Quantum Computation & Cryptography
Day 4

Entanglement and device-independence

Andru Gheorghiu

Recap

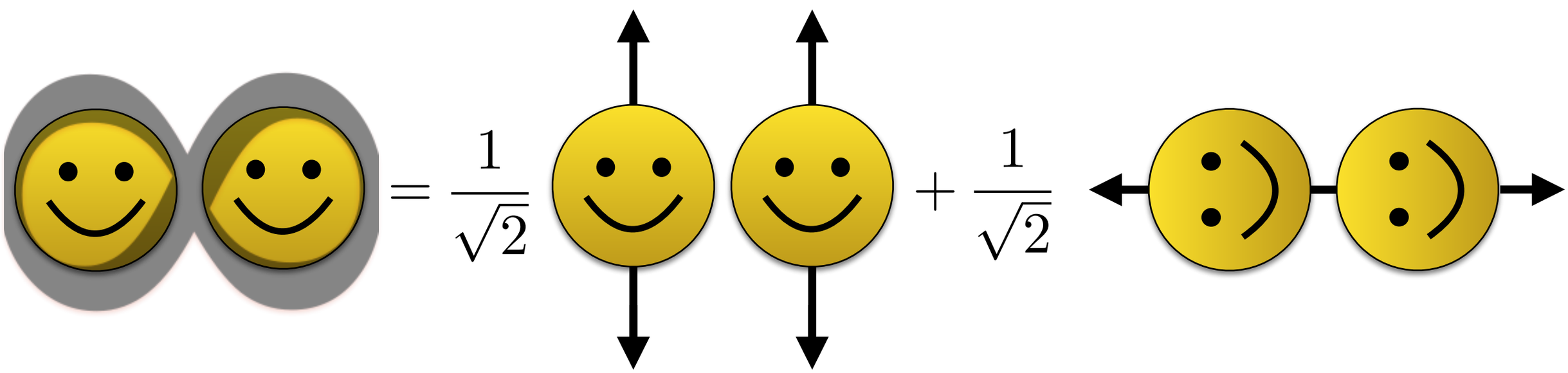
Entanglement

States that cannot be expressed as

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$$

E.g. a Bell state

$$|\phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_B$$

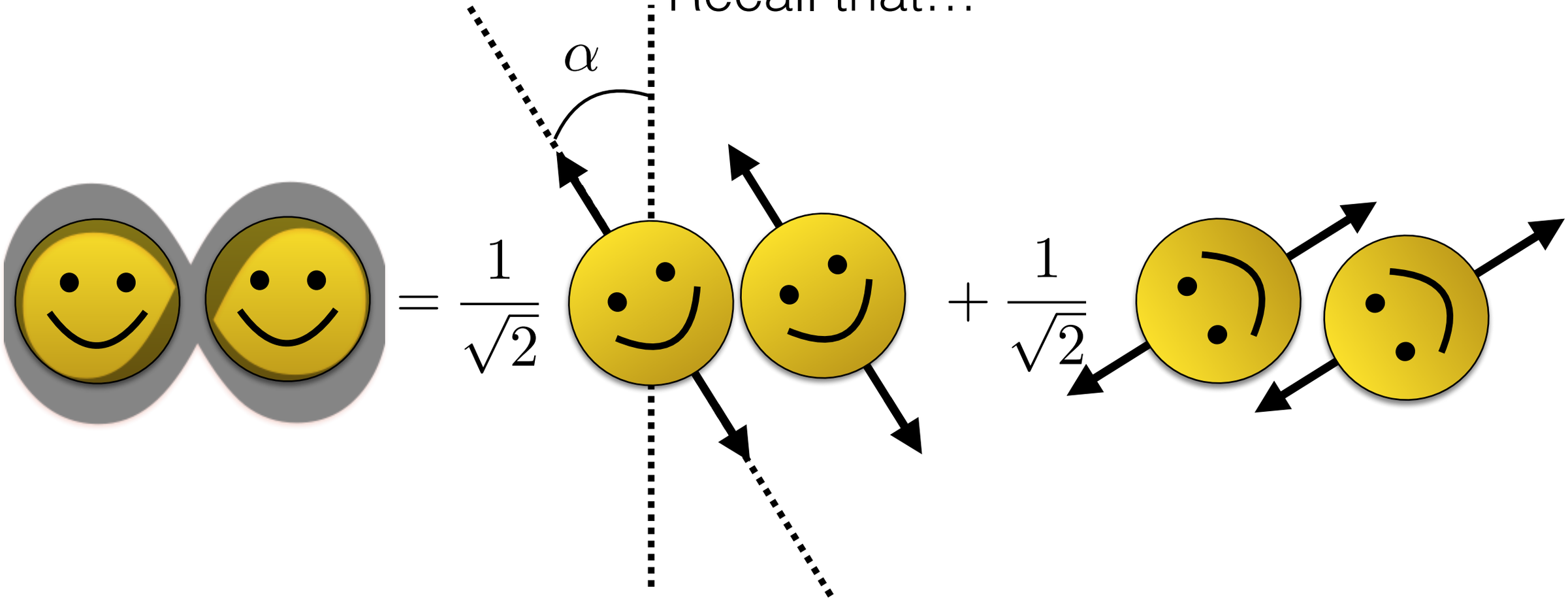


Recap

What if we re-express the Bell state in the $(|+\rangle, |-\rangle)$ basis?

$$|\phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}|+\rangle_A|+\rangle_B + \frac{1}{\sqrt{2}}|-\rangle_A|-\rangle_B$$

Recall that…



For any α

Recap

Recall that measurements are essentially performed in the eigenbasis defined by a hermitian operator

$$O = O^\dagger$$

$$O|v_i\rangle = \lambda_i |v_i\rangle$$

$\{|v_1\rangle, |v_2\rangle, ...|v_n\rangle\}$ can form an orthonormal basis

For simplicity assume no two eigenvalues are the same (operator is non-degenerate)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Recap

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

X has eigenvectors $(|+\rangle, |-\rangle)$

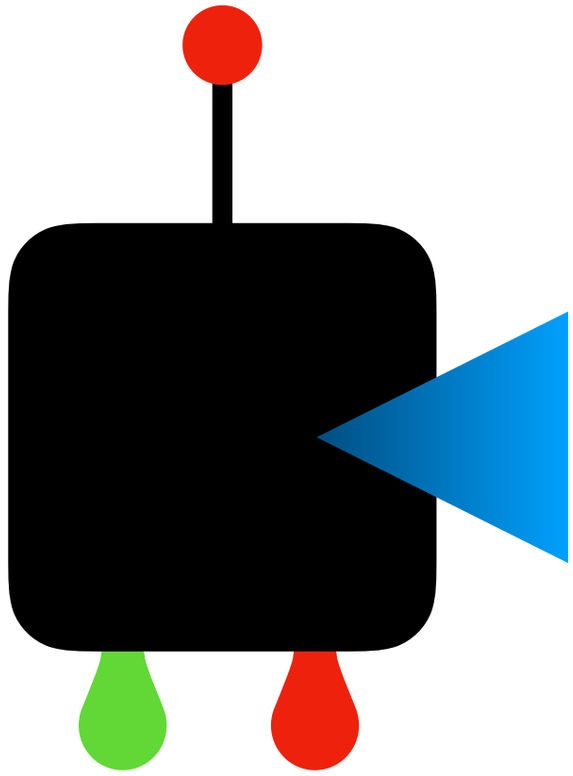
Z has eigenvectors $(|0\rangle, |1\rangle)$

Saying that we “measure an operator O” is the same as measuring in the basis of its eigenvectors

We’ll also consider

$$H_+ = \frac{1}{\sqrt{2}}(X + Z) \qquad H_- = \frac{1}{\sqrt{2}}(X - Z)$$

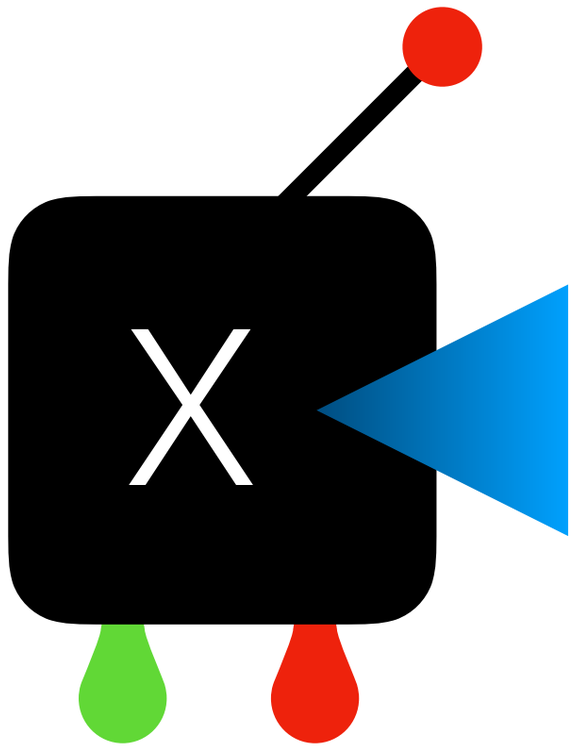
A simple experiment



$|\phi_+\rangle$

Alice will measure one qubit of a Bell state

A simple experiment

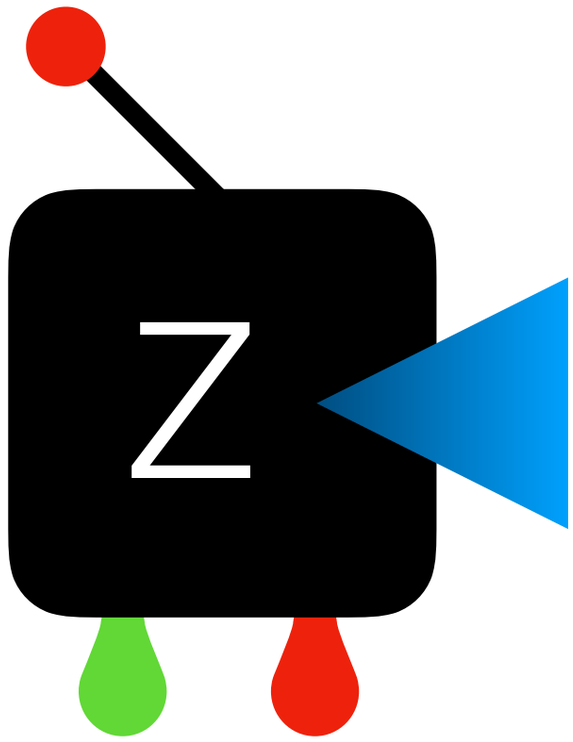


$|\phi_+\rangle$

Alice will measure one qubit of a Bell state

She will either measure X

A simple experiment



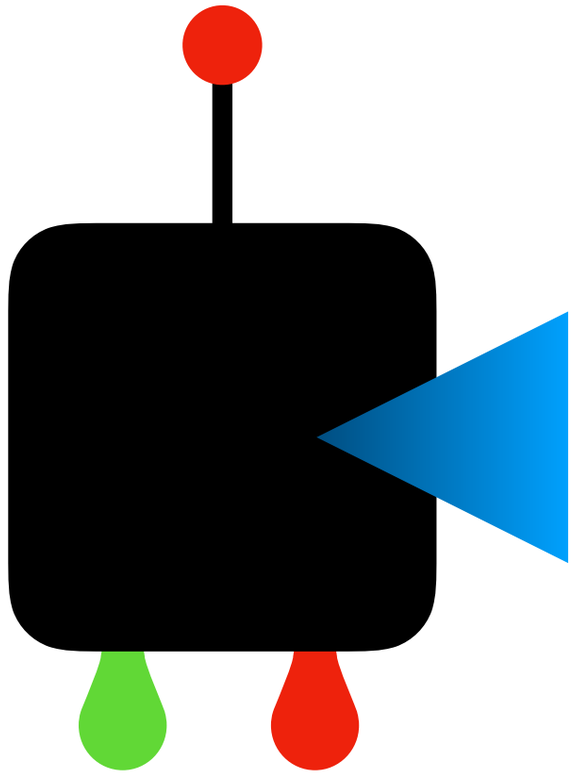
$|\phi_+\rangle$

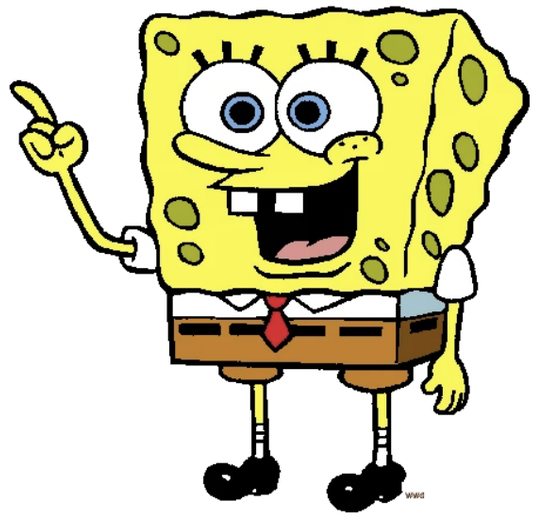
Alice will measure one qubit of a Bell state

She will either measure X

Or she will measure Z

A simple experiment





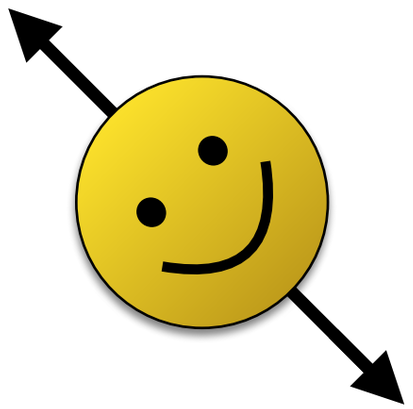
Alice will measure one qubit of a Bell state

She will either measure X

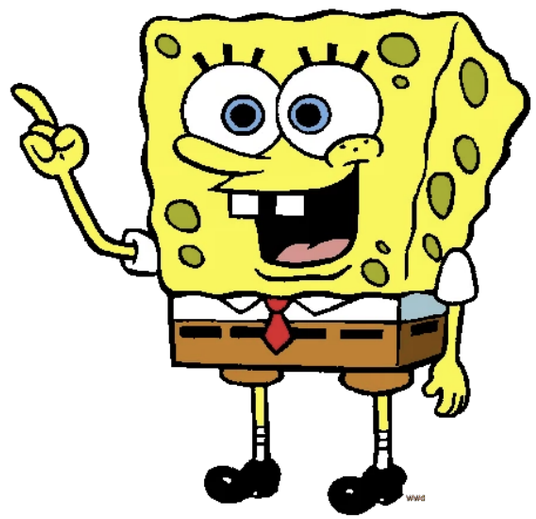
Or she will measure Z

She will give the second qubit to Bob

A simple experiment

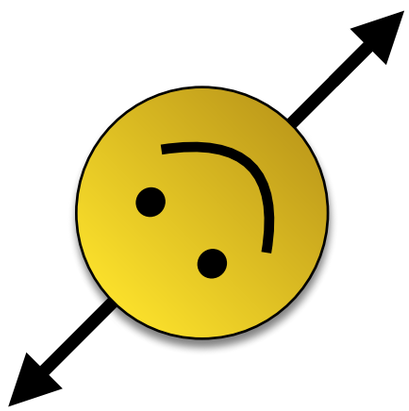


$|+\rangle$

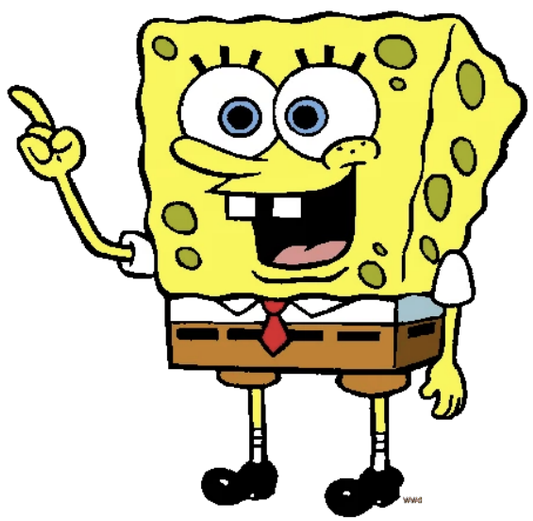


If Alice measured X and got outcome 0, she knows Bob's qubit is in the state $|+\rangle$

A simple experiment



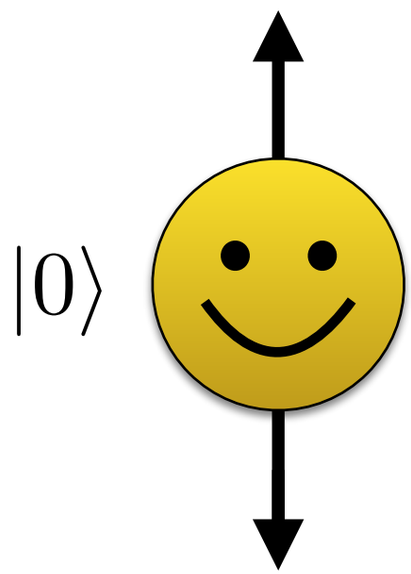
$|-\rangle$

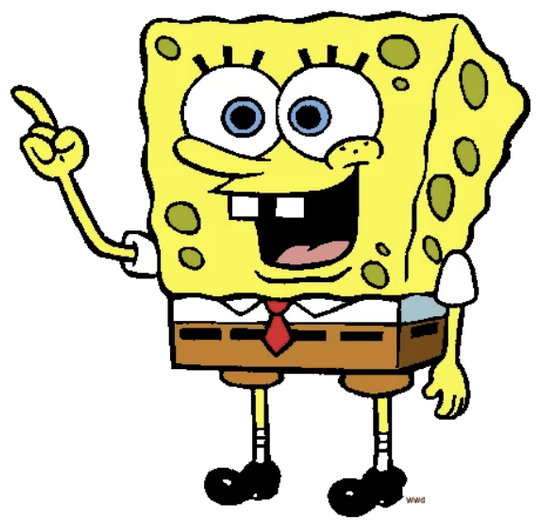


If Alice measured X and got outcome 0, she knows Bob's qubit is in the state $|+\rangle$

If Alice measured X and got outcome 1, she knows Bob's qubit is in the state $|-\rangle$

A simple experiment



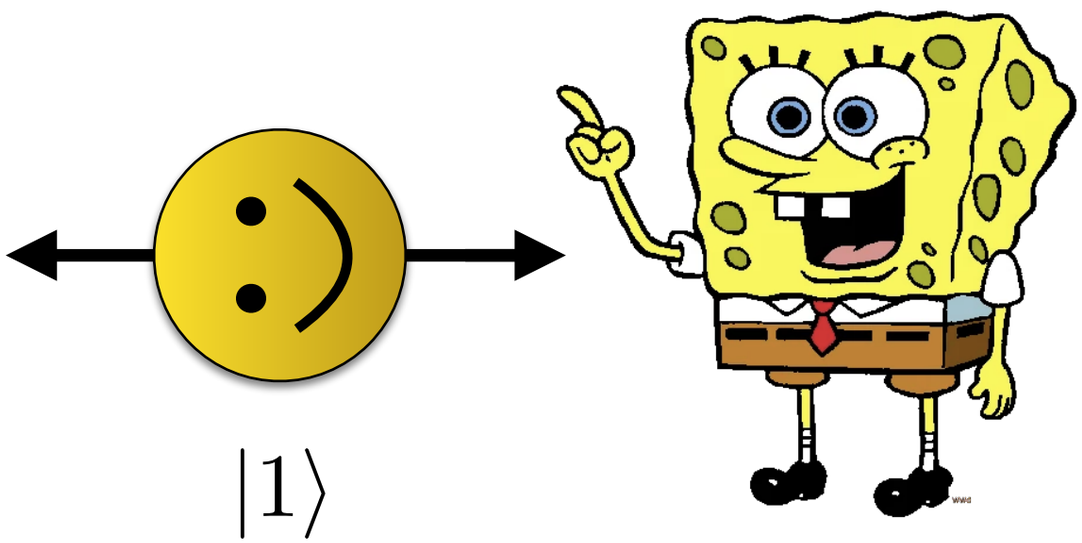


If Alice measured X and got outcome 0, she knows Bob's qubit is in the state $|+\rangle$

If Alice measured X and got outcome 1, she knows Bob's qubit is in the state $|-\rangle$

If Alice measured Z and got outcome 0, she knows Bob's qubit is in the state $|0\rangle$

A simple experiment



$|1\rangle$

If Alice measured X and got outcome 0, she knows Bob's qubit is in the state $|+\rangle$

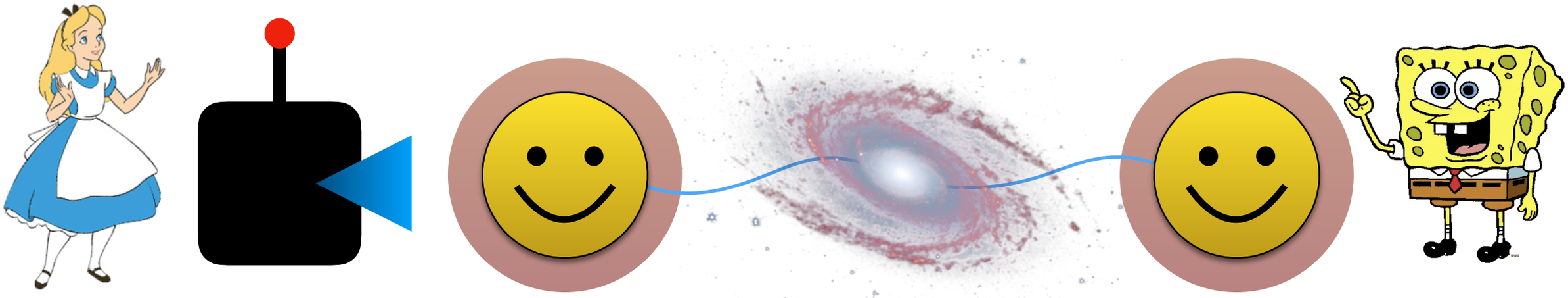
If Alice measured X and got outcome 1, she knows Bob's qubit is in the state $|-\rangle$

If Alice measured Z and got outcome 0, she knows Bob's qubit is in the state $|0\rangle$

If Alice measured Z and got outcome 1, she knows Bob's qubit is in the state $|1\rangle$

A simple experiment

But what if Alice and Bob were separated by a large distance when the experiment began



How can Alice instantaneously know Bob's state?

Was his state pre-determined from the beginning?

If so, why doesn't QM account for this?

The EPR paradox

These are the questions that Einstein, Rosen and Podolsky asked

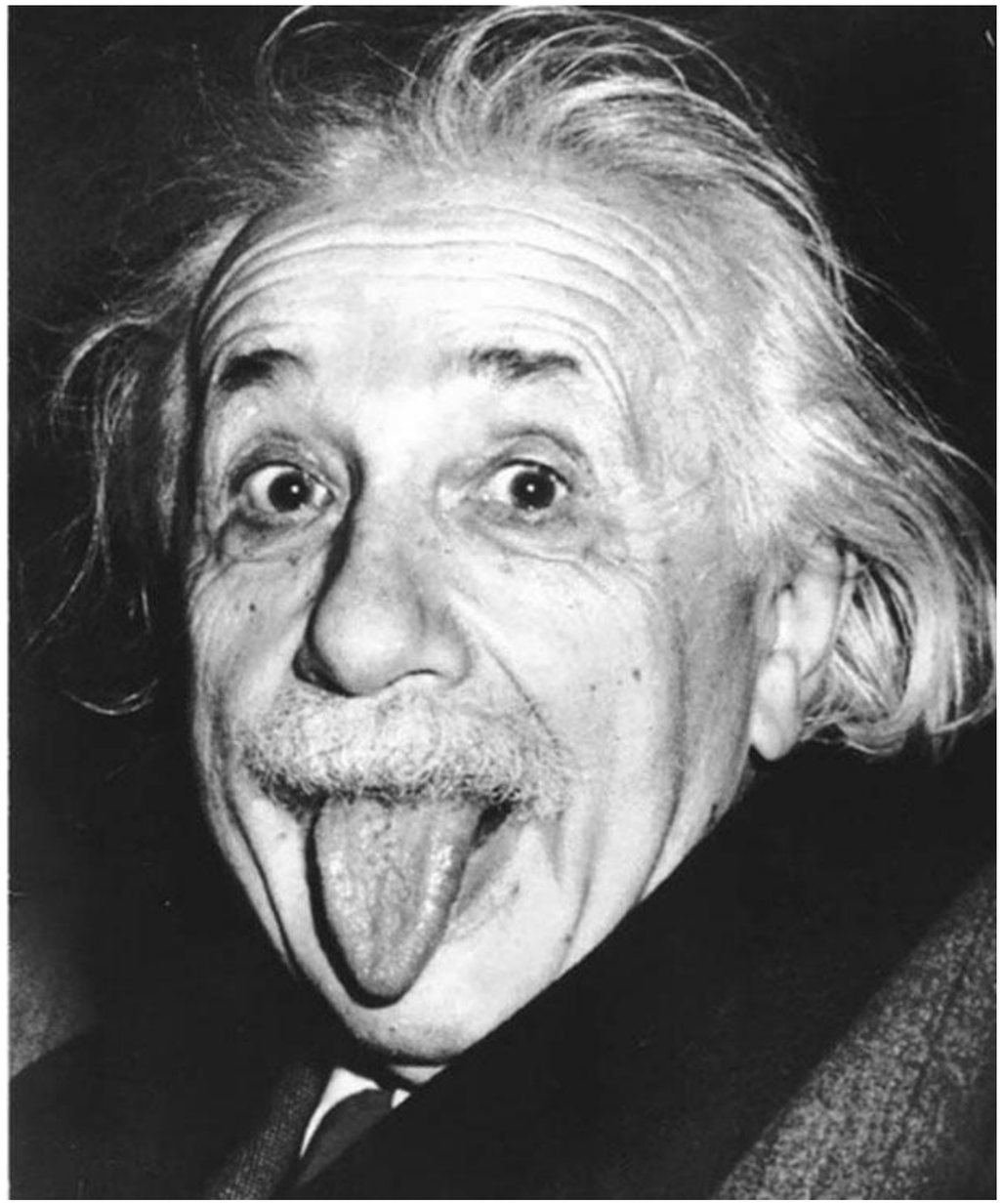
Einstein didn't like entanglement

"Spooky action-at-a-distance"

They concluded that there is a contradiction between the following

1. QM provides a <u>complete</u> description of nature

2. Any action at-a-distance must propagate <u>at most</u> at the speed of light

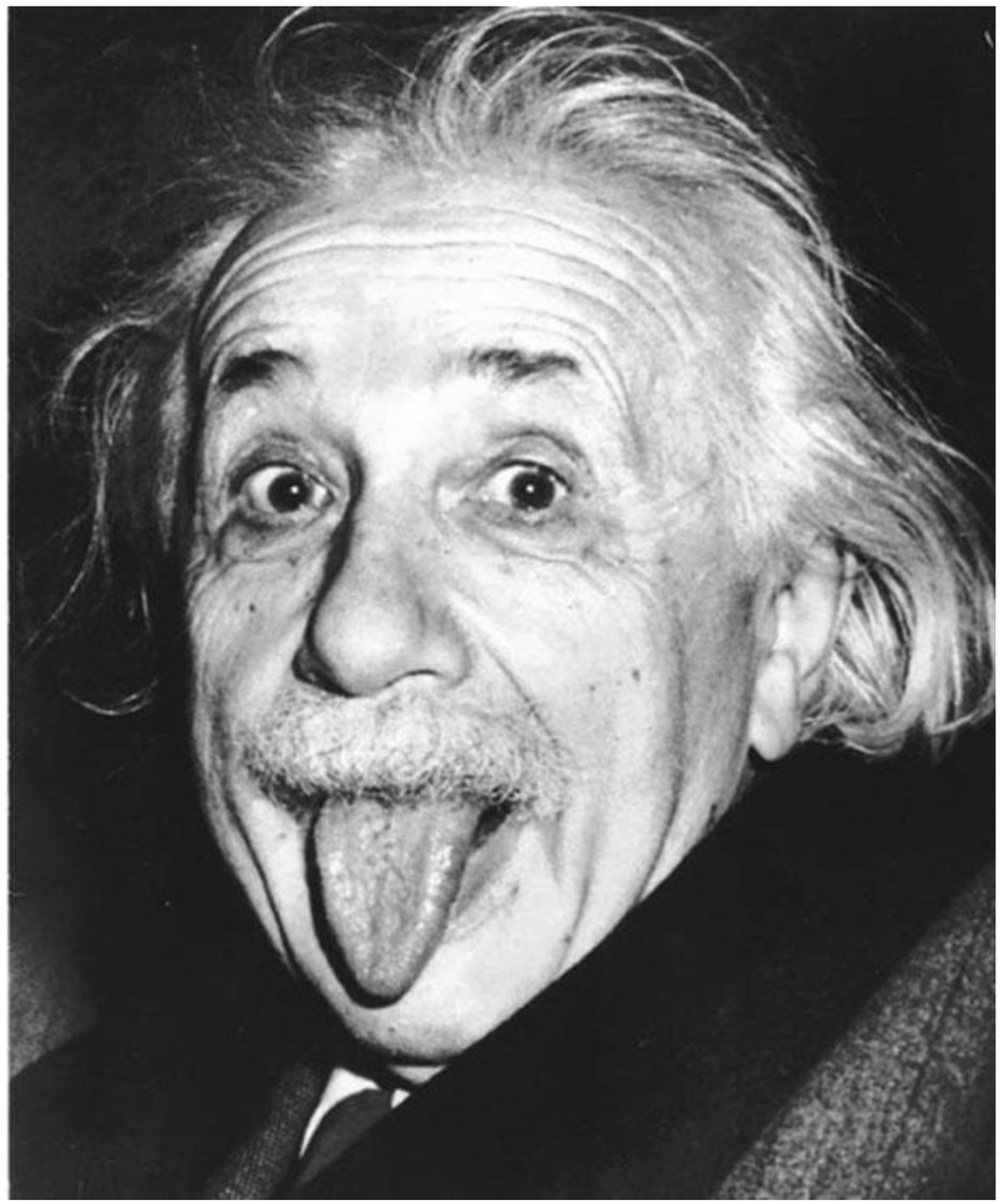


The EPR paradox

These are the questions that Einstein, Rosen and Podolsky asked

Einstein didn't like entanglement

"Spooky action-at-a-distance"



They concluded that there is a contradiction between the following

1. Completeness

2. Locality

Since locality is in the spirit of relativity, they dropped completeness

The EPR paradox

There are actually 3 ways to resolve the contradiction

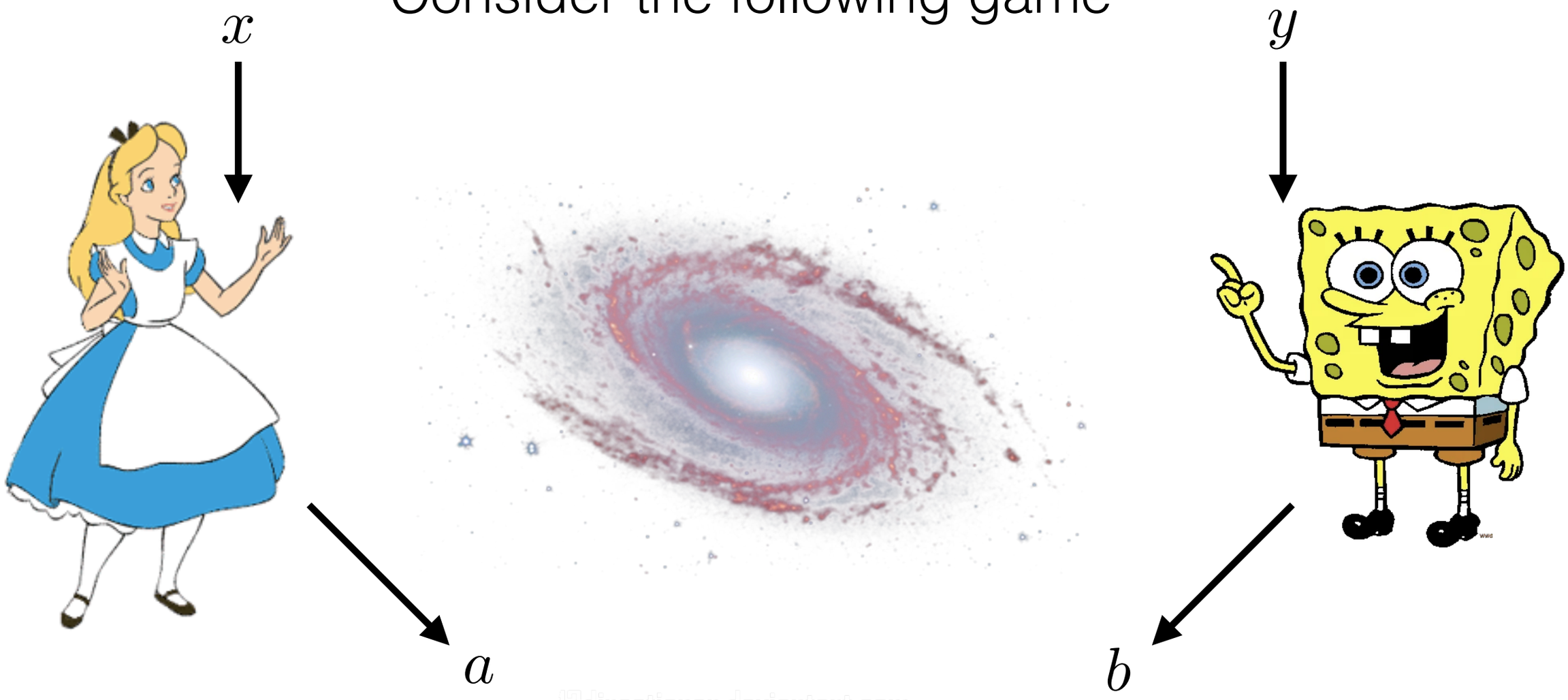
1. Completeness is wrong
2. Locality is wrong
3. Both are wrong

For the moment, let us assume completeness
is false but locality is true

QM would need to be supplemented by
local hidden-variables

CHSH game

Consider the following game



$$x, y, a, b \in \{0, 1\}$$

Alice and Bob win the game if: $a \oplus b = x \cdot y$

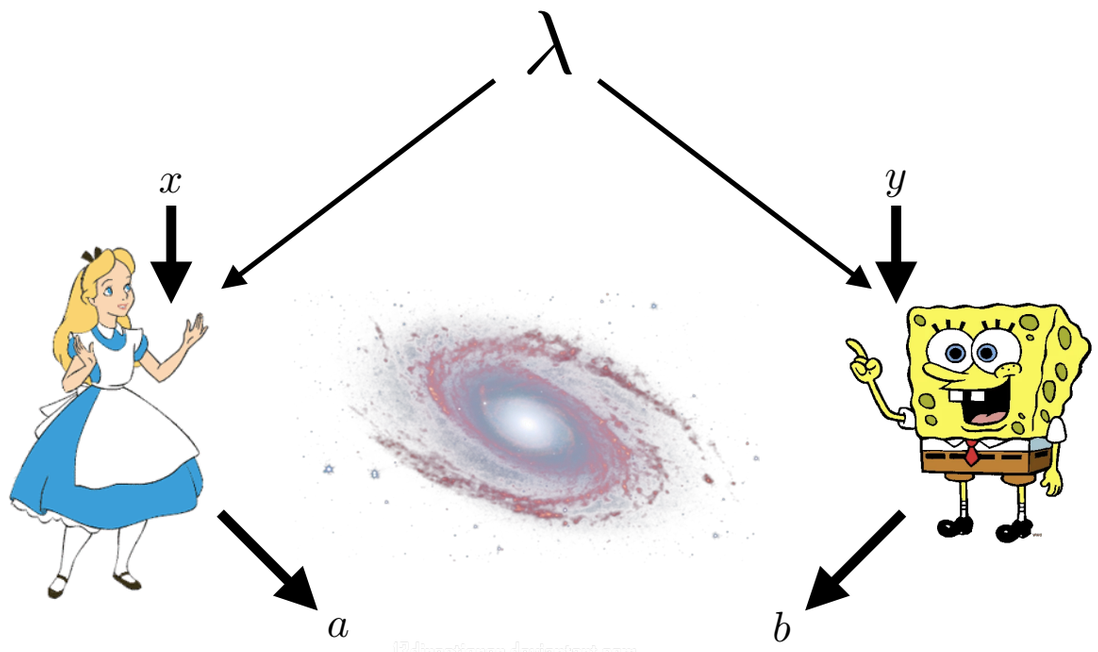
CHSH game

Alice and Bob win the game if: $a \oplus b = x \cdot y$

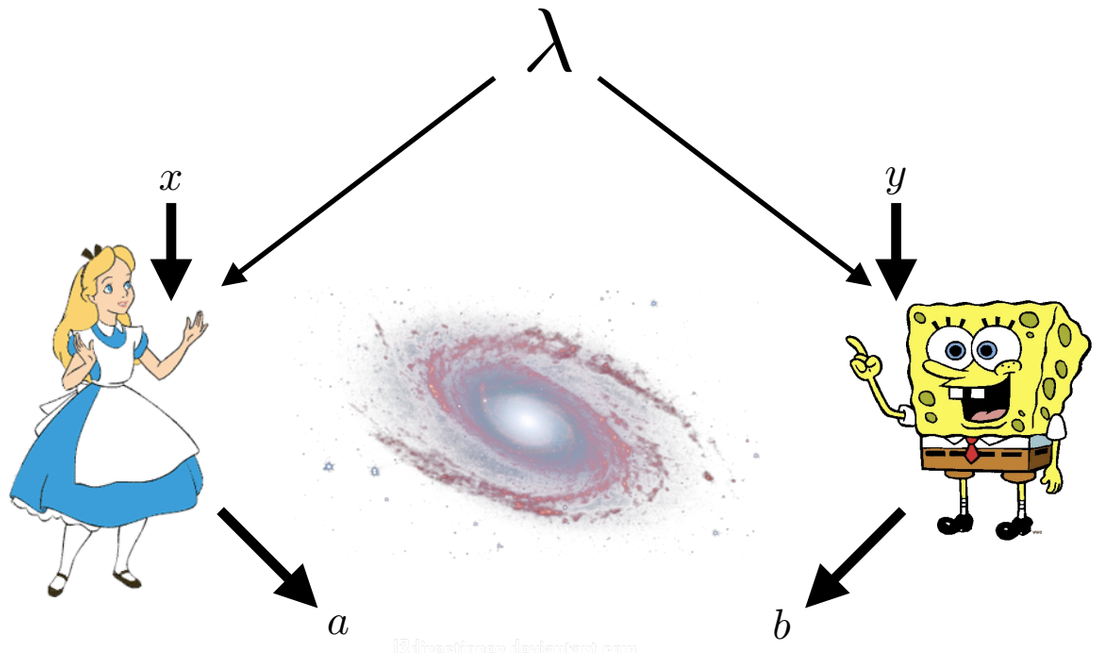
What is the maximum win-rate for the CHSH game?

Assume $Pr(x, y) = 1/4$

We're going to assume local hidden-variable theories



CHSH game



First, let's assume Alice and Bob's strategies are **deterministic**

Local hidden-variables tells us that $a(x, \lambda), b(y, \lambda)$

Alice and Bob's outcomes can only depend on their inputs and the hidden variable(s) (pre-shared information)

$$a \oplus b = x \cdot y$$

CHSH game

$$a \oplus b = x \cdot y$$

Say $a(0, \lambda) = 0$ then $b(y, \lambda) = 0$

But then $1 \oplus b(y, \lambda) = y$

Which doesn't work when y=0

Say $a(0, \lambda) = 1$ then $b(y, \lambda) = 1$

Same problem!

There is no deterministic local hidden variable strategy that achieves better than 3/4 win-rate

CHSH game

What about a probabilistic strategy?

Any probabilistic strategy can be viewed as a probabilistic mixture of deterministic strategies!

Wlog, the randomness comes from the hidden variables alone

$$Pr(a, b|x, y) = \sum_{\lambda} Pr(a|x, \lambda) Pr(b|y, \lambda) Pr(\lambda)$$

$$\sum_{\lambda} Pr(\lambda) = 1$$

$$Pr(a|x, \lambda) = 1, \text{ when } a = a(x, \lambda)$$
$$Pr(b|y, \lambda) = 1, \text{ when } b = b(y, \lambda)$$

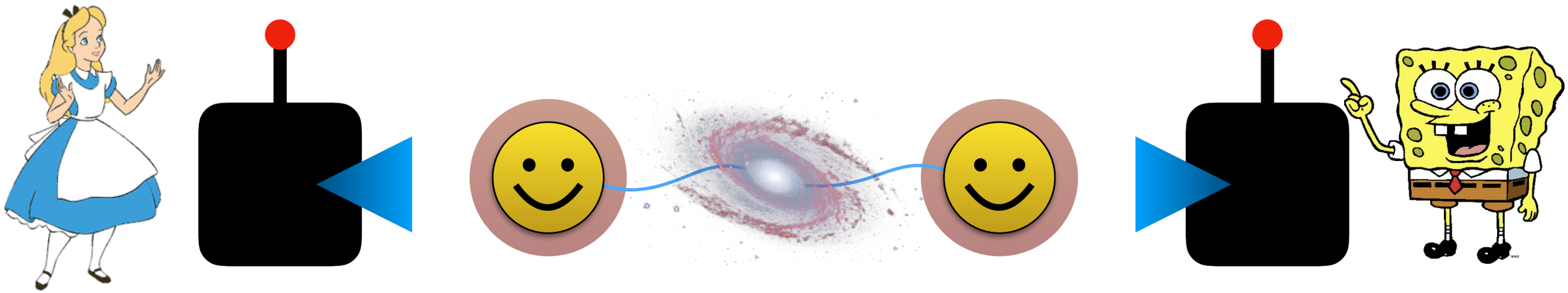
CHSH game

It follows that we cannot obtain a higher win-rate than 3/4
in a local hidden-variable theory

A similar result was shown by John Bell prior to the CHSH game

CHSH game

Now suppose Alice and Bob share a Bell state to begin with



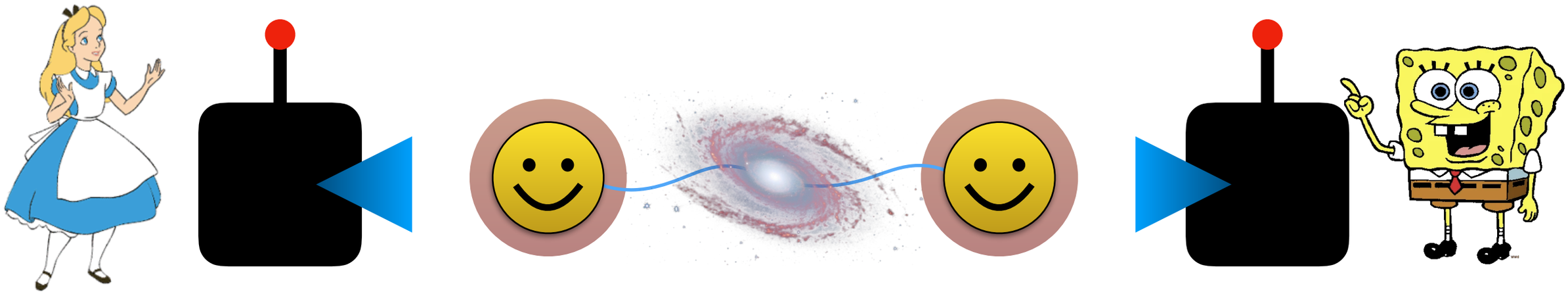
For x = 0, Alice measures X and reports outcome

For x = 1, Alice measures Z and reports outcome

For y = 0, Bob measures H_+ and reports outcome

For y = 1, Bob measures H_- and reports outcome

CHSH game



In this case, it can be shown that

$$Pr(win) = cos^2(\pi/8) \approx 0.85 > 3/4$$

This has been observed experimentally!

QM **is not** a local hidden-variable theory

Maybe QM is incomplete, but it is definitely non-local!

Bell's theorem

No theory of <u>local</u> hidden variables can reproduce the predictions of QM

"It is the requirement of locality [...] that creates the essential difficulty"

"Moreover, a hidden variable interpretation of elementary quantum theory has been explicitly constructed. That particular interpretation has indeed a grossly non-local structure."

CHSH game

But wait, there's more!

Can be shown that $cos^2(\pi/8)$ is optimal for quantum mechanics!

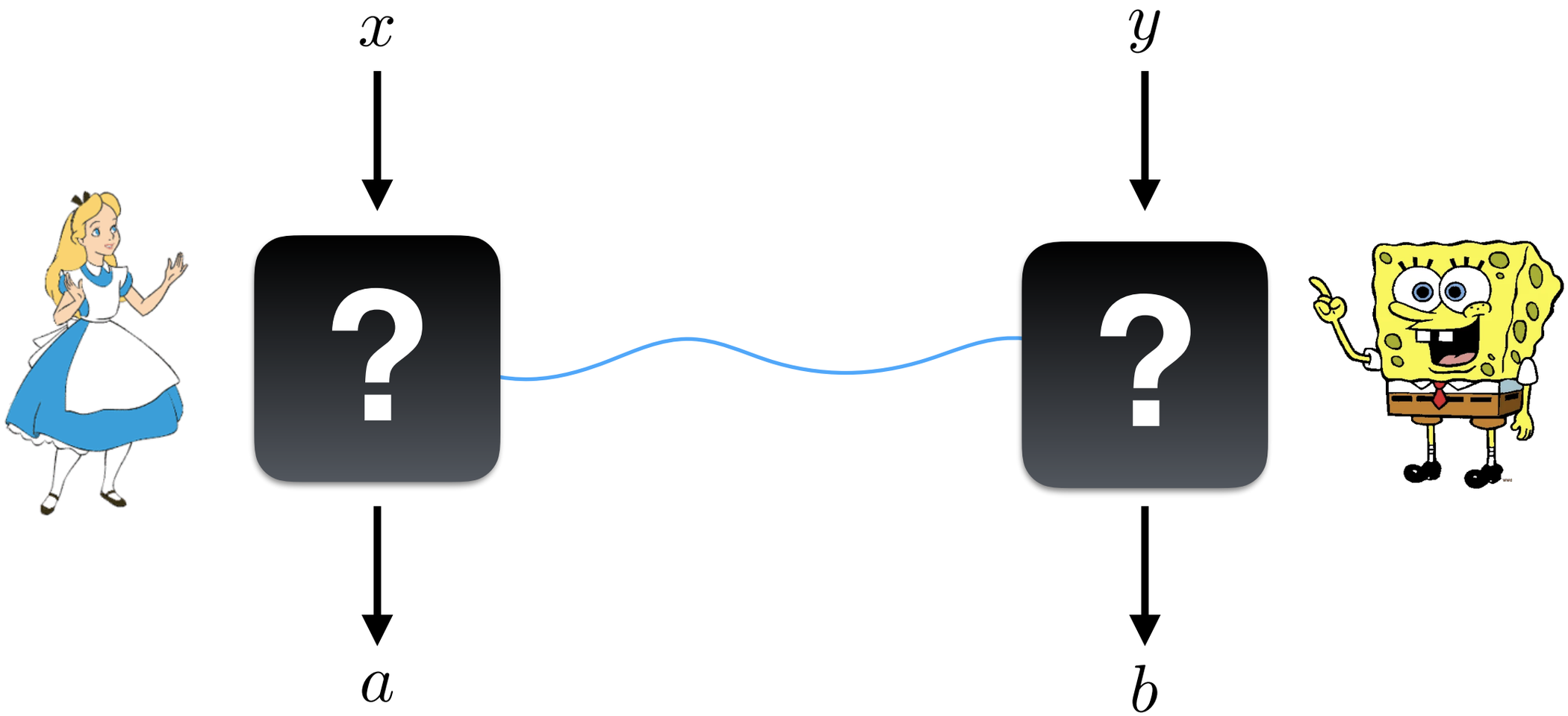
Can also be shown that the strategy we looked at
is the only one that achieves the optimum
(up to local changes of basis)

What can be concluded from this?

If we know that Alice and Bob are separated by a great distance
and they're winning the CHSH game with the optimal win-rate
then we know exactly what they're doing!

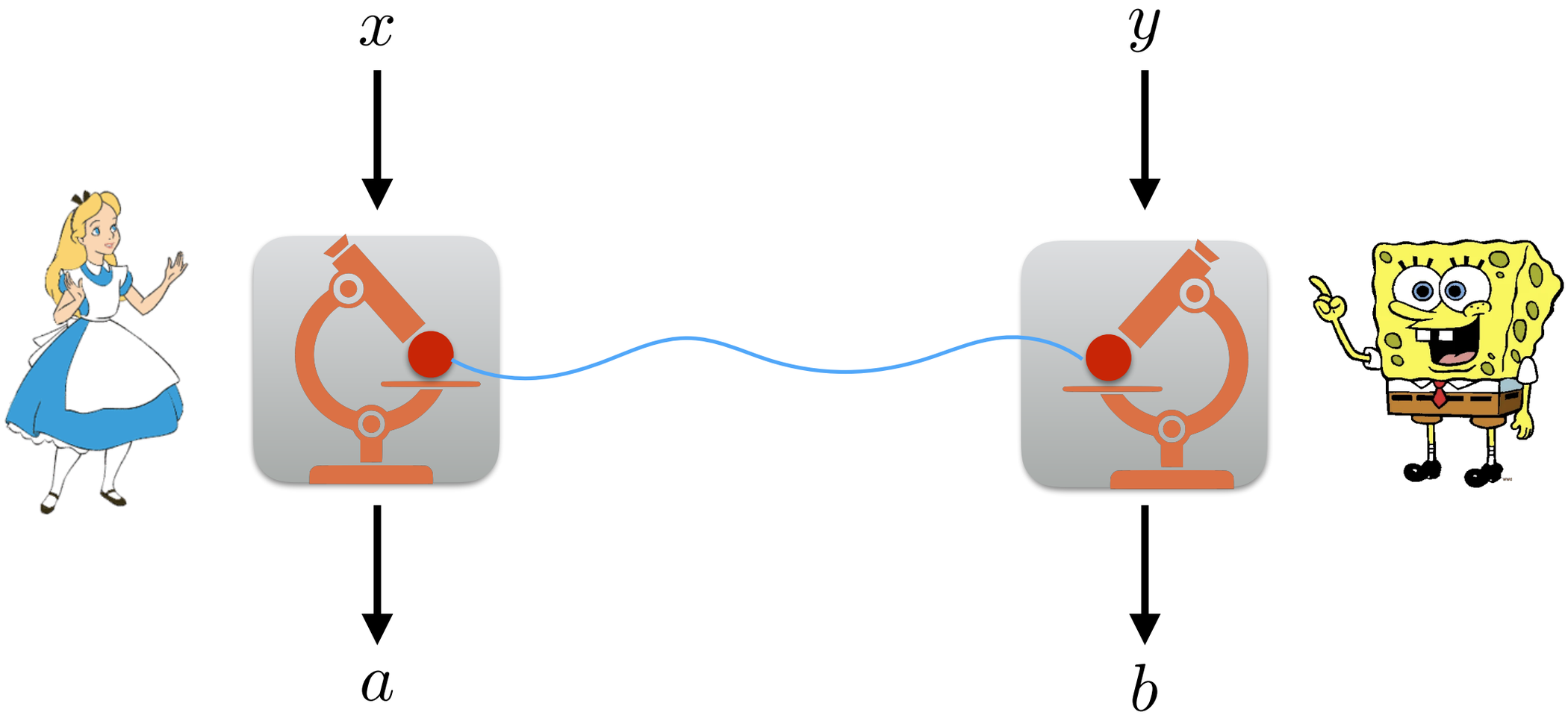
Device independence

Device independence



By just looking at correlations of their inputs and outputs
Alice and Bob can determine whp what their boxes are doing

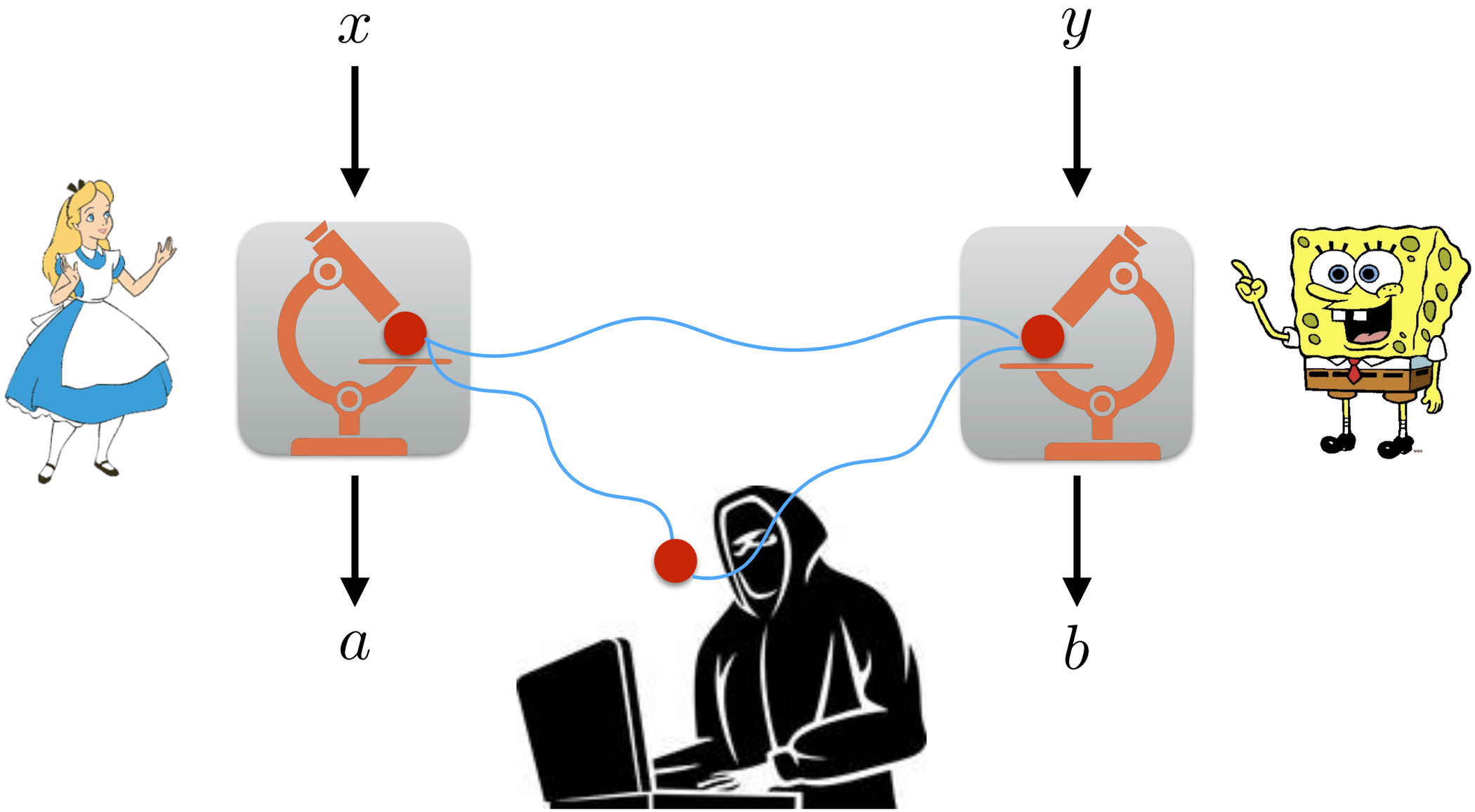
Device independence



By just looking at correlations of their inputs and outputs
Alice and Bob can determine whp what their boxes are doing

Can an attacker be correlated with their systems?

Device independence



No! This is not possible!

Monogamy of entanglement

Bell states cannot be correlated (even classically) with other states

More generally, states that saturate the CHSH game are maximally entangled

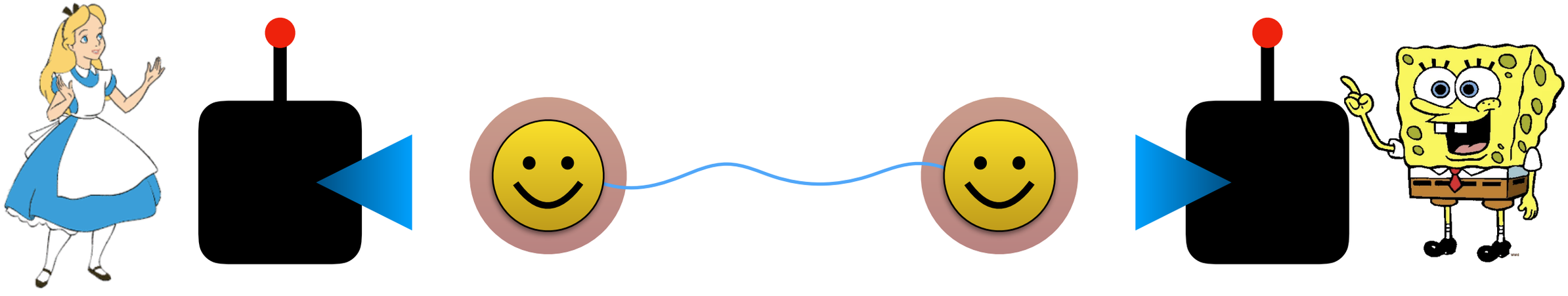
Maximal entanglement is monogamous

If 2 systems are maximally correlated (non-locally) they cannot be correlated with a third system

How do we use this for cryptography?

Ekert's protocol

The E91 protocol



Alice and Bob share Bell states
(the states can be distributed by a third party)

Alice chooses randomly to measure either: X, Z, H_+

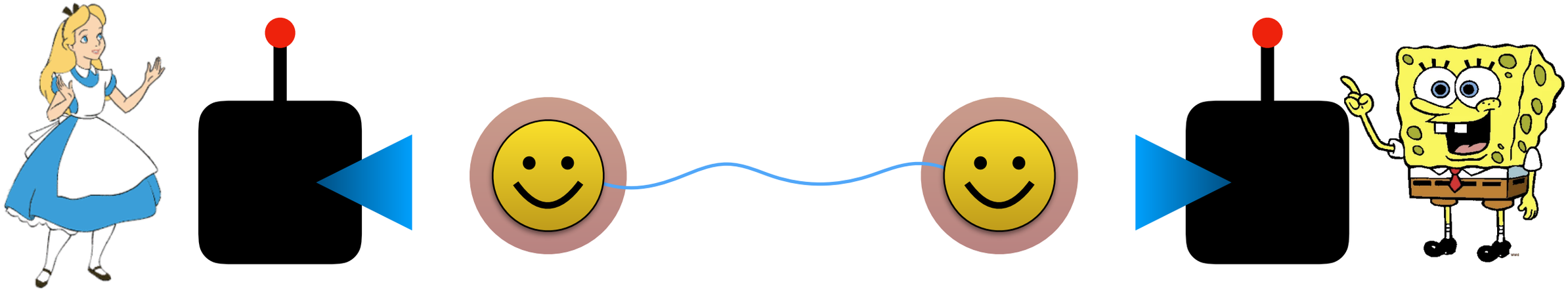
Bob chooses randomly to measure either: X, H_+, H_-

They announce the observables, but not the outcomes

When observables match, do as in BB84, otherwise CHSH
(or discard)

Ekert's protocol

The E91 protocol



Essentially, Alice and Bob are using CHSH to test that they indeed share Bell states and these are measured correctly

If so, they trust the remaining measurement outcomes and proceed as in BB84

The non-local correlations allow them to test their devices!

Some final remarks

What if devices store classical outcomes and transmit them later?

This is one of the caveats to device-independence (solutions include isolating devices or destroying them after use)

Device-independence proofs are notoriously difficult!

The same setup can be used to implement device-independent randomness generation

Different types of device independence (measurement device-independence, one-sided device independence etc)

References and resources

The EPR paper

https://journals.aps.org/pr/abstract/10.1103/PhysRev.47.777

http://www.drchinese.com/David/EPR.pdf

Einstein, incompleteness,
and the epistemic view of quantum states

https://arxiv.org/abs/0706.2661

Two awesome lectures on entanglement by R. Spekkens

http://pirsa.org/displayFlash.php?id=16070008

http://pirsa.org/displayFlash.php?id=16070014

Contextuality

http://scienceblogs.com/pontiff/2008/01/17/contextuality-of-quantum-theor/

https://plato.stanford.edu/entries/kochen-specker/

References and resources

Bell's paper

https://web.archive.org/web/20131126021928/http://philoscience.unibe.ch/documents/TexteHS10/bell1964epr.pdf

The CHSH paper

https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.23.880

The magic square game

https://en.wikipedia.org/wiki/Quantum_pseudo-telepathy#The_Mermin-Peres_magic_square_game

What Bell did, T. Maudlin

https://arxiv.org/abs/1408.1826

Computational perspectives on Bell inequalities and many-body quantum correlations, M. Hoban

https://arxiv.org/pdf/1204.5913.pdf

References and resources

Device-independence

https://arxiv.org/abs/quant-ph/9809039

https://arxiv.org/pdf/quant-ph/0405101.pdf

https://arxiv.org/abs/1201.4407

https://arxiv.org/pdf/1210.1810.pdf

Device independence with more than 2 devices

https://arxiv.org/abs/1309.5675

https://arxiv.org/abs/1706.07090