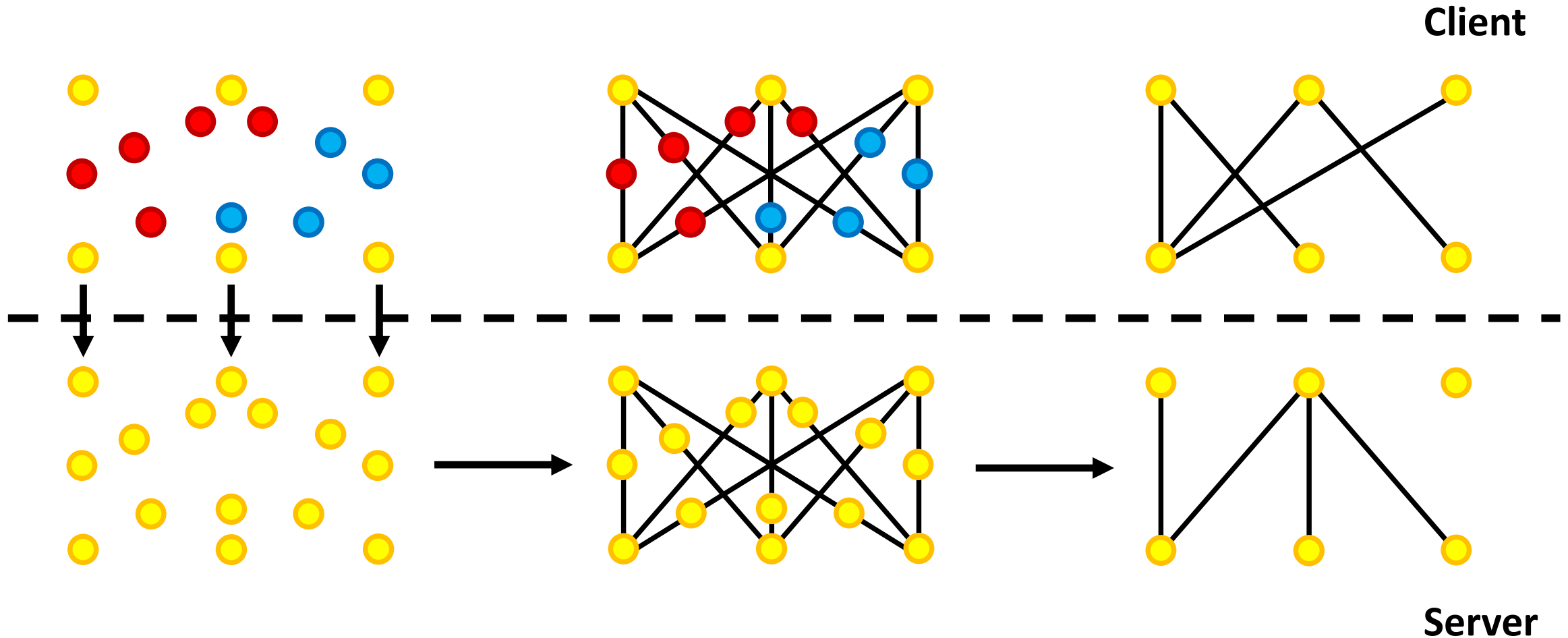
Blind IQP MBQC Graph Generation



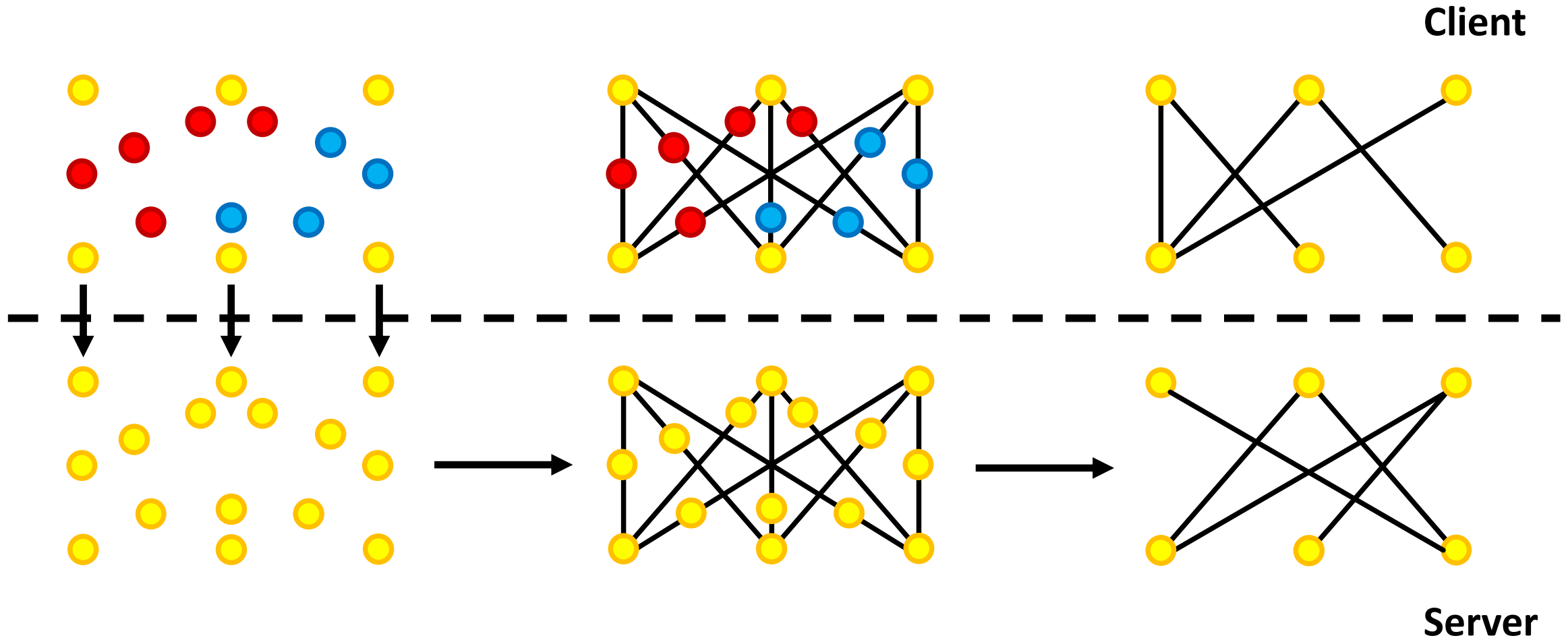
Blind IQP MBQC Graph Generation



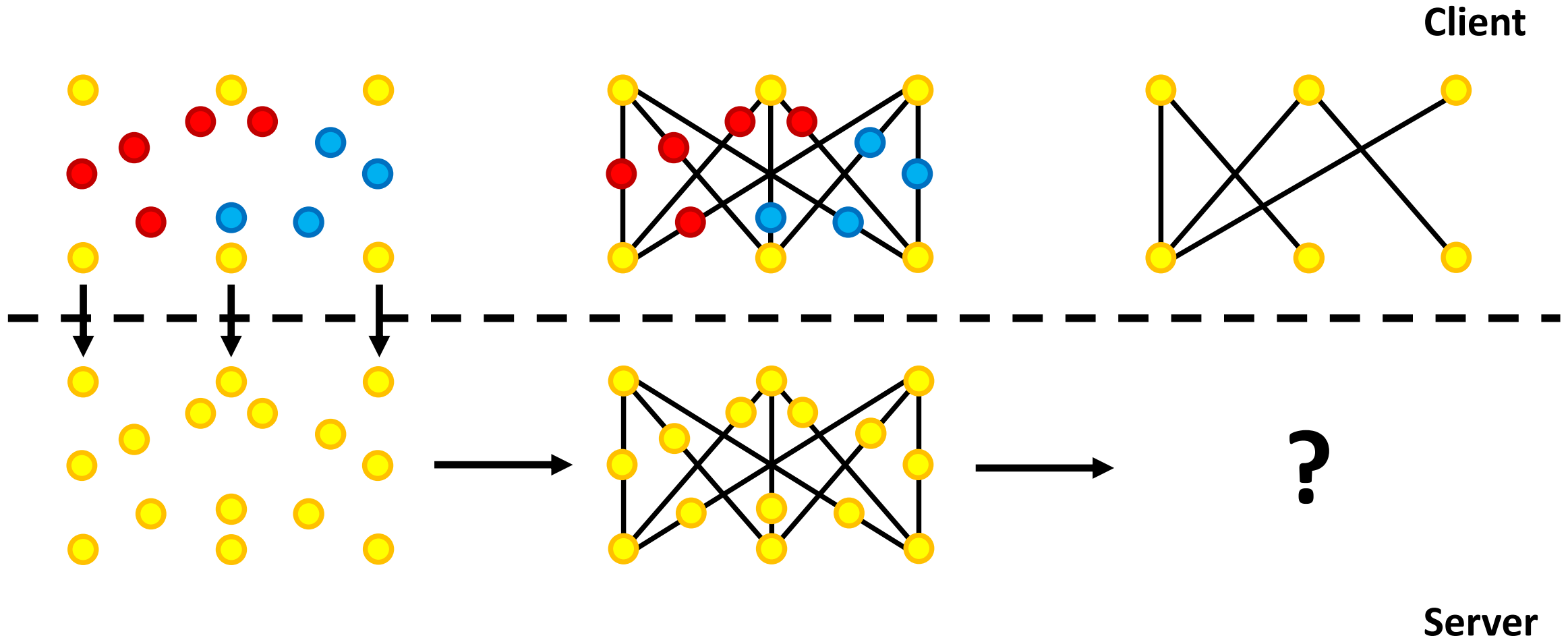
Blind IQP MBQC Graph Generation



Blind IQP MBQC Graph Generation



Blind IQP MBQC Graph Generation



Three Building Blocks Of Hypothesis Test

1. Server solves **hard problem**
2. Client knows **something** allowing them to check server's solution
3. Server **must not use** this something to help solve problem

Our Hypothesis Test

Client

Server



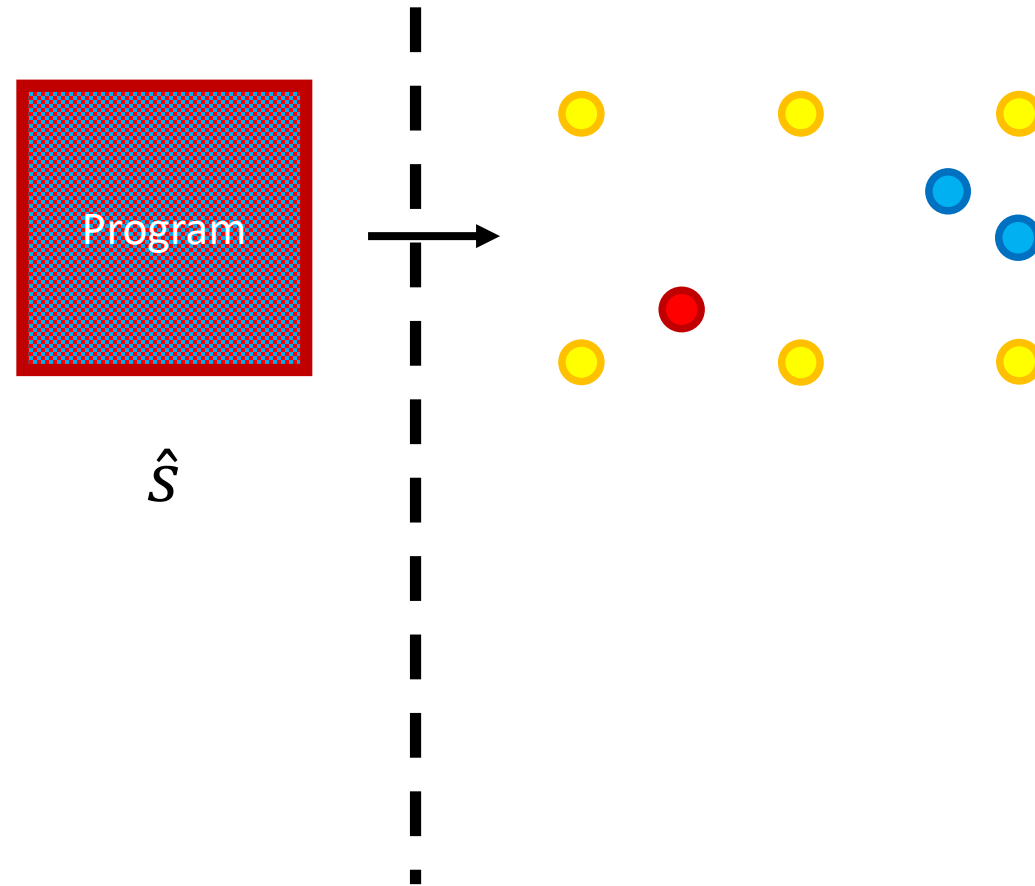
\hat{S}



Our Hypothesis Test

Client

Server

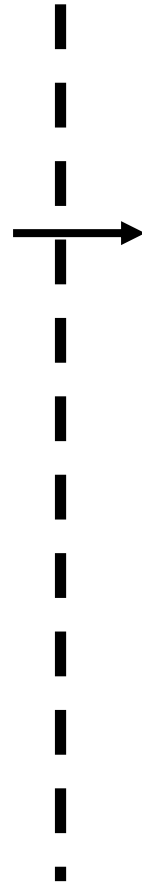


Our Hypothesis Test

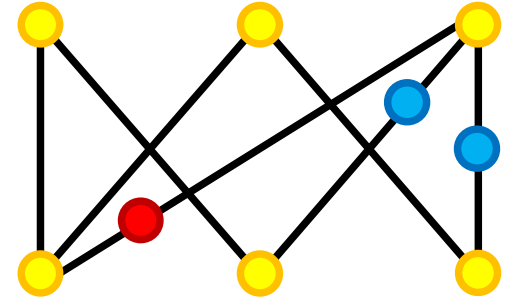
Client



\hat{S}

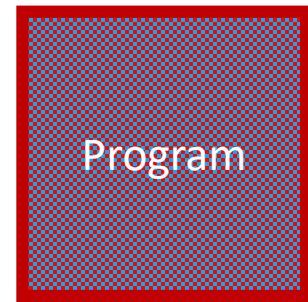


Server

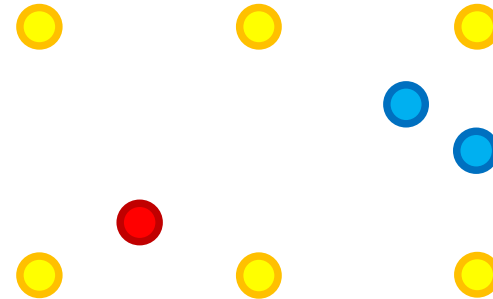
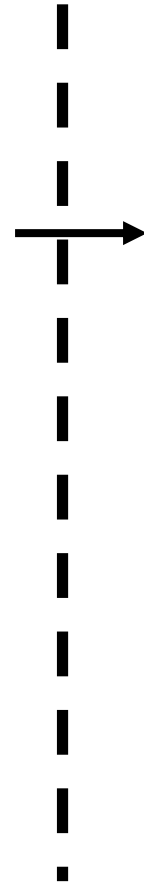


Our Hypothesis Test

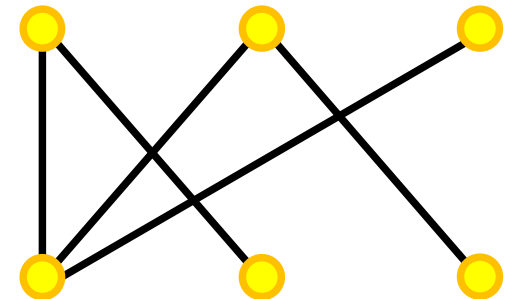
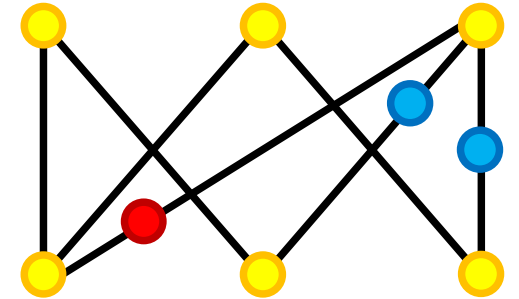
Client



\hat{S}



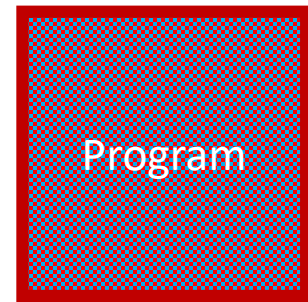
Server



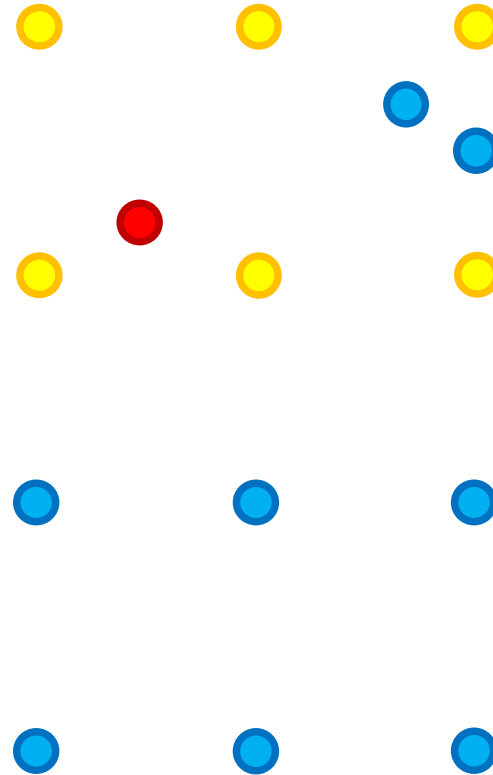
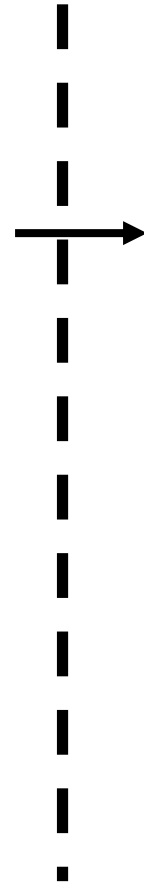
Key: The graph depends on \hat{S} but graph built blindly so \hat{S} is not revealed

Our Hypothesis Test

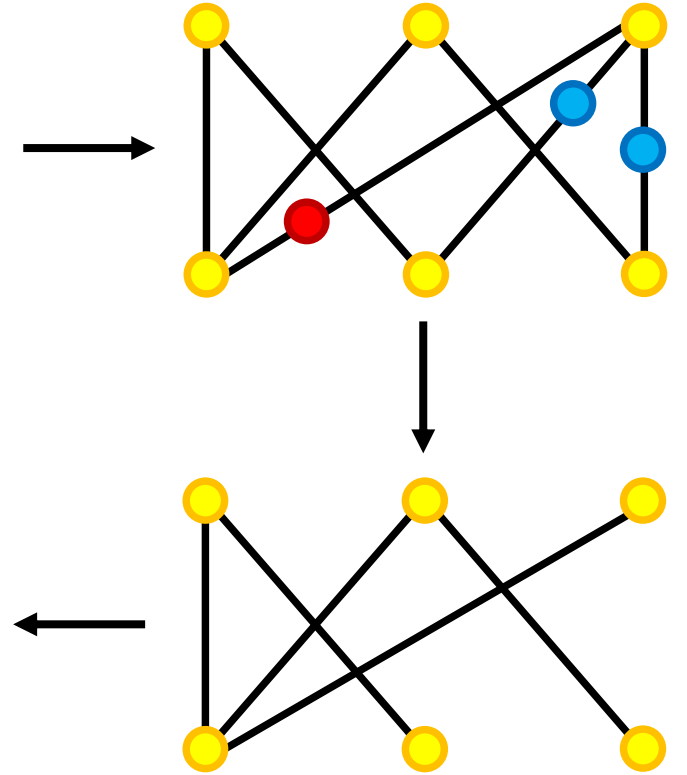
Client



\hat{S}



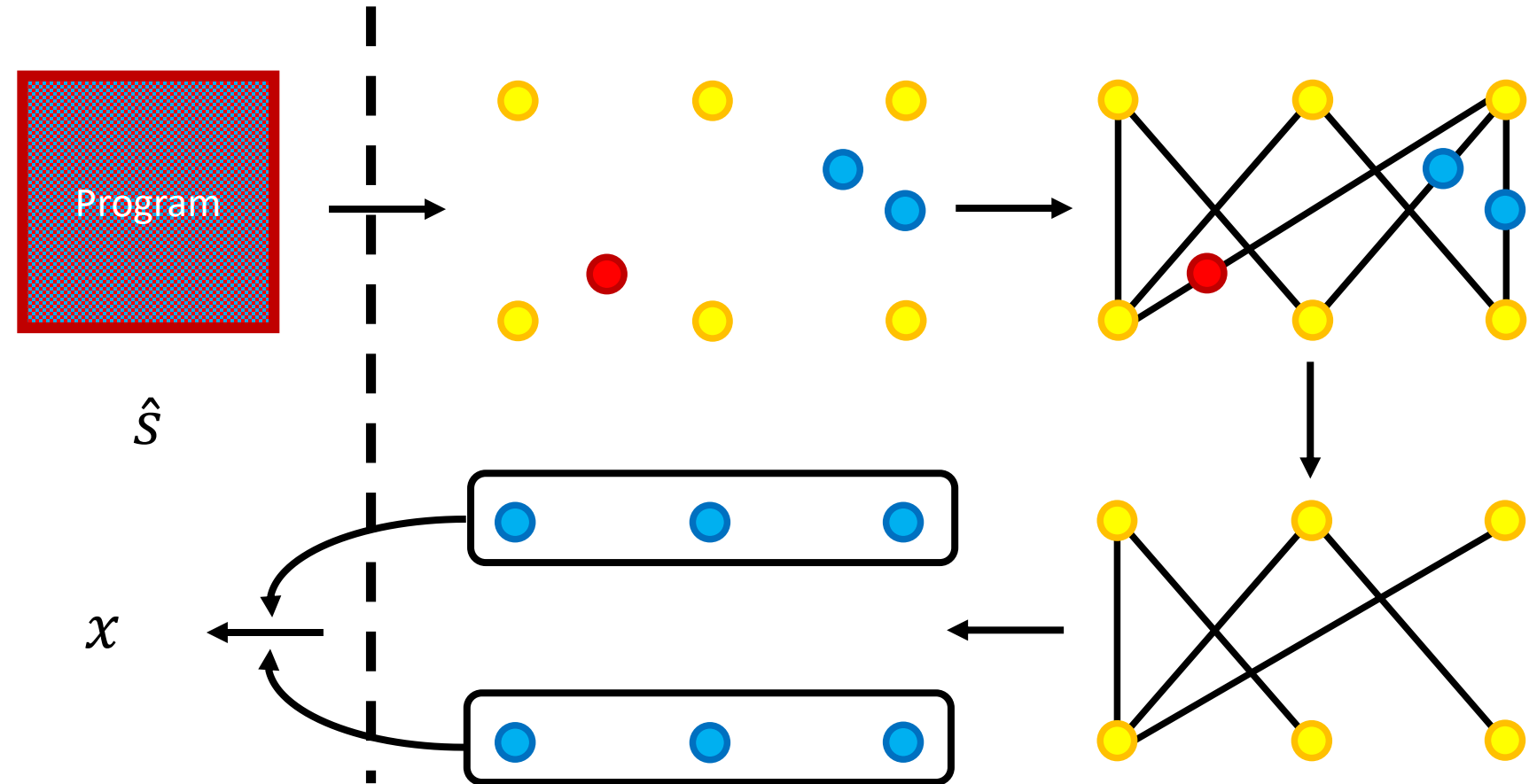
Server



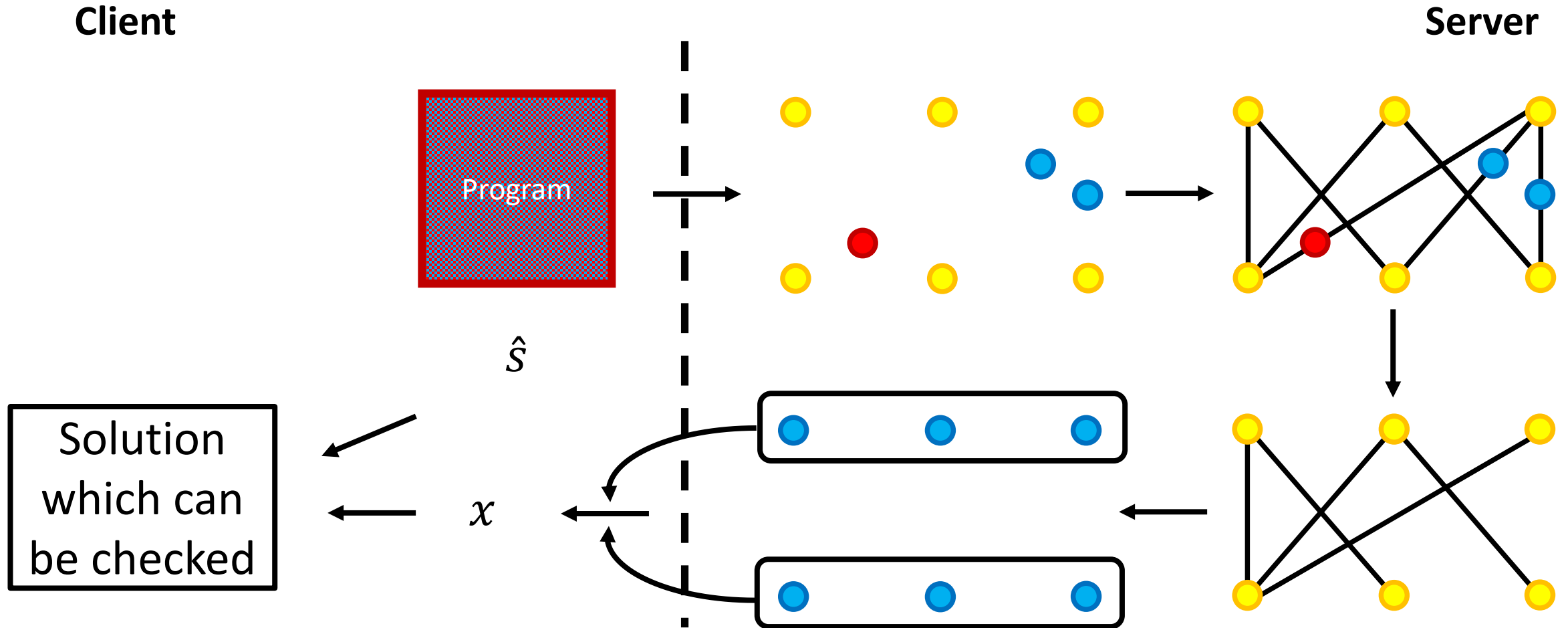
Our Hypothesis Test

Client

Server



Our Hypothesis Test



Questions

No, I don't know when we will see quantum computers in our homes