A device-independent test of an entropic uncertainty relation

and its application to quantum cryptography

Charles Ci Wen Lim
Group of Applied Physics, University of Geneva

in collaboration with
Christopher Portmann, Marco Tomamichel, Renato Renner and Nicolas Gisin

(Practical) Main Messages

(Practical) Main Messages

1. A simple framework for cryptographic protocols with minimal assumptions.

(Practical) Main Messages

1. A simple framework for cryptographic protocols with minimal assumptions.

2. Bell's inequalities can be used to certify entropic uncertainty relations.

(Practical) Main Messages

1. A simple framework for cryptographic protocols with minimal assumptions.

2. Bell's inequalities can be used to certify entropic uncertainty relations.

Uncertainty Principle

Traditional version

In the strict formulation of the law of causality—if we know the present, we can calculate the future—it is not the conclusion that is wrong but the premise. On an implication of the uncertainty principle.

Werner Heisenberg

Uncertainty Principle

Traditional version

In the strict formulation of the law of causality—if we know the present, we can calculate the future—it is not the conclusion that is wrong but the premise. On an implication of the uncertainty principle.

Werner Heisenberg

Robertson–Schrödinger Uncertainty Principle

$$\Delta\mathcal{O}_X \Delta\mathcal{O}_Z \geq \frac{1}{2} \left|\langle\phi|[\mathcal{O}_Z, \mathcal{O}_X]|\phi\rangle\right|$$

where $\Delta\mathcal{O}_A = \sqrt{\langle\phi|\mathcal{O}_A^2|\phi\rangle - \langle\phi|\mathcal{O}_A|\phi\rangle^2}$

Uncertainty Principle

Traditional version

In the strict formulation of the law of causality—if we know the present, we can calculate the future—it is not the conclusion that is wrong but the premise. On an implication of the uncertainty principle.

Werner Heisenberg

Robertson–Schrödinger Uncertainty Principle

$$\Delta\mathcal{O}_X \Delta\mathcal{O}_Z \geq \frac{1}{2} \left|\langle\phi|[\mathcal{O}_Z, \mathcal{O}_X]|\phi\rangle\right|$$

where $\Delta\mathcal{O}_A = \sqrt{\langle\phi|\mathcal{O}_A^2|\phi\rangle - \langle\phi|\mathcal{O}_A|\phi\rangle^2}$

State-dependent!!!

Uncertainty Principle

Traditional version

Robertson–Schrödinger Uncertainty Principle

$$\Delta \mathcal{O}_X \Delta \mathcal{O}_Z \geq \frac{1}{2} \left| \langle \phi | [\mathcal{O}_Z, \mathcal{O}_X] | \phi \rangle \right|$$

A statistical statement for two (specified) measurements and a (specified) state

Uncertainty Principle

Traditional version

Robertson–Schrödinger Uncertainty Principle

$$\Delta \mathcal{O}_X \Delta \mathcal{O}_Z \geq \frac{1}{2} \left| \langle \phi | [\mathcal{O}_Z, \mathcal{O}_X] | \phi \rangle \right|$$

A statistical statement for two (specified) measurements and a (specified) state

To (verify) test this inequality, we require the accurate preparation of the specified input state and the specified measurements.

Uncertainty Principle

Entropic version

Rewrite it in terms of information-theoretic quantities: Shannon Entropies

Uncertainty Principle

Entropic version

Rewrite it in terms of information-theoretic quantities: Shannon Entropies

Def. of Shannon Entropy for a RV.

$$H(X) := -\sum_x \Pr[X = x] \log \Pr[X = x]$$

Uncertainty Principle

Entropic version

Rewrite it in terms of information-theoretic quantities: Shannon Entropies

Def. of Shannon Entropy for a RV.

$$H(X) := -\sum_x \Pr[X = x] \log \Pr[X = x]$$

Maassen-Uffink Entropic Uncertainty Principle

$$H(X) + H(Z) \geq -\log \max_{x,z} |\langle x|z\rangle|^2$$

for any two projective measurements

$$\mathbb{M}_X := \{|x\rangle\langle x|\}_x, \mathbb{M}_Z := \{|z\rangle\langle z|\}_z$$

Uncertainty Principle

Entropic version

Rewrite it in terms of information-theoretic quantities: Shannon Entropies

Def. of Shannon Entropy for a RV.

$$H(X) := -\sum_x \Pr[X = x] \log \Pr[X = x]$$

Maassen-Uffink Entropic Uncertainty Principle

$$H(X) + H(Z) \geq -\log \max_{x,z} |\langle x|z\rangle|^2$$

State-independent!!!

for any two projective measurements

$$\mathbb{M}_X := \{|x\rangle\langle x|\}_x, \mathbb{M}_Z := \{|z\rangle\langle z|\}_z$$

Uncertainty Principle

Entropic version

Maassen-Uffink Entropic Uncertainty Principle

$$H(X) + H(Z) \geq -\log \max_{x,z} |\langle x|z\rangle|^2$$

Uncertainty Principle

Entropic version

Maassen-Uffink Entropic Uncertainty Principle

$$H(X) + H(Z) \geq -\log \max_{x,z} |\langle x|z\rangle|^2$$

Example.

Choose the measurements as the Pauli X and Z operators σ_X, σ_Z

$$H(X) + H(Z) \geq 1$$

Uncertainty Principle

Entropic version

Maassen-Uffink Entropic Uncertainty Principle

$$H(X) + H(Z) \geq -\log \max_{x,z} |\langle x|z\rangle|^2$$

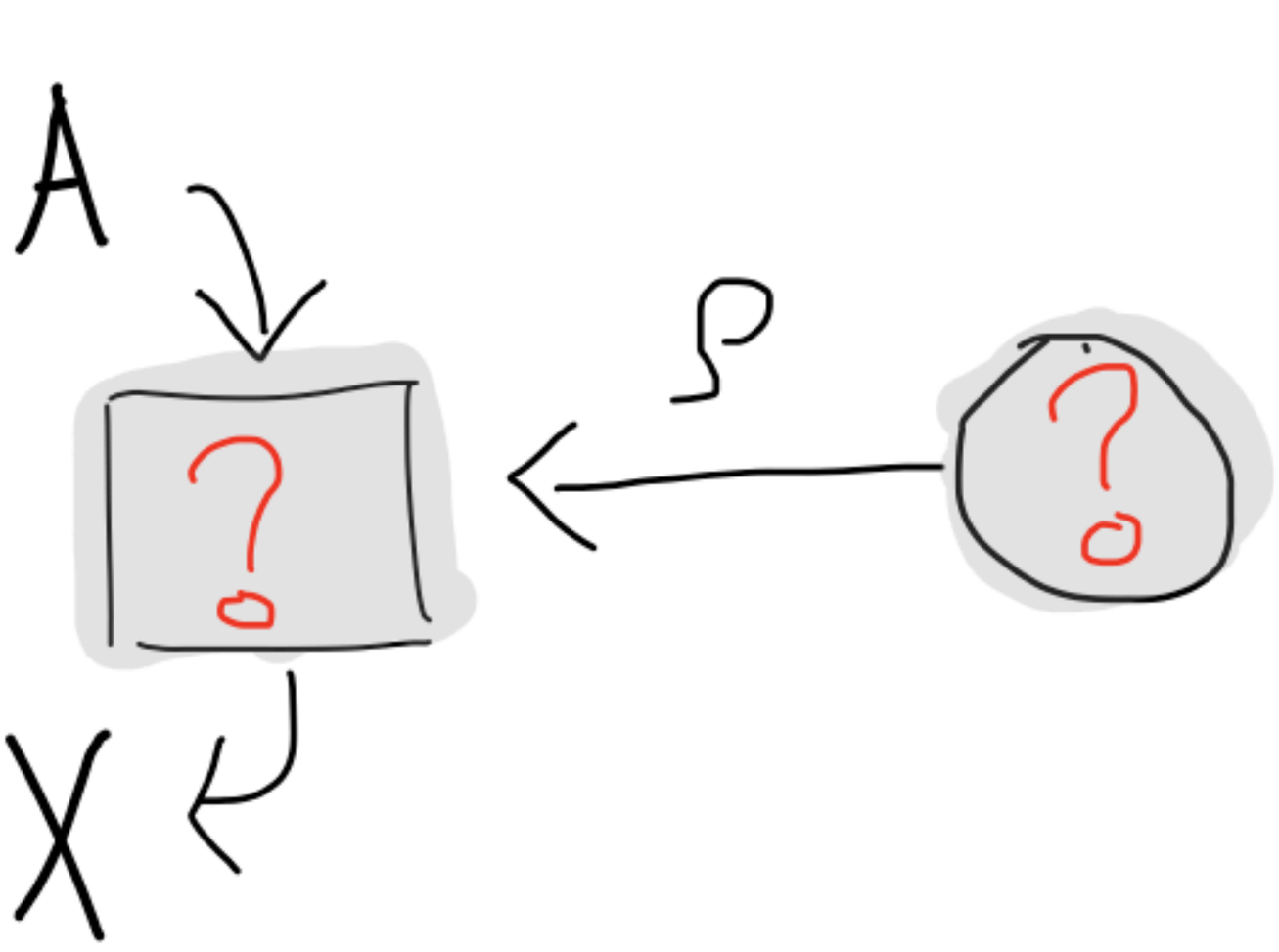
Example.

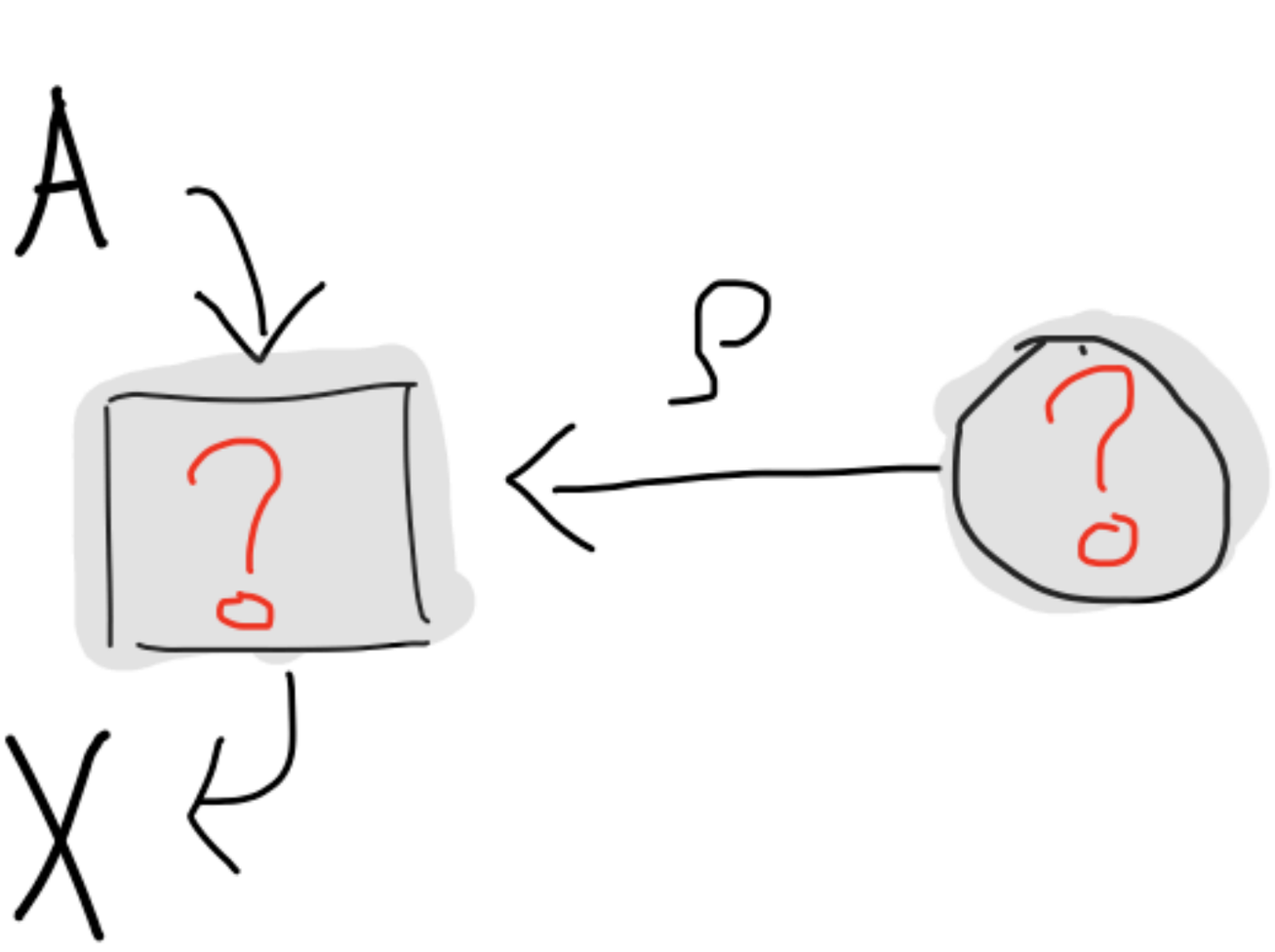
Choose the measurements as the Pauli X and Z operators σ_X, σ_Z

$$H(X) + H(Z) \geq 1$$

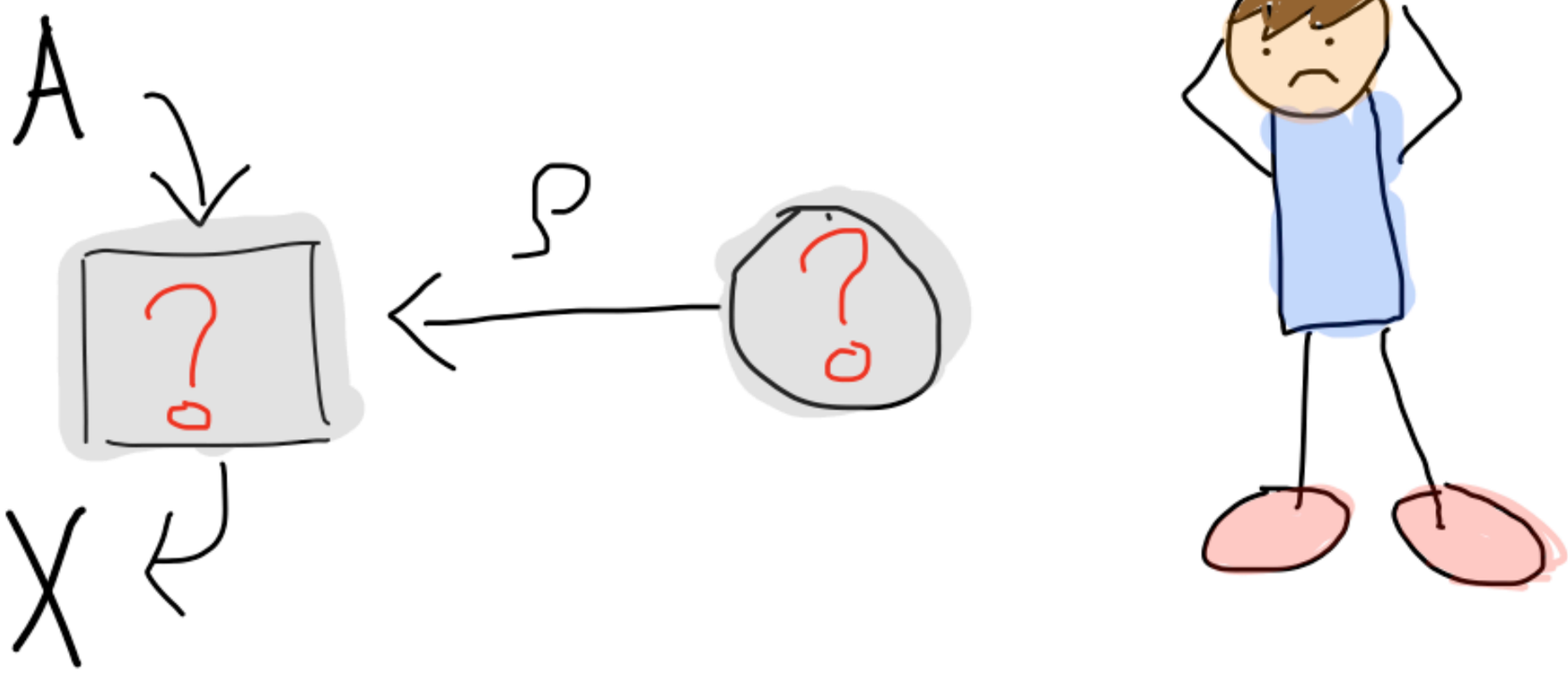
Certainty vs Uncertainty, e.g.,

$$H(X) = 0 \Rightarrow H(Z) = 1$$


A
ρ
?
?
X

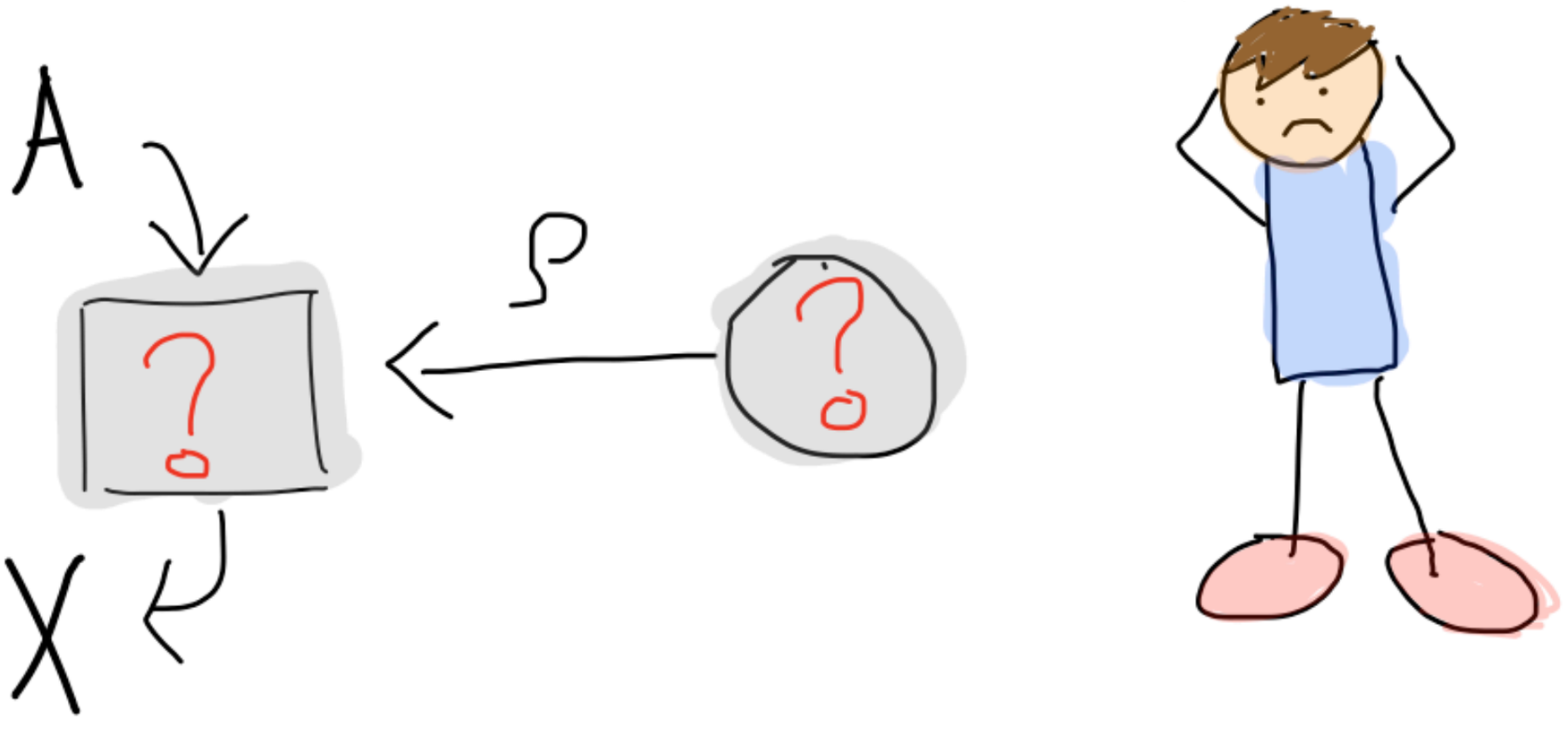


(Informal) Problem Statement:
How do we know if the setup "respects" the uncertainty principle?

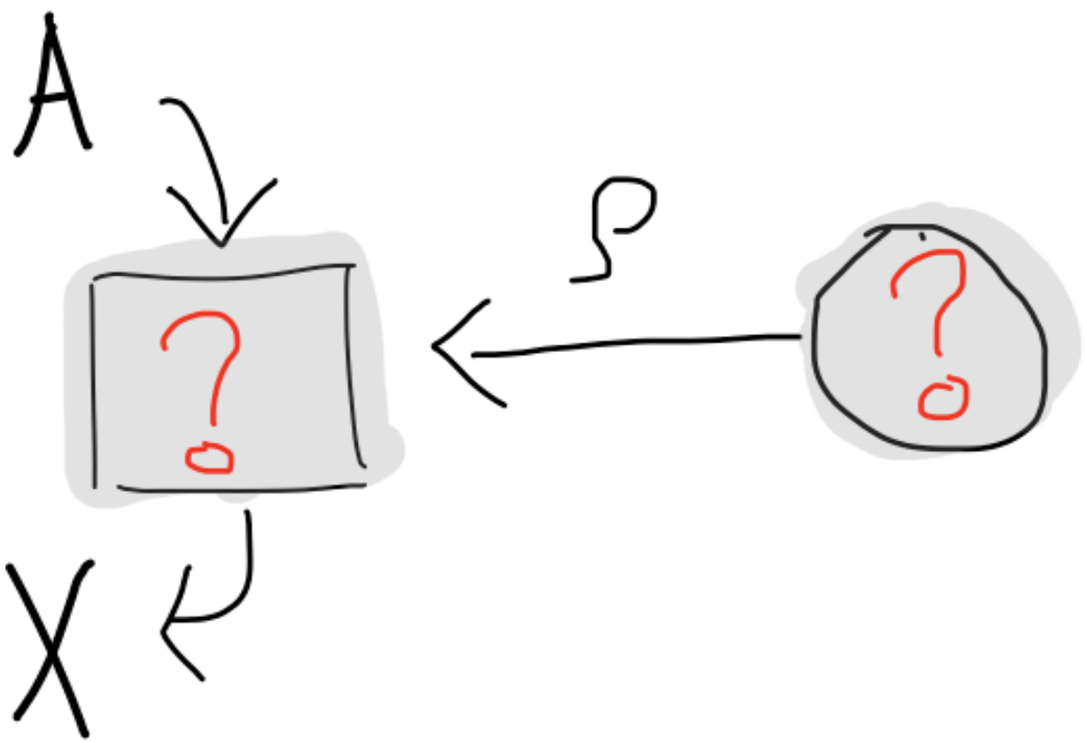

A
ρ
X

Accessible statistics in the Expt:
conditional probabilities

$$\{\Pr[X = x | A = a]\}_{x,a}$$

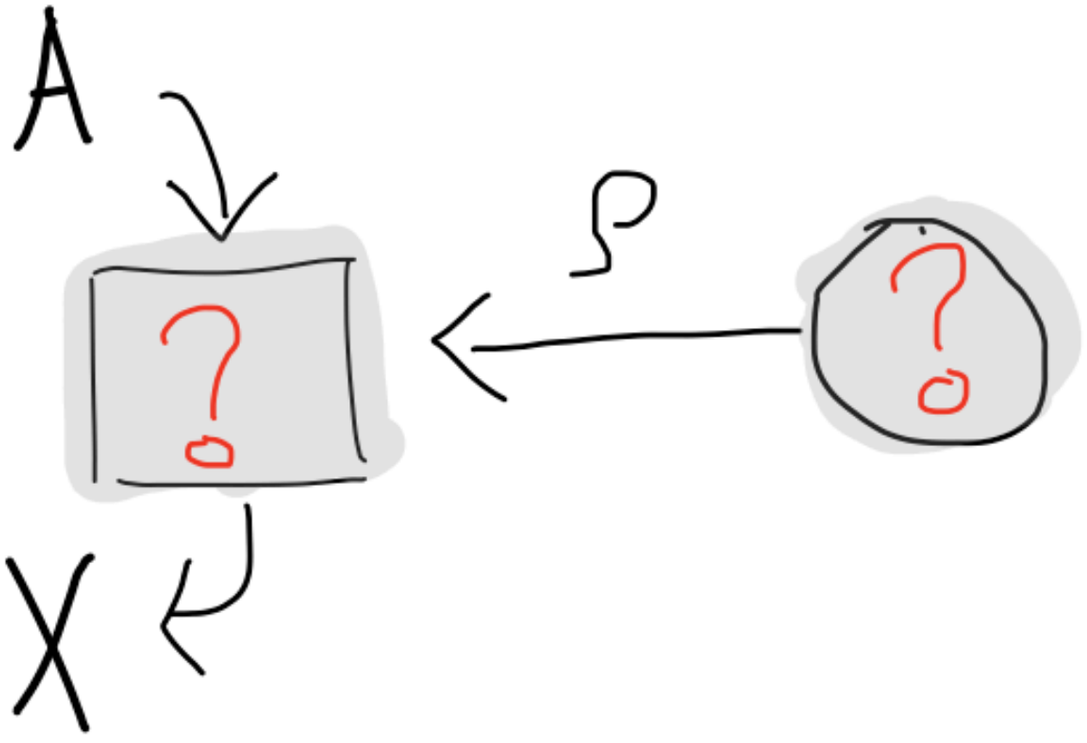


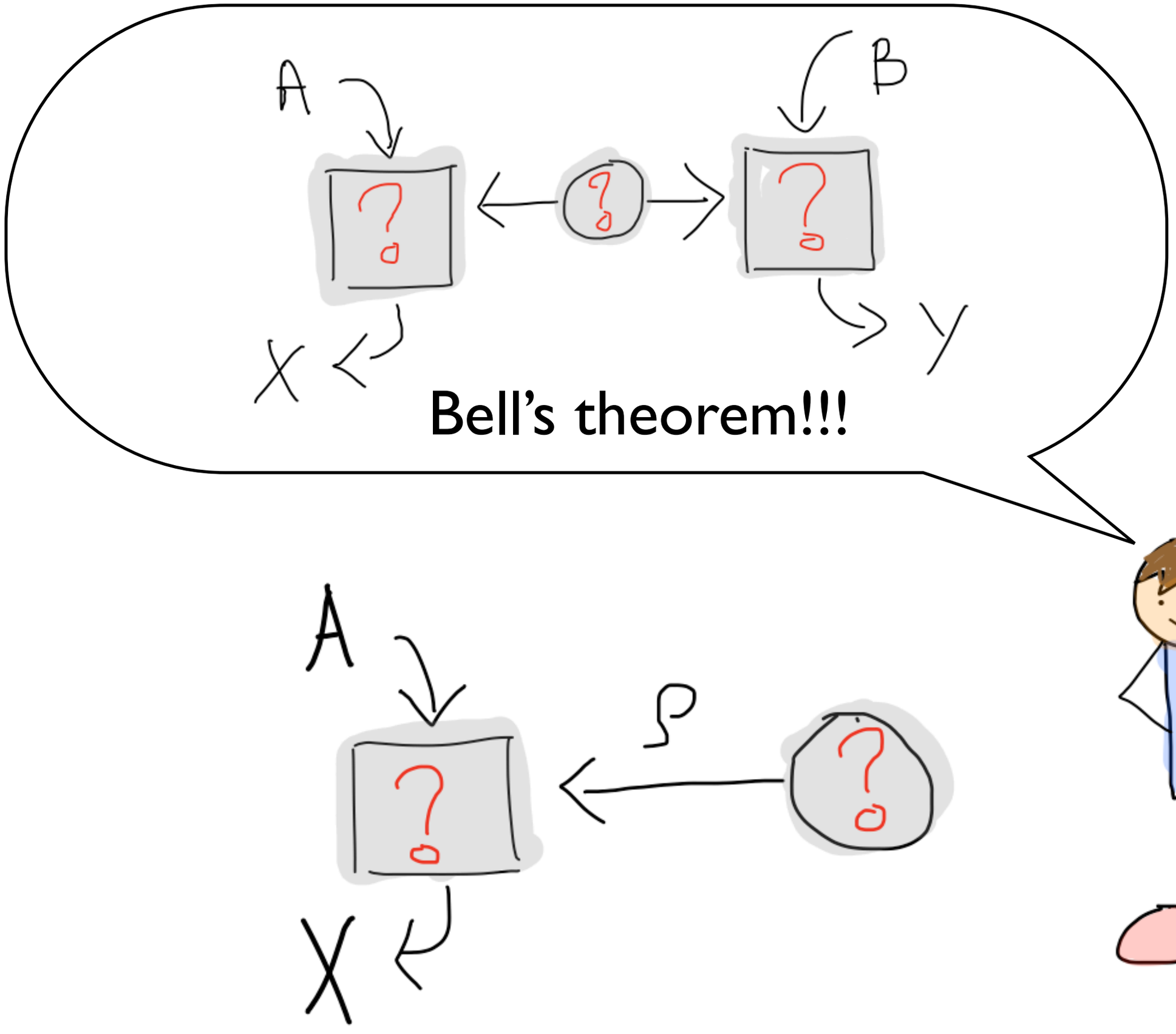
However, in this situation, there is always a classical strategy that can be used to explain any statistics (predicted by quantum mechanics).



In that case, lets try to imagine a bipartite scenario...

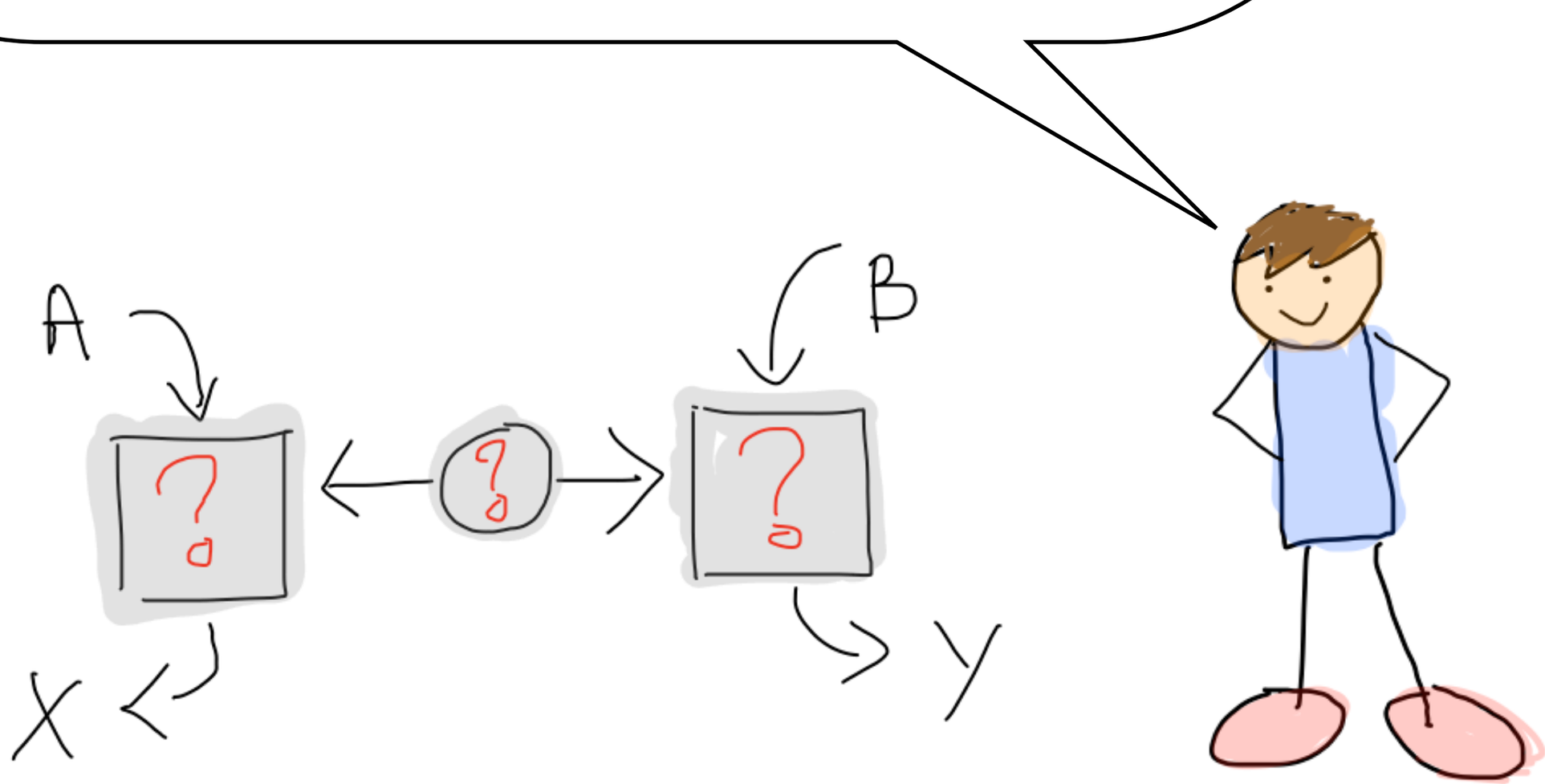
Where we know that there are certain correlations that cannot be explained by any classical strategies.




A
B
?
?
?
X
Y
Bell's theorem!!!
A
ρ
?
?
X

Accessible statistics in the Expt:

$$\{\Pr[X = x, Y = y | A = a, B = b]\}_{x,y,a,b}$$

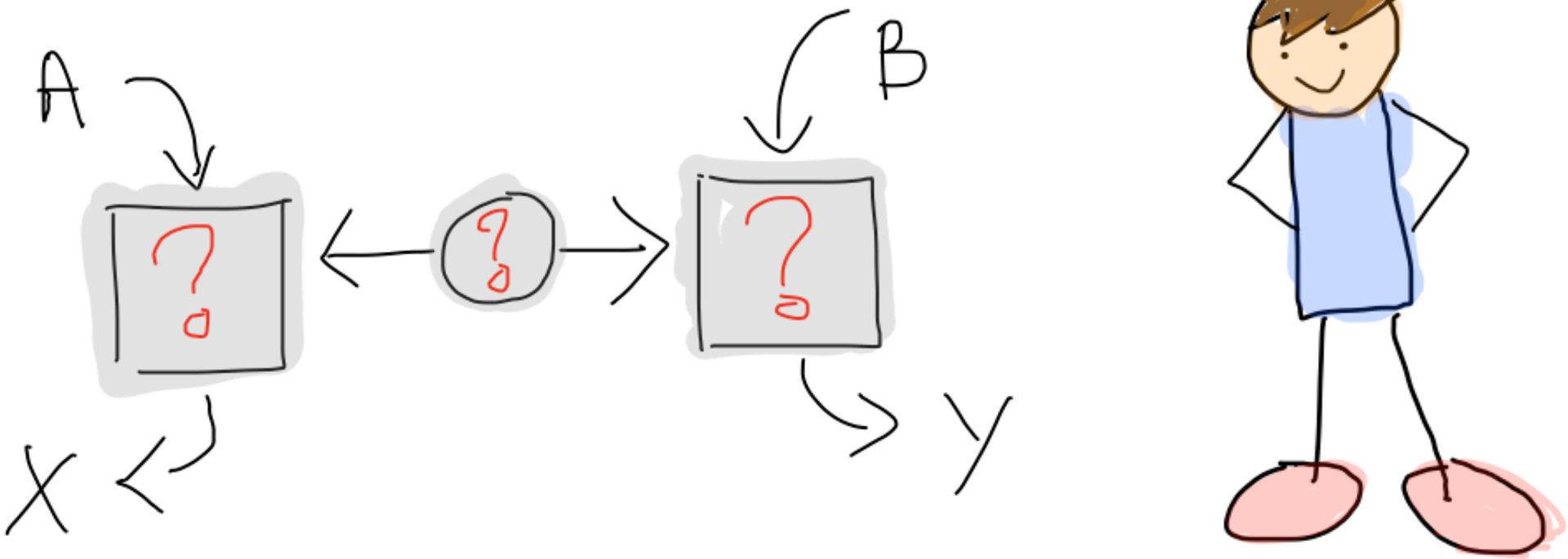


Accessible statistics in the Expt:

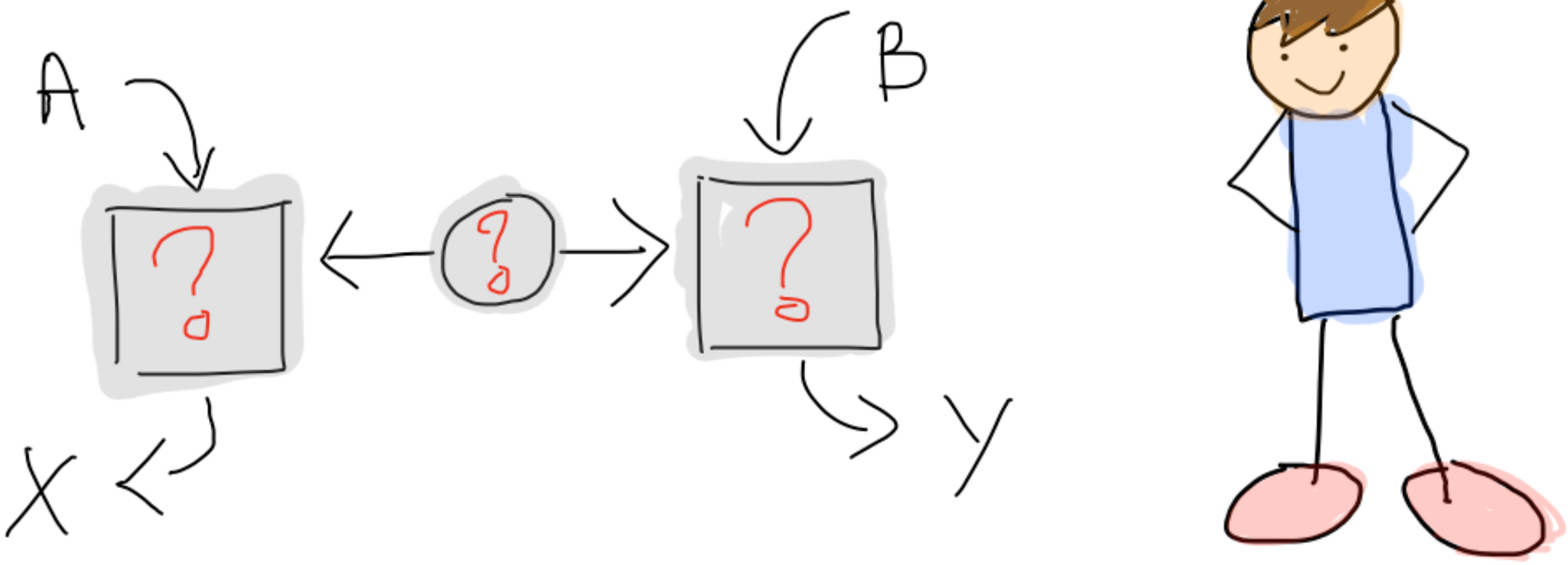
$$\{\Pr[X = x, Y = y | A = a, B = b]\}_{x,y,a,b}$$

Say, we consider the CHSH inequality

$$S = \sum_{x,y,a,b} (-1)^{a \wedge b \oplus x \oplus y} \Pr[x, y | a, b] \leq 2$$

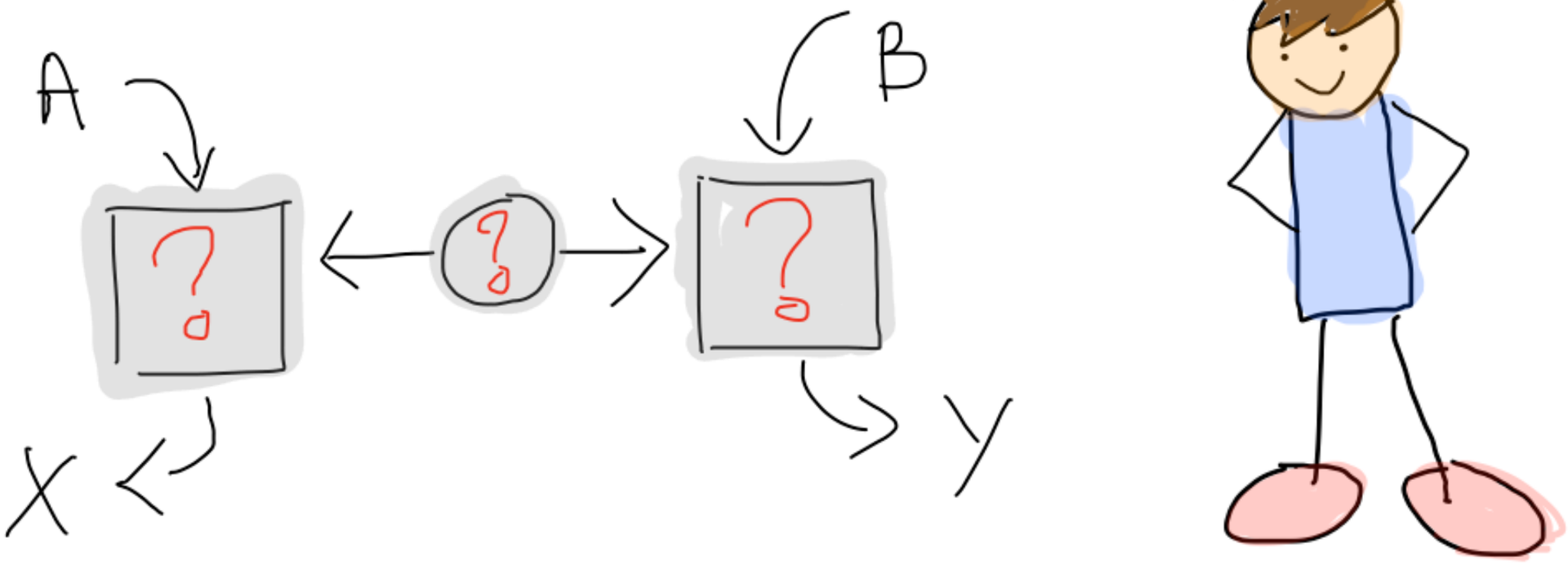


Observation 1.
The violation of the CHSH inequality depends on the bipartite state and the measurements.



Observation 1.
The violation of the CHSH inequality depends on the bipartite state and the measurements.

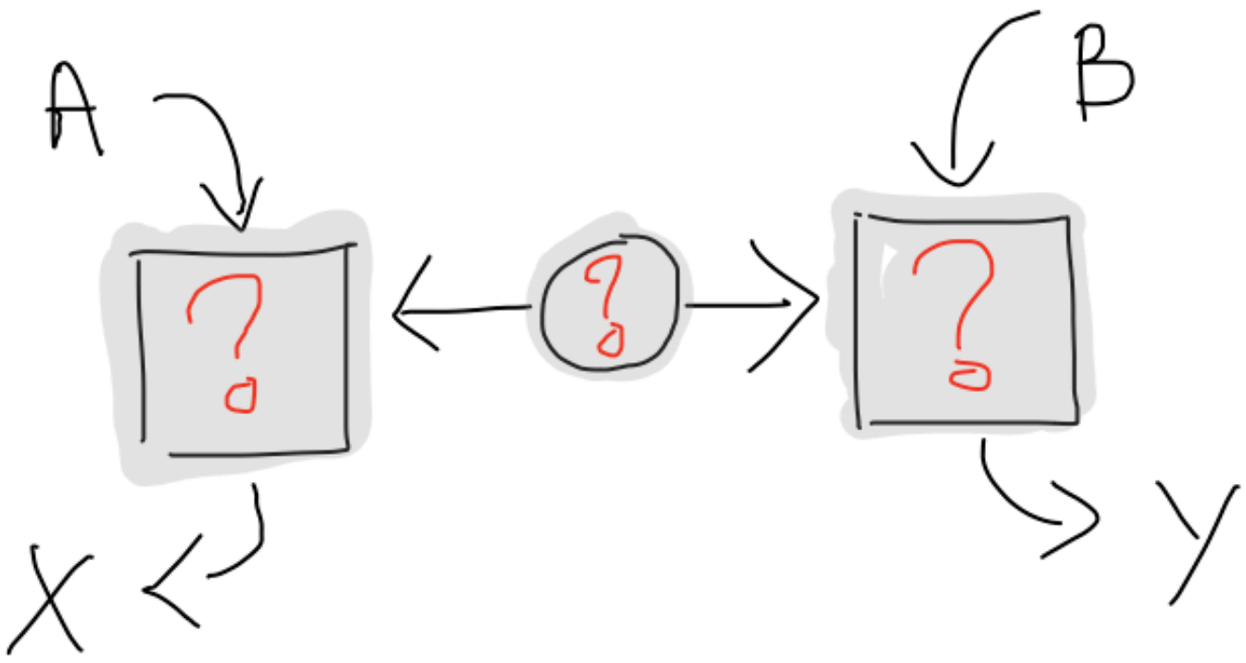
For an EPR state, the maximum CHSH violation is given by the following measurements:

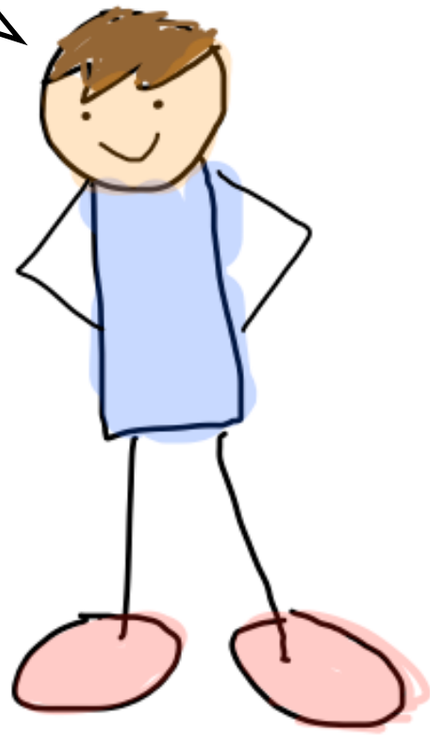


Observation 1.
The violation of the CHSH inequality depends on the bipartite state and the measurements.

For an EPR state, the maximum CHSH violation is given by the following measurements:

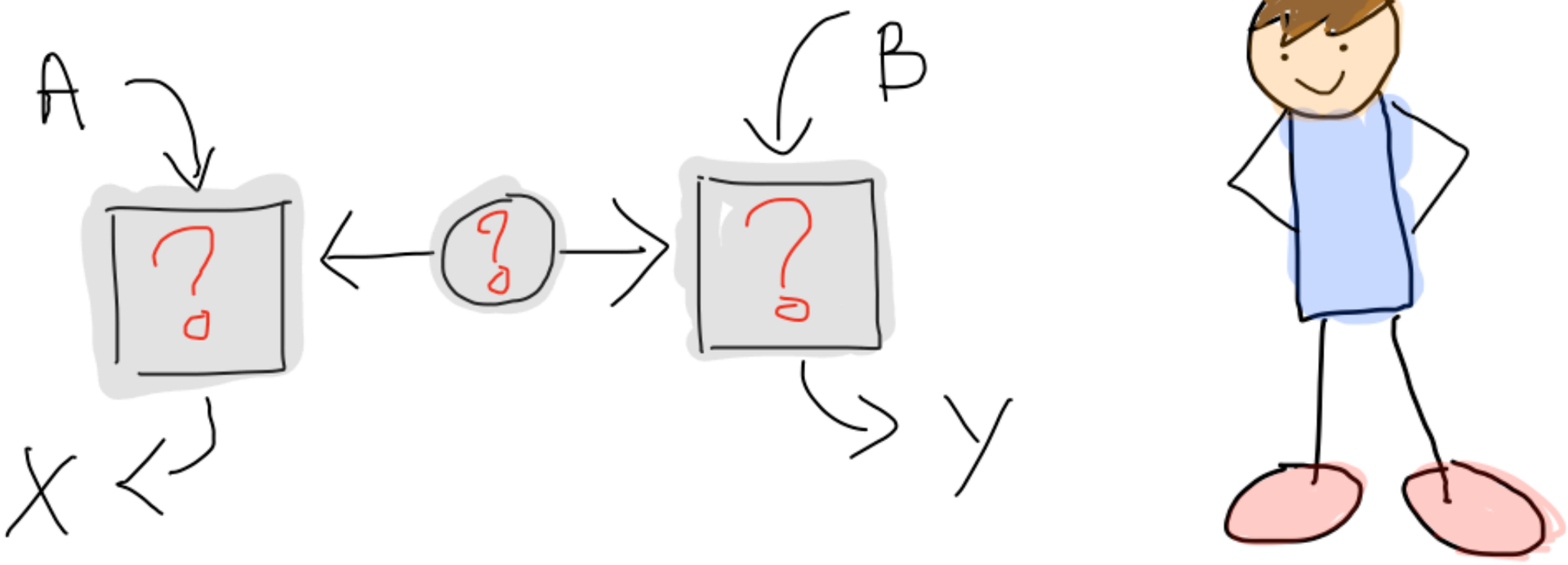
A: σ_X, σ_Z B: $\frac{\sigma_Z + \sigma_X}{\sqrt{2}}, \frac{\sigma_Z - \sigma_X}{\sqrt{2}}$





Observation 2.
All non-local correlations respect the "monogamy" law

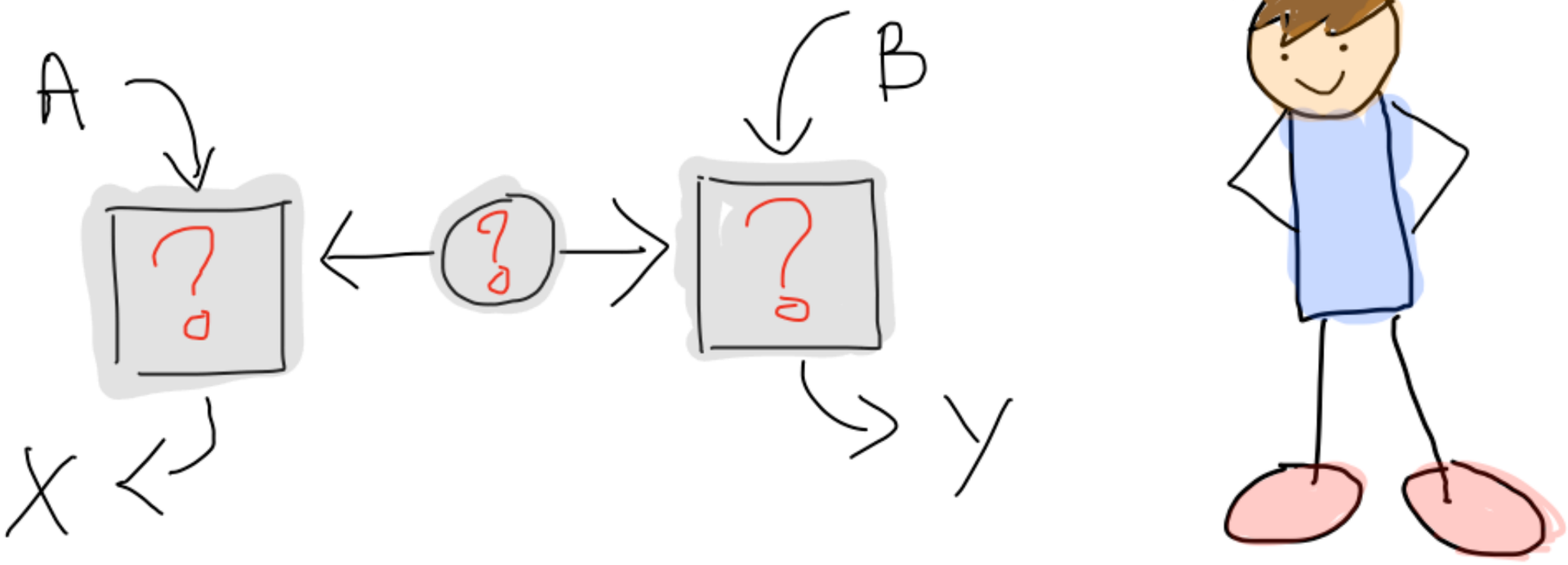
That is, if we observe the maximal CHSH value, then we can be sure that no one in the universe can be correlated to our observed statistics.



Lets gather what we know now:

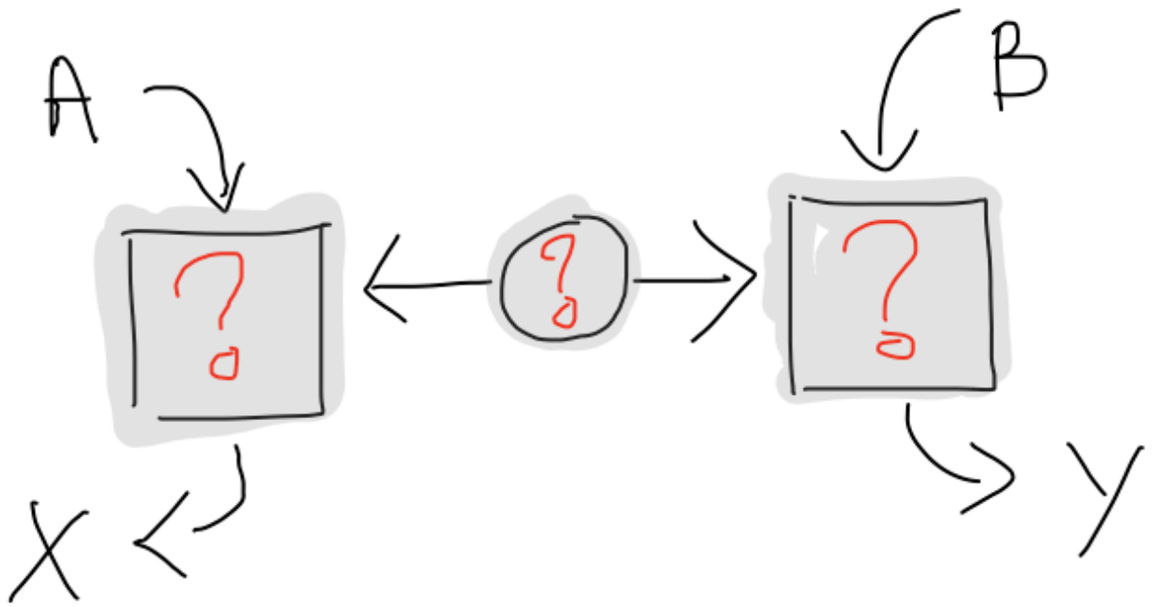
1. The CHSH test allows us to certify if the measurements are maximally non-commuting, which allows us to check if the setup is respecting the uncertainty principle.

2. Also, the correlations generated from the CHSH test respect the "monogamy" law.



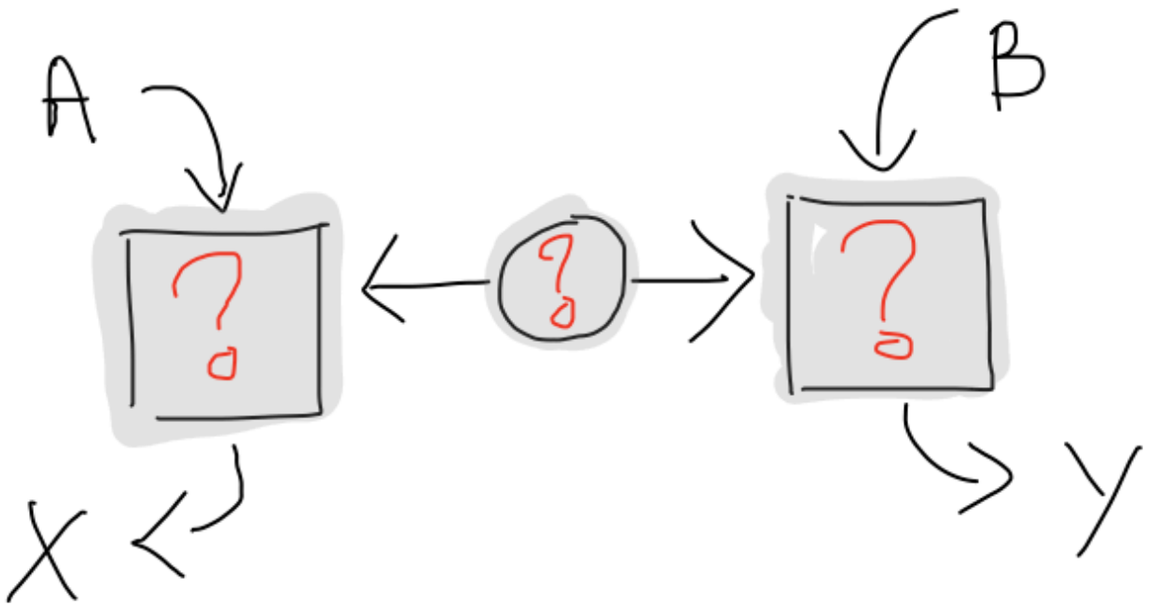
Uncertainty Principle

Entropic and device-independent Version



Uncertainty Principle

Entropic and device-independent Version



The Maassen-Uffink entropic uncertainty principle can be lower bounded as

$$H(X) + H(X') \geq 1 - \log_2 \left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

Uncertainty Principle

Entropic and device-independent Version

$$H(X) + H(X') \geq 1 - \log_2 \left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

A device-independent test of an entropic uncertainty principle

Uncertainty Principle

Entropic and device-independent Version

$$H(X) + H(X') \geq 1 - \log_2 \left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

A device-independent test of an entropic uncertainty principle

In the limiting case where the CHSH test generates the maximal violation,

$$H(X) + H(X') \geq 1$$

Uncertainty Relation

Entropic and device-independent Version

Most importantly, by using certain properties of conditional entropies, we obtain

$$H(X|E) + H(X'|B) \geq 1 - \log_2 \left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

which is an entropic inequality for tripartite scenarios.

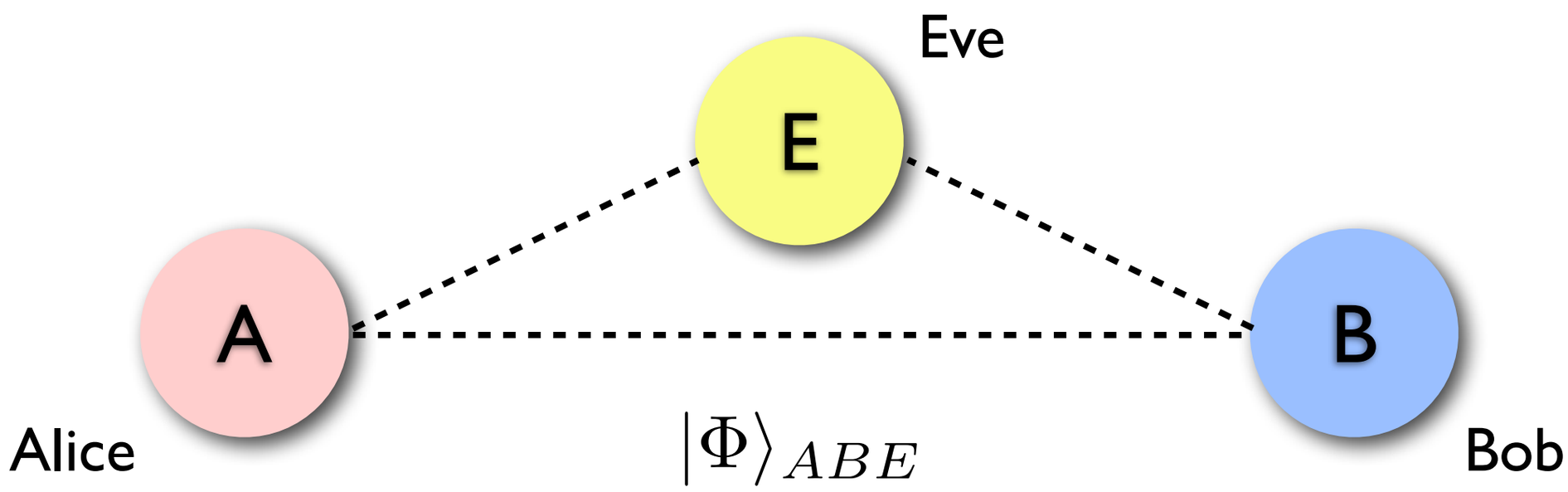
Uncertainty Relation

Entropic and device-independent Version

Most importantly, by using certain properties of conditional entropies, we obtain

$$H(X|E) + H(X'|B) \geq 1 - \log_2 \left(1 + \frac{S}{4}\sqrt{8 - S^2}\right)$$

which is an entropic inequality for tripartite scenarios.



Quantum Cryptography

Brief overview and Secret Key Length

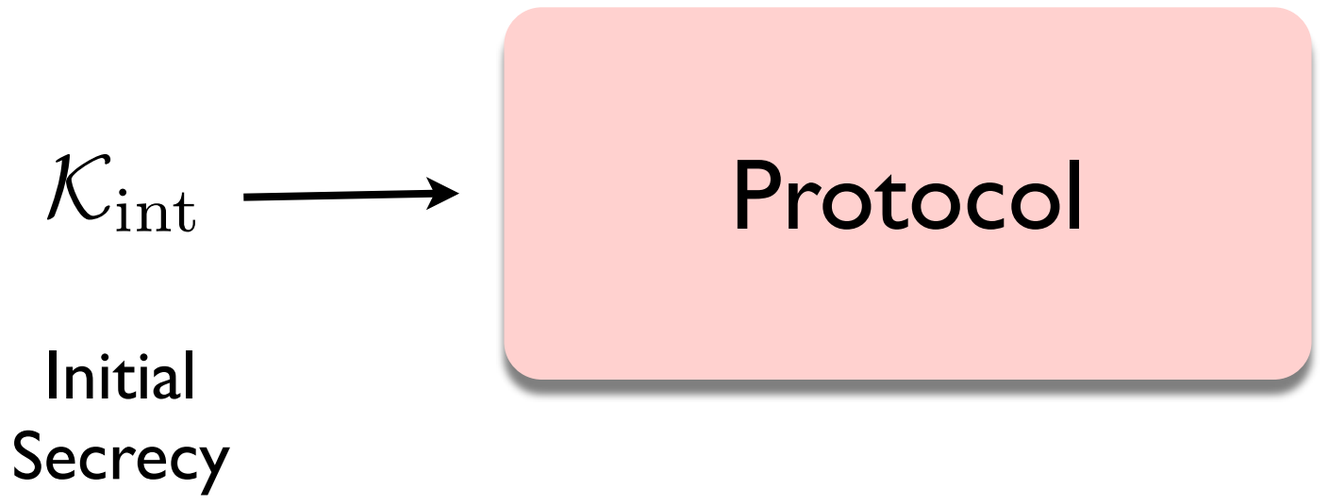
Quantum Cryptography

Brief overview and Secret Key Length

Protocol

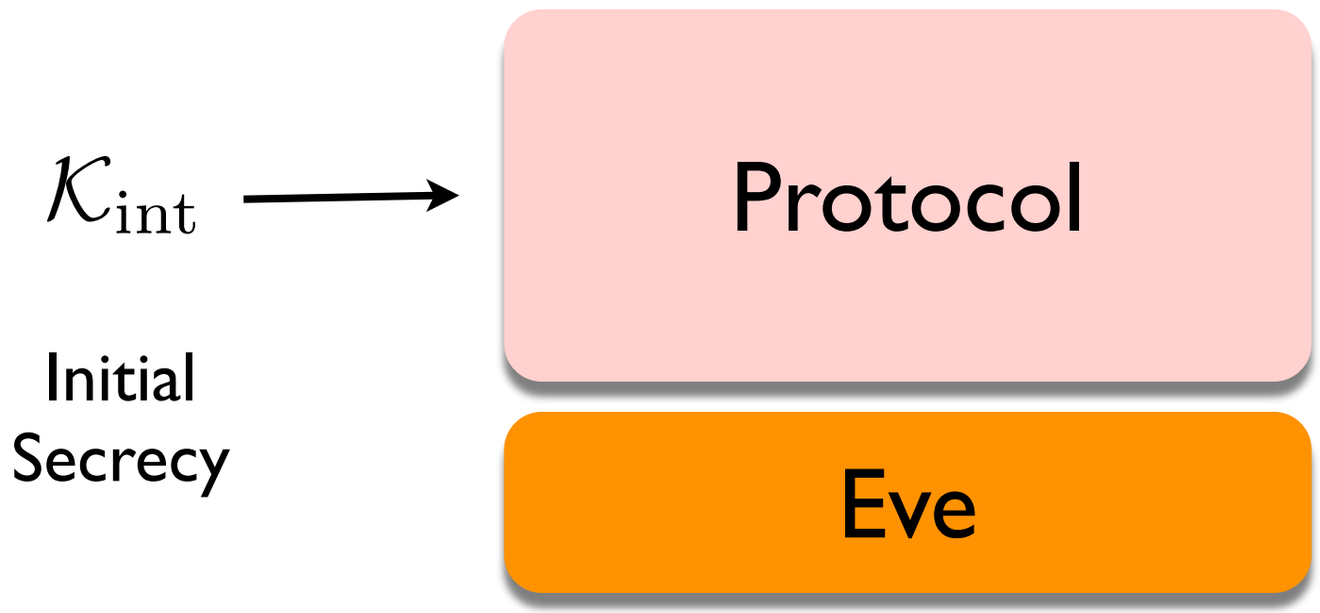
Quantum Cryptography

Brief overview and Secret Key Length



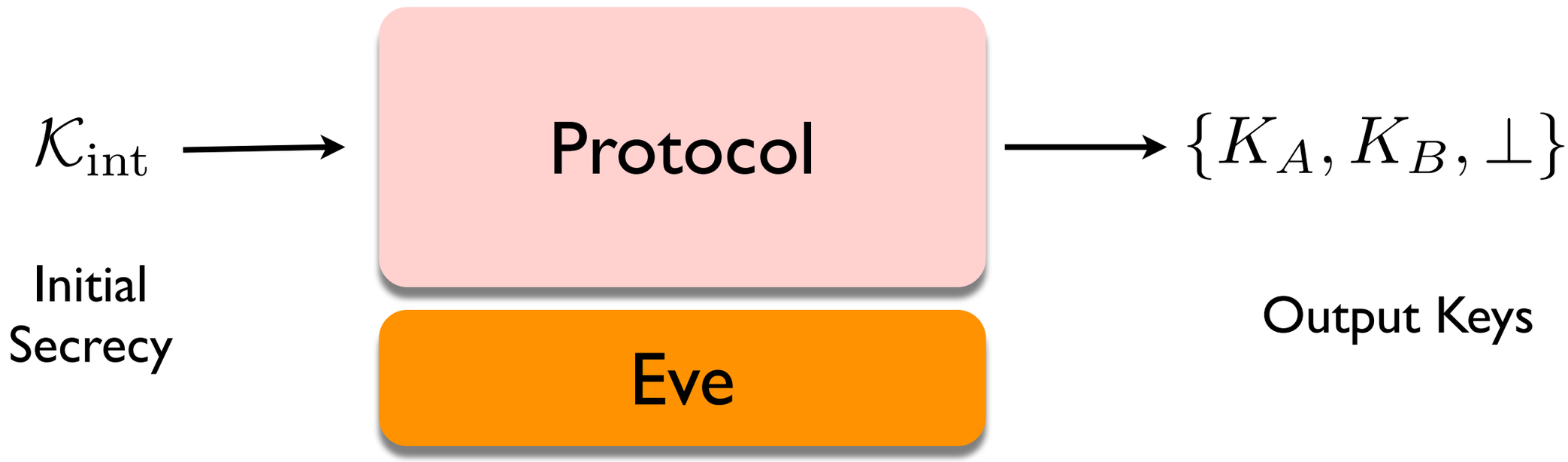
Quantum Cryptography

Brief overview and Secret Key Length



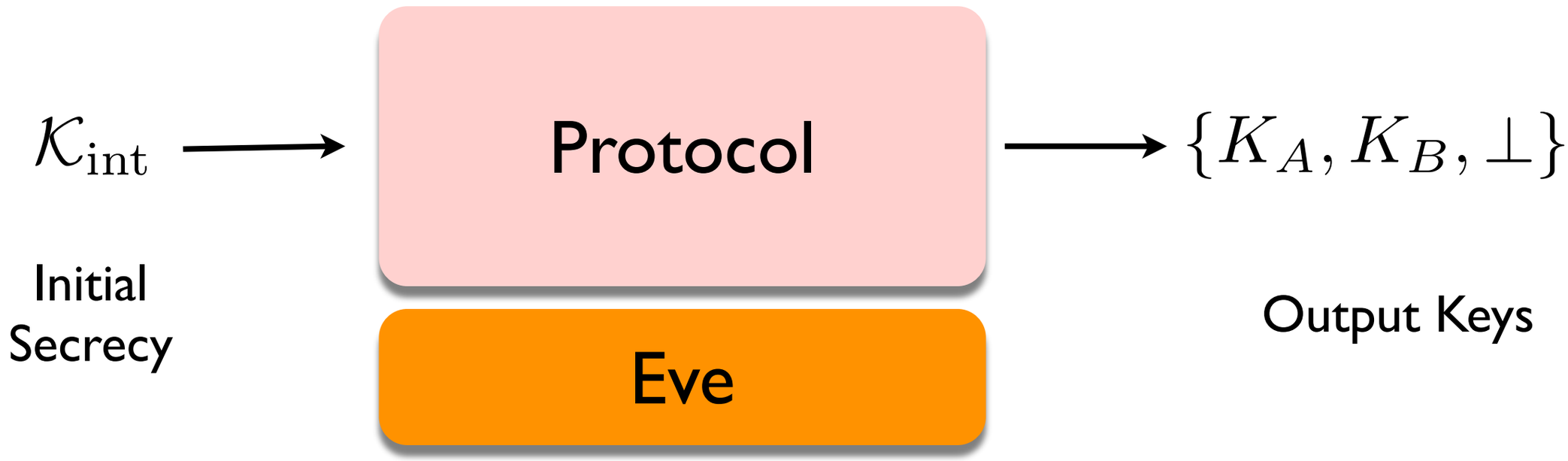
Quantum Cryptography

Brief overview and Secret Key Length



Quantum Cryptography

Brief overview and Secret Key Length



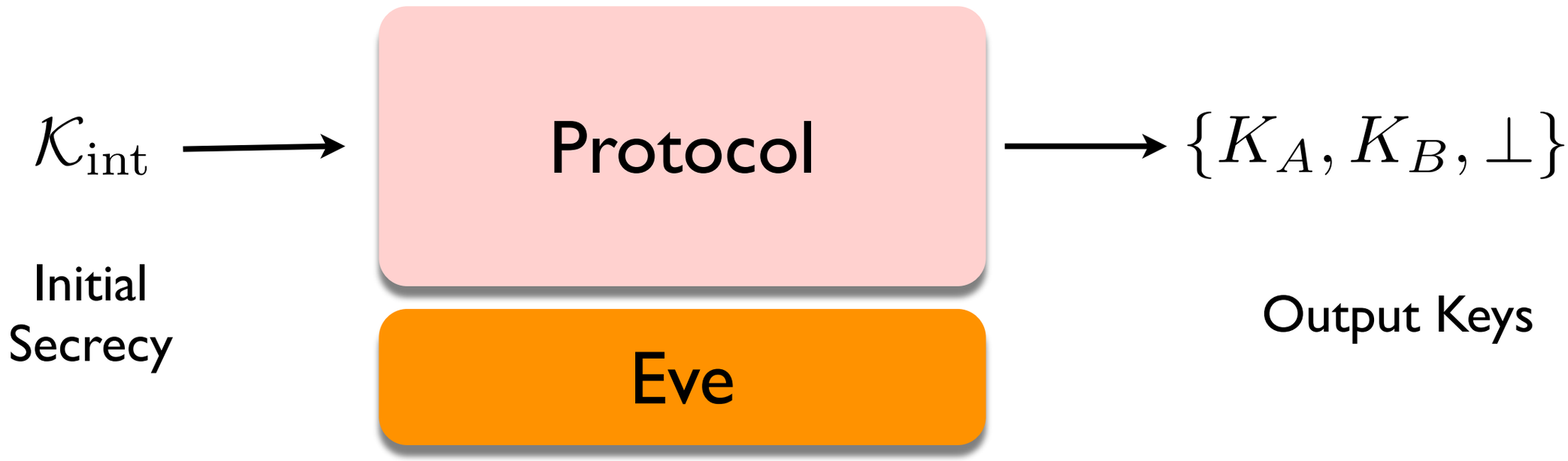
The length of the final secret key

$$|K_A| \approx H(X|E) - H(X|B)$$

Renes and Renner 2012

Quantum Cryptography

Brief overview and Secret Key Length



The length of the final secret key

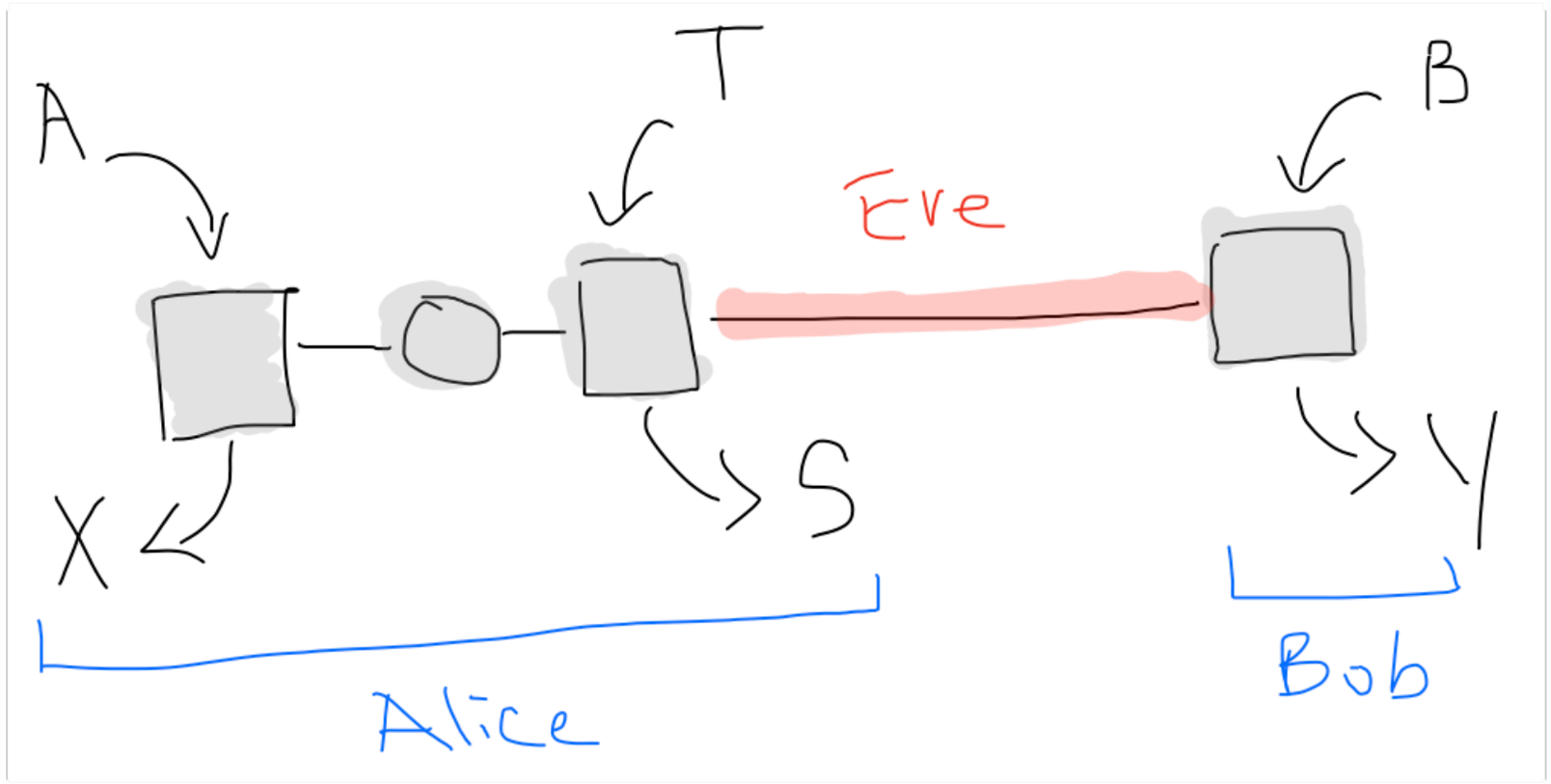
$$|K_A| \approx H(X|E) - H(X|B)$$

Renes and Renner 2012

In theory, establishing meaningful bounds on $H(X|E)$ is hard.

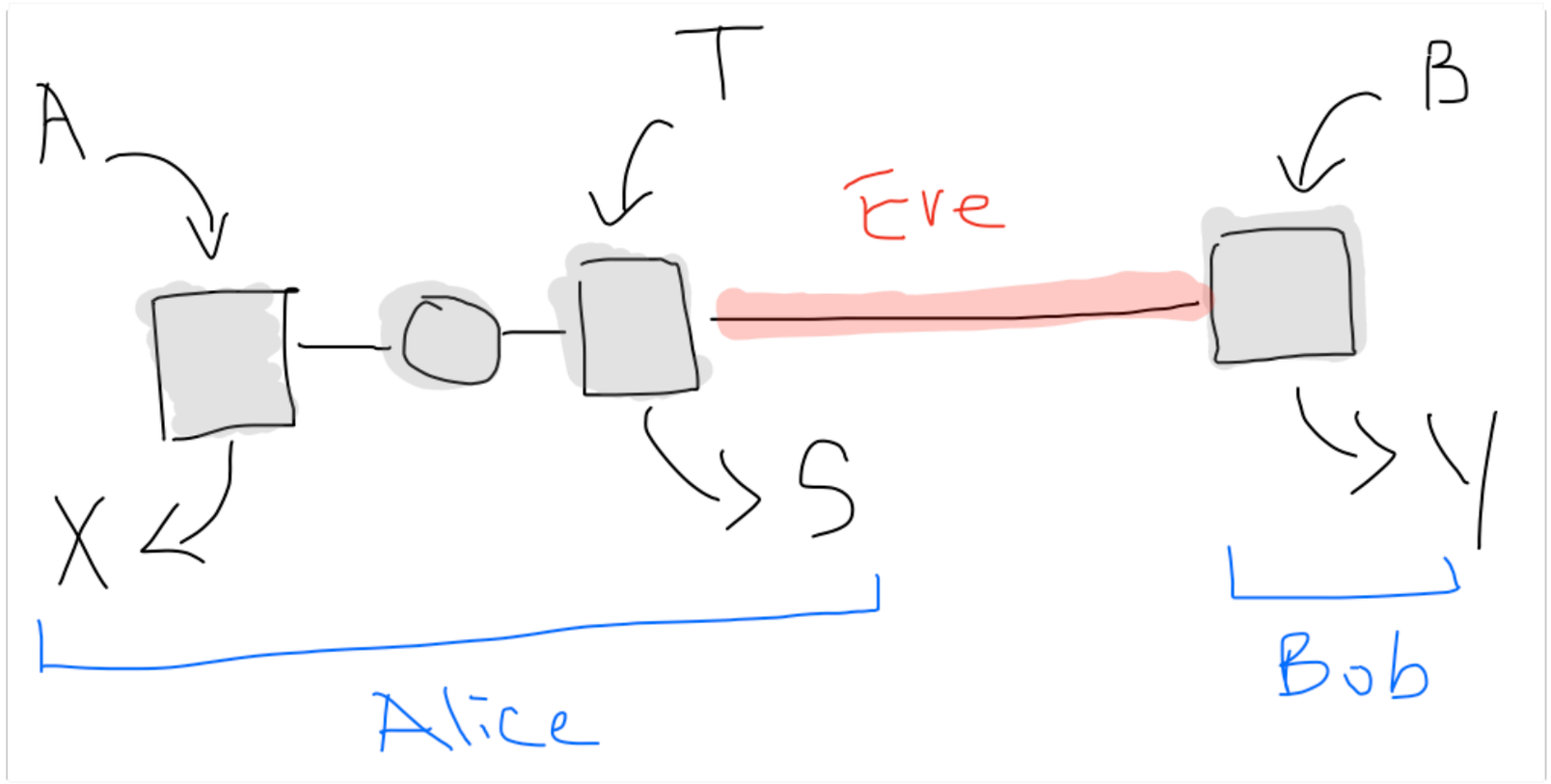
Protocol

A device-independent QKD scheme



Protocol

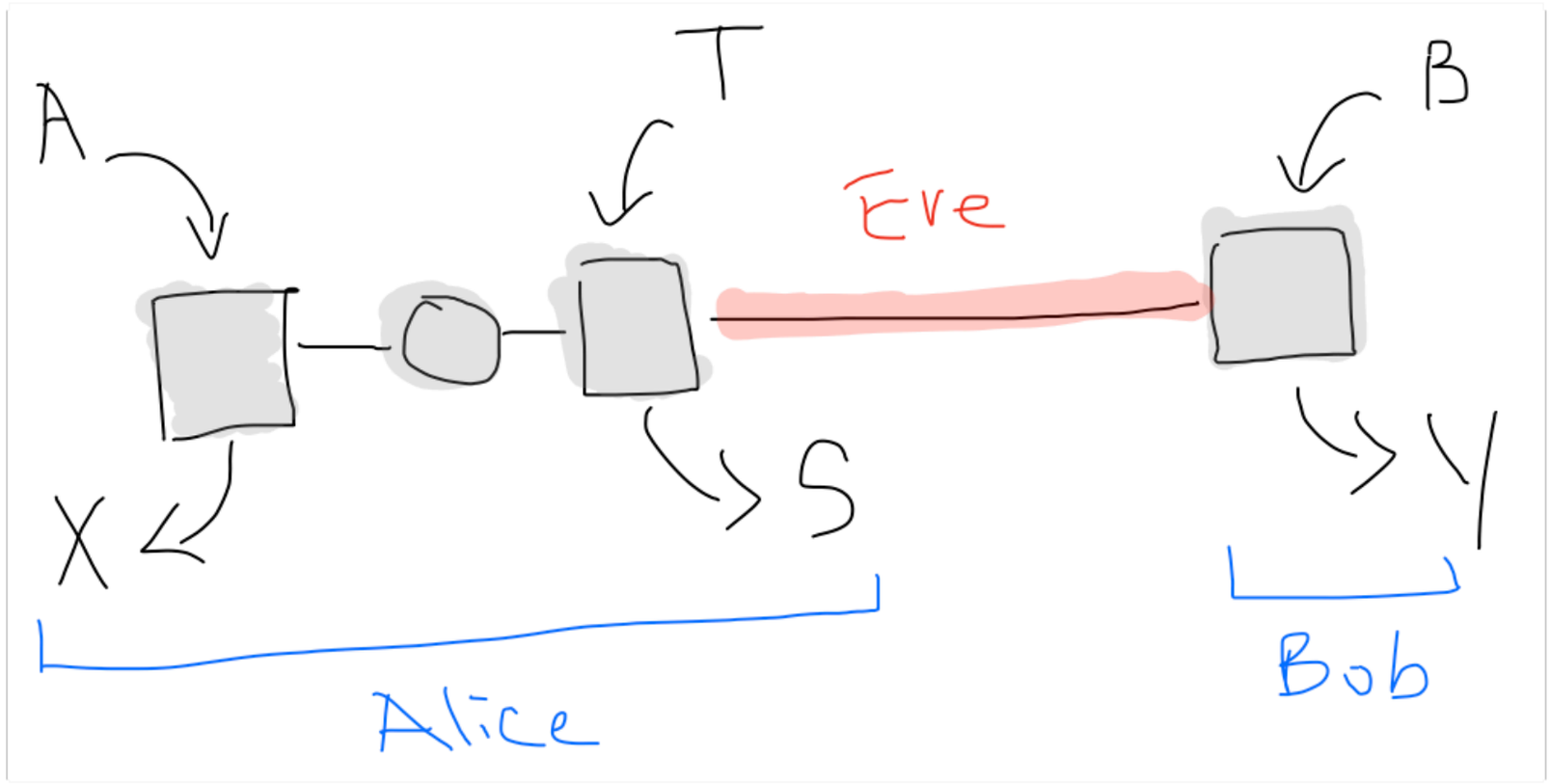
A device-independent QKD scheme



Security proof sketch.

Protocol

A device-independent QKD scheme

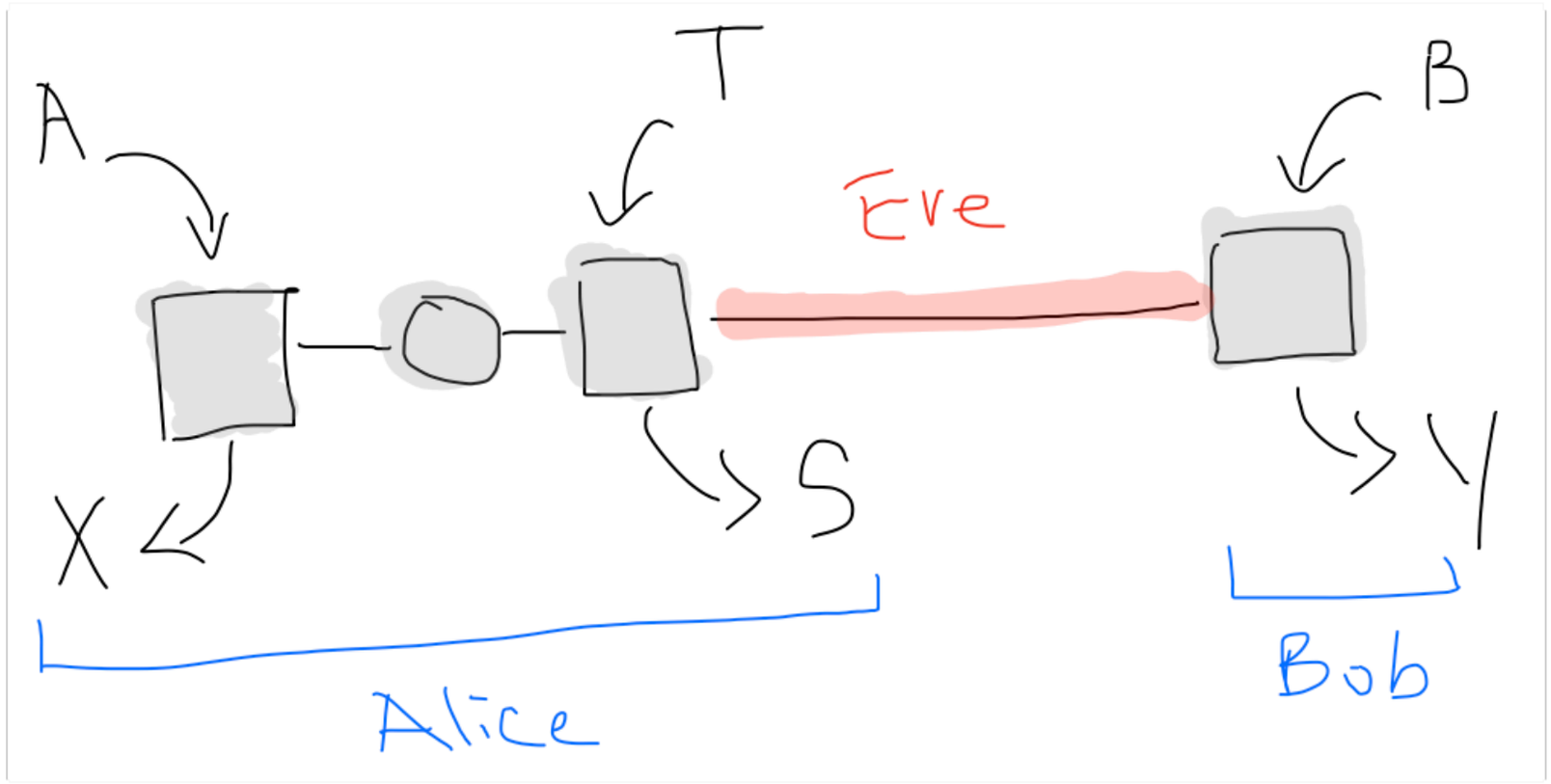


Security proof sketch.

$$|K_A| \approx H(X|E) - H(X|B)$$

Protocol

A device-independent QKD scheme



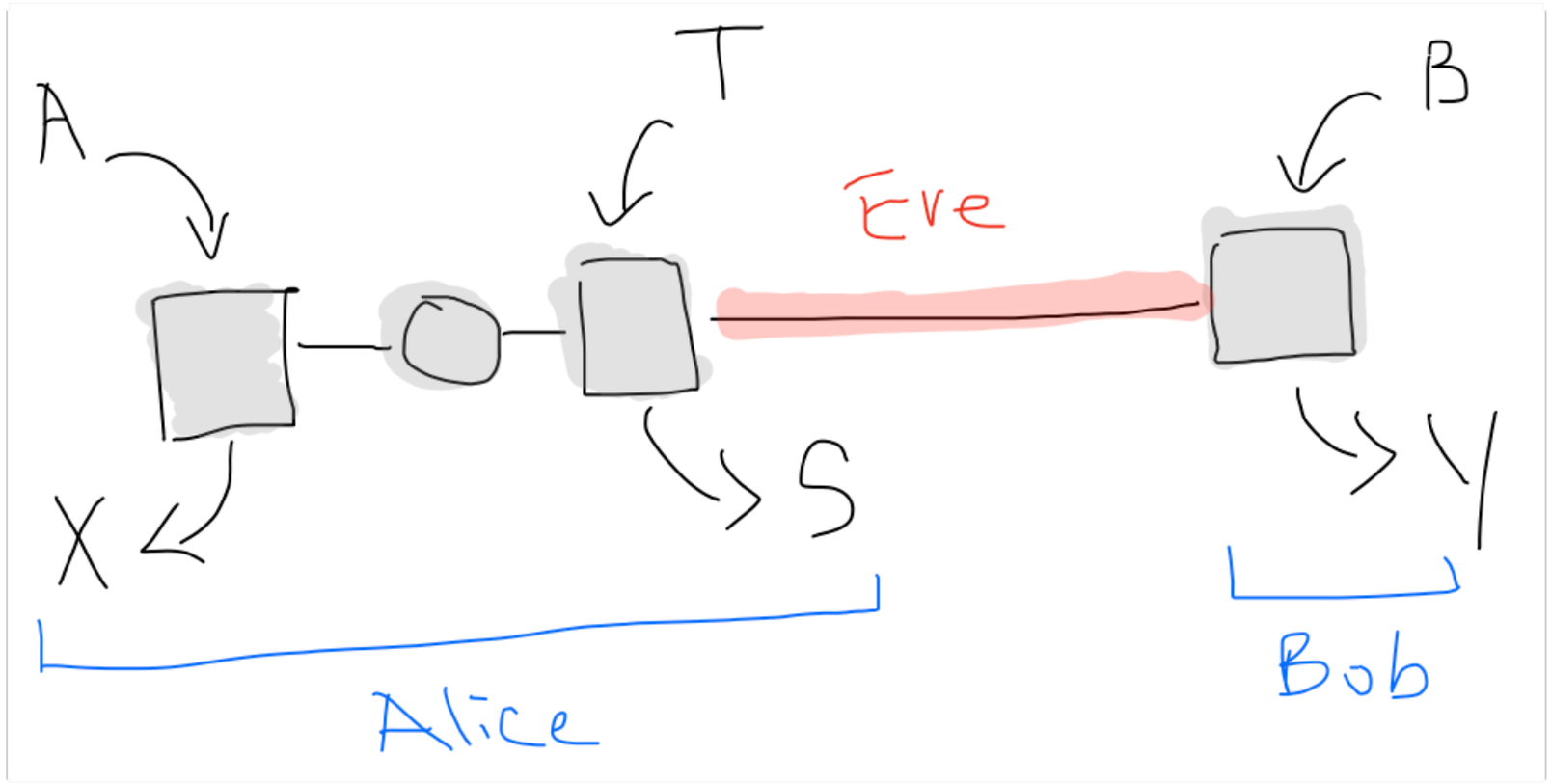
Security proof sketch.

$$|K_A| \approx H(X|E) - H(X|B)$$

$$\geq n - n\log_2\left(1 + \frac{S}{4}\sqrt{8 - S^2}\right) - H(X'|B) - H(X|B)$$

Protocol

A device-independent QKD scheme



Security proof sketch.

$$|K_A| \approx H(X|E) - H(X|B)$$

$$\geq n - n\log_2\left(1 + \frac{S}{4}\sqrt{8 - S^2}\right) - H(X'|B) - H(X|B)$$

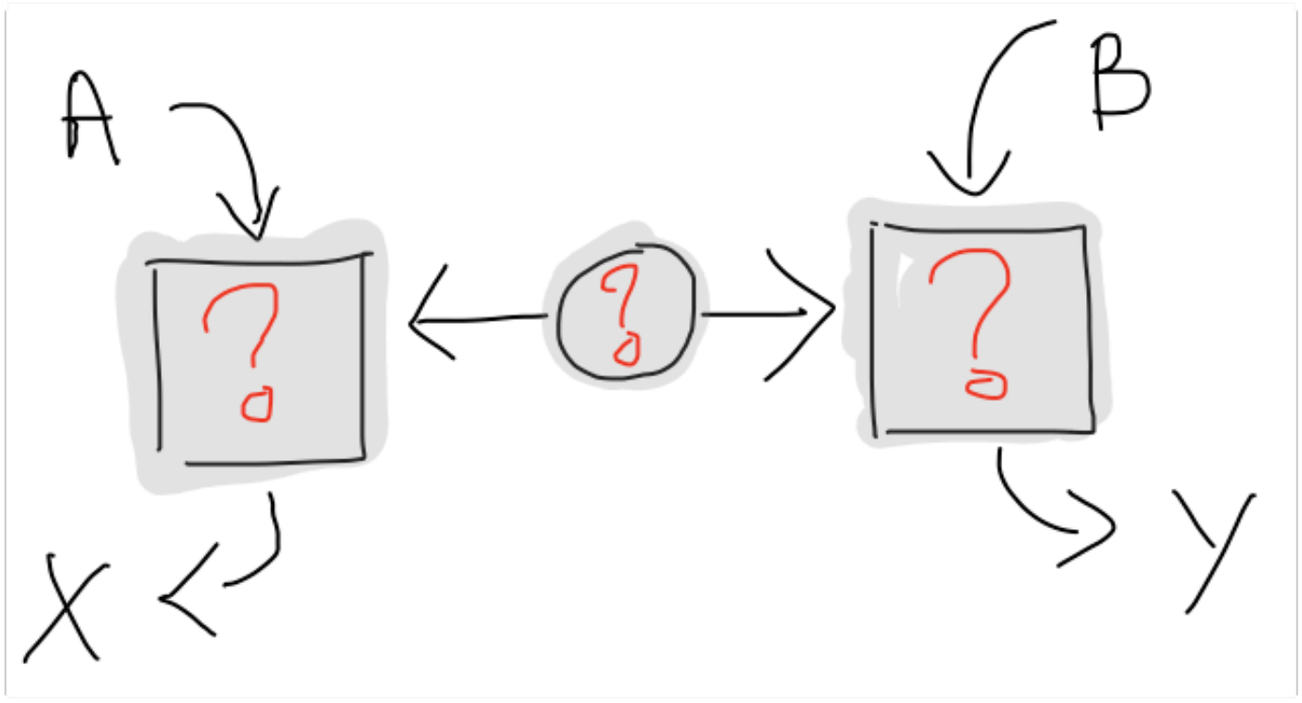
$$\geq n - n\log_2\left(1 + \frac{S}{4}\sqrt{8 - S^2}\right) - 2n\mathrm{h}_2(\delta)$$

Detection loophole

How to avoid the detection loophole

Detection loophole

How to avoid the detection loophole

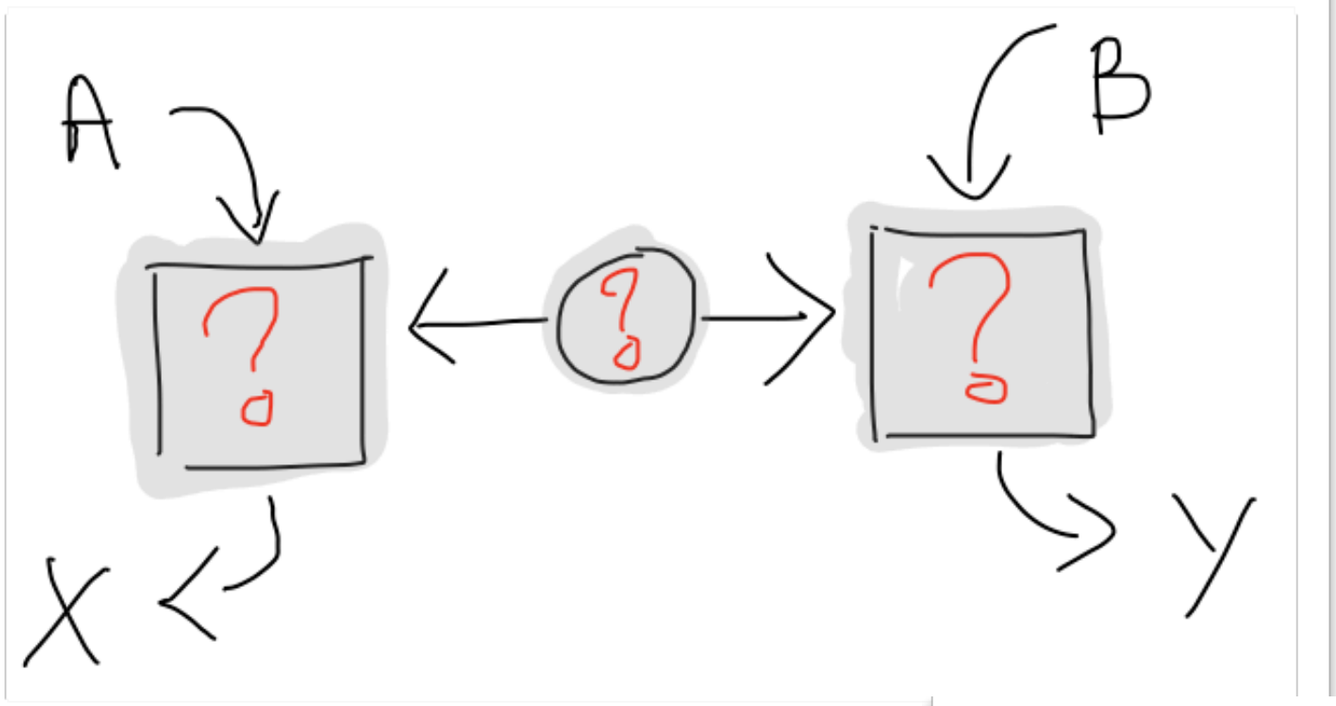


Device-Independent QKD

Pironio et al 2007,
Haenggi and Renner 2011,
Masanes, Pironio and Acin 2011,
Reichardt, Unger and Vazirani 2012,
Vazirani and Vidick 2012, etc

Detection loophole

How to avoid the detection loophole

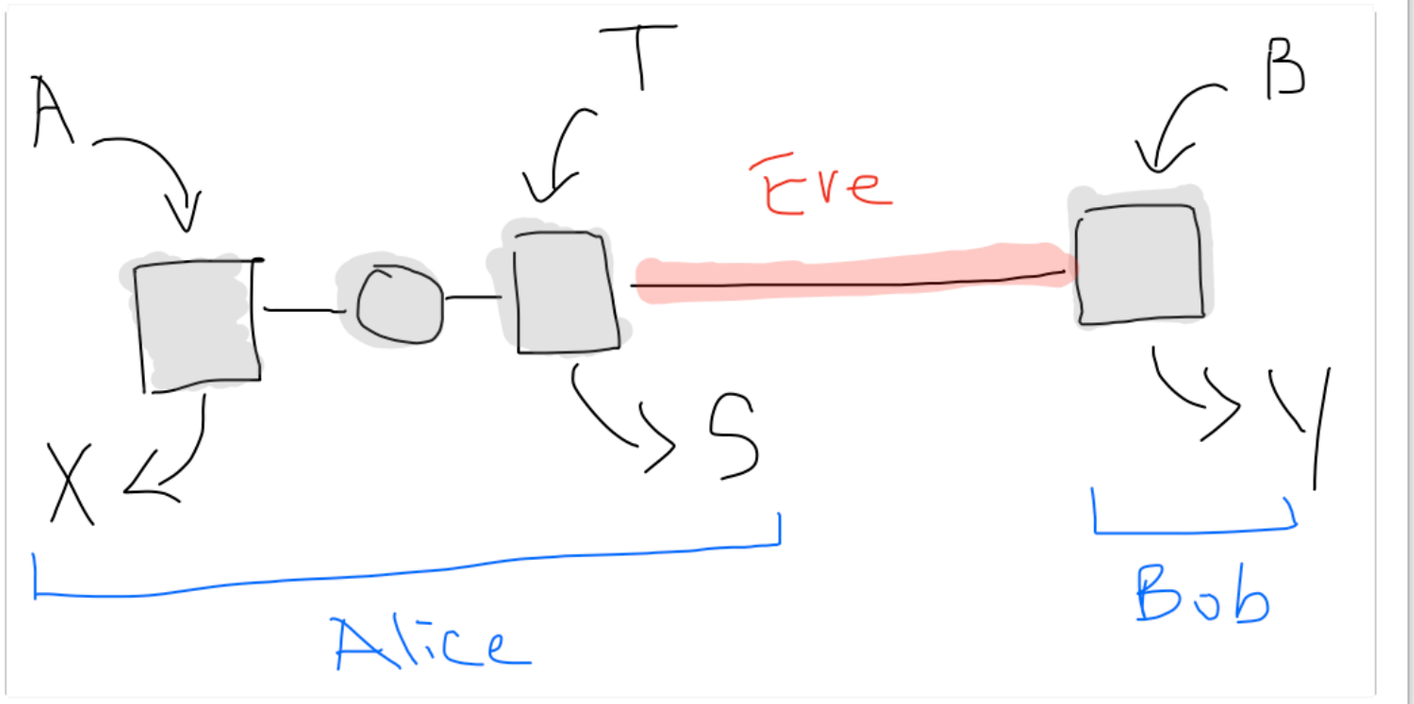


Device-Independent QKD

Pironio et al 2007,
Haenggi and Renner 2011,
Masanes, Pironio and Acin 2011,
Reichardt, Unger and Vazirani 2012,
Vazirani and Vidick 2012, etc

Device-Independent QKD with local Bell test

Lim, Portmann, Tomamichel, Renner and Gisin 2012.



(Practical) Main Messages

(Practical) Main Messages

1. A simple framework for cryptographic protocols with minimal assumptions.

(Practical) Main Messages

1. A simple framework for cryptographic protocols with minimal assumptions.

2. Bell's inequalities can be used to certify entropic uncertainty relations.

(Practical) Main Messages

1. A simple framework for cryptographic protocols with minimal assumptions.

2. Bell's inequalities can be used to certify entropic uncertainty relations.

Thank you

For more information, see

- Quantum Cryptography with Local Bell test, Lim et al, arXiv: 1208.0023 (2012)
- Tight Finite-Key Analysis for Quantum Cryptography, Tomamichel et al, Nature. Commun. **3** 634 (2012)
- Entropic uncertainty relations – A survey, Wehner and Winter, New. J. Phys. **12** 025009 (2010).
- The Uncertainty Principle in the Presence of Quantum Memory, Berta et al, Nature. Phys. **6** 659–662 (2010).