One-Sided Device Independence of BB84 Via Monogamy-of-Entanglement Game

Marco Tomamichel[1], Serge Fehr[2], Jędrzej Kaniewski[1], Stephanie Wehner[1]

[1]Centre for Quantum Technologies, National University of Singapore, Singapore

[2]Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands

Waterloo, August 7, 2013

Status of Device-Independent QKD

Status of Device-Independent QKD

Goal: Security from basic physical principles!

Status of Device-Independent QKD

Goal: Security from basic physical principles!

1. State Assumptions

(have they already been successfully attacked, e.g. fair sampling?)

2. Formalize Security ✓

(there is almost universal agreement on how to do this for QKD)

3. Prove security using the laws of quantum mechanics applied to the formalized protocol/assumptions (✓)

(many techniques are known, we add one more in this talk)

4. Is the protocol feasible?

(using current technology, does the protocol ever output something non-trivial?)

Status of Device-Independent QKD

Goal: Security from basic physical principles!

1. State Assumptions
(have they already been successfully attacked, e.g. fair sampling?)
2. Formalize Security ✓
(there is almost universal agreement on how to do this for QKD)
3. Prove security using the laws of quantum mechanics applied to the formalized protocol/assumptions (✓)
(many techniques are known, we add one more in this talk)
4. Is the protocol feasible?
(using current technology, does the protocol ever output something non-trivial?)

There does not currently exist a protocol/proof for which both 1. and 4. have a satisfactory answer.

Example: Errors vs. Fair Sampling

How do we deal with lost signals?

Example: Errors vs. Fair Sampling

How do we deal with lost signals?

Often, this issue is completely ignored — theorists presume the existence of a measurement result / experimentalists presume that the security proof survives if one just applies it to the measured signals.

Example: Errors vs. Fair Sampling

How do we deal with lost signals?

Often, this issue is completely ignored — theorists presume the existence of a measurement result / experimentalists presume that the security proof survives if one just applies it to the measured signals.

Solution	Assumption	Feasibility
Ignore them!	fair sampling	key is produced
Randomize!	none	too many errors

Problem is not solved yet!

Reichhardt et al., Vazirani/Vidick: Security without assumptions on devices is shown.

Problem is not solved yet!

Reichhardt et al., Vazirani/Vidick: Security without assumptions on devices is shown.

However, low key rate and error tolerance!

Losses not considered $\Rightarrow$ not feasible.

Problem is not solved yet!

Reichhardt et al., Vazirani/Vidick: Security without assumptions on devices is shown.

However, low key rate and error tolerance!

Losses not considered $\Rightarrow$ not feasible.

Interesting approaches:

- Restrict adversary, e.g. no long-term memory (Pironio et al.)
- Allow some device assumptions: measurement device independent QKD (Lo/Curty/Qi, Braunstein/Pirandola), **one-sided device independent QKD**

Problem is not solved yet!

Reichhardt et al., Vazirani/Vidick: Security without assumptions on devices is shown.

However, low key rate and error tolerance!

Losses not considered $\Rightarrow$ not feasible.

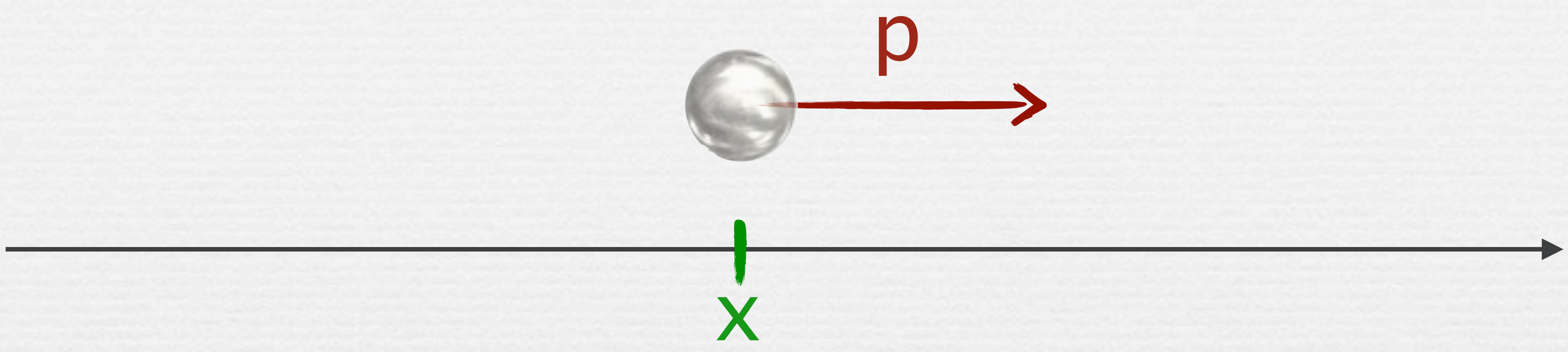
Interesting approaches:

- Restrict adversary, e.g. no long-term memory (Pironio et al.)
- Allow some device assumptions: measurement device independent QKD (Lo/Curty/Qi, Braunstein/Pirandola), **one-sided device independent QKD**

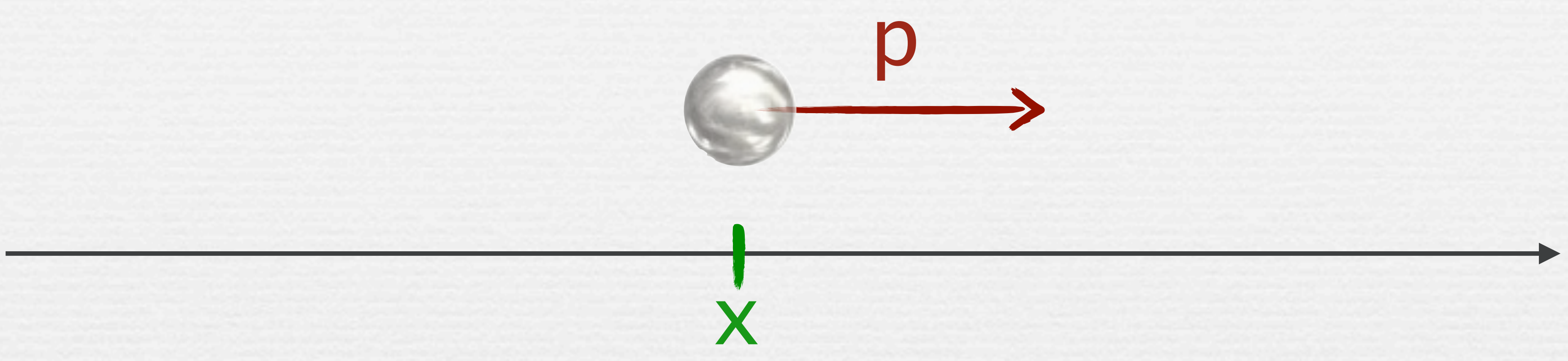
We show that BB84 is one-sided device independent

The Uncertainty Principle

The Uncertainty Principle



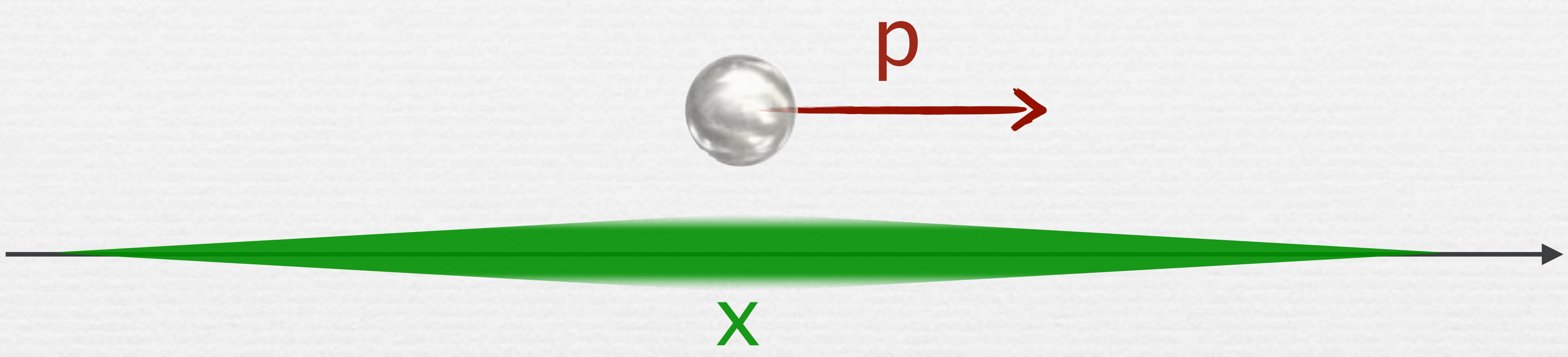
The Uncertainty Principle



Heisenberg

It is **impossible** that **both** the position x **and** the momentum p are fully determined.

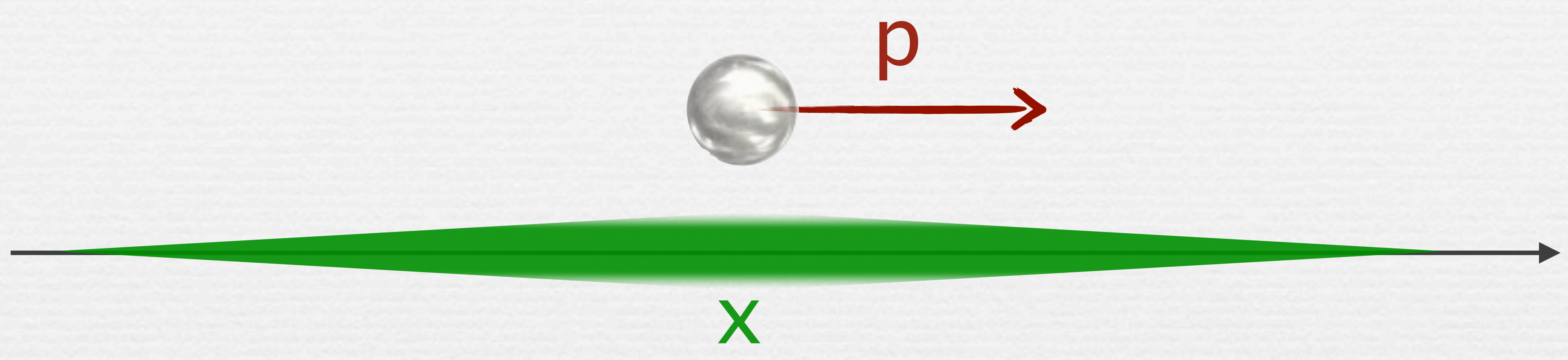
The Uncertainty Principle



Heisenberg

It is **impossible** that **both** the position x **and** the momentum p are fully determined.

The Uncertainty Principle



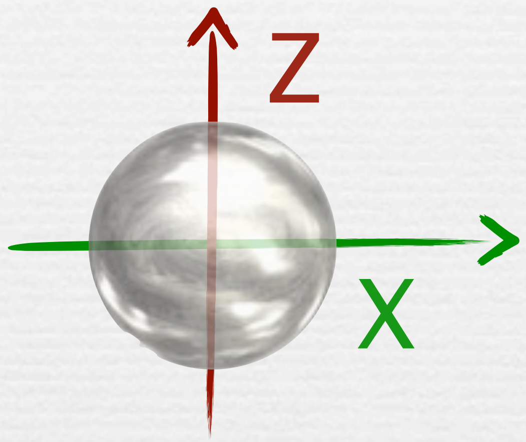
Heisenberg

It is **impossible** that **both** the position x **and** the momentum p are fully determined.

Many different formalizations of this statement have been proposed.

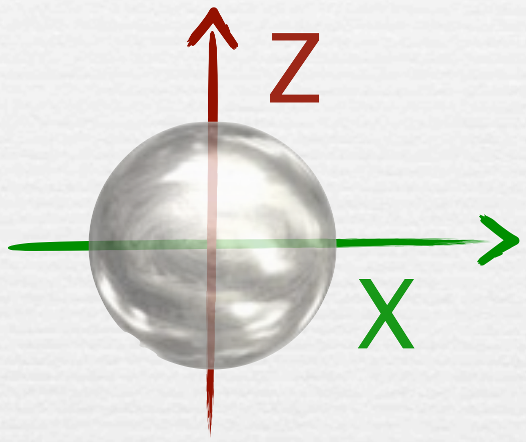
The Uncertainty Principle

Example: Polarization in X and Z direction



The Uncertainty Principle

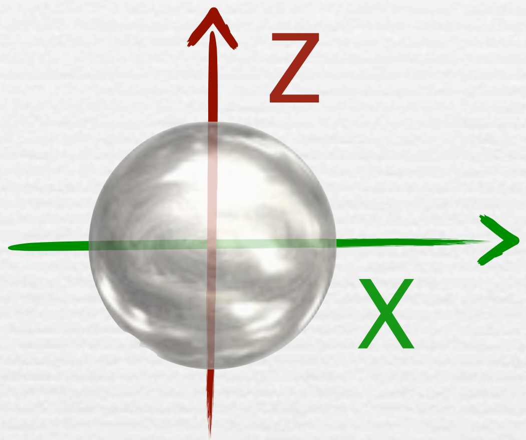
Example: Polarization in X and Z direction



It is **impossible to predict**, with high probability, the outcomes of polarization measurements in **both** directions.

The Uncertainty Principle

Example: Polarization in X and Z direction



It is **impossible to predict**, with high probability, the outcomes of polarization measurements in **both** directions.

More formally: $p_{\text{guess}}(X) + p_{\text{guess}}(Z) \leq 1 + \frac{1}{\sqrt{2}}$

Monogamy of Entanglement

Monogamy of Entanglement

- The more A is entangled with B, the less it can be with C .
- And vice versa.

Monogamy of Entanglement

- The more A is entangled with B, the less it can be with C .
- And vice versa.

- As given above: is a qualitative statement.
- Exist different quantitative statements.
- Part of our contribution:
  - new way to get a quantitative statement
  - with applications to quantum crypto

A Monogamy (of Entanglement) Game

ALICE
(Game Master)

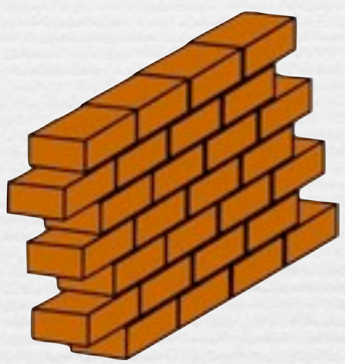
BOB

CHARLIE

A Monogamy (of Entanglement) Game

ALICE
(Game Master)

BOB

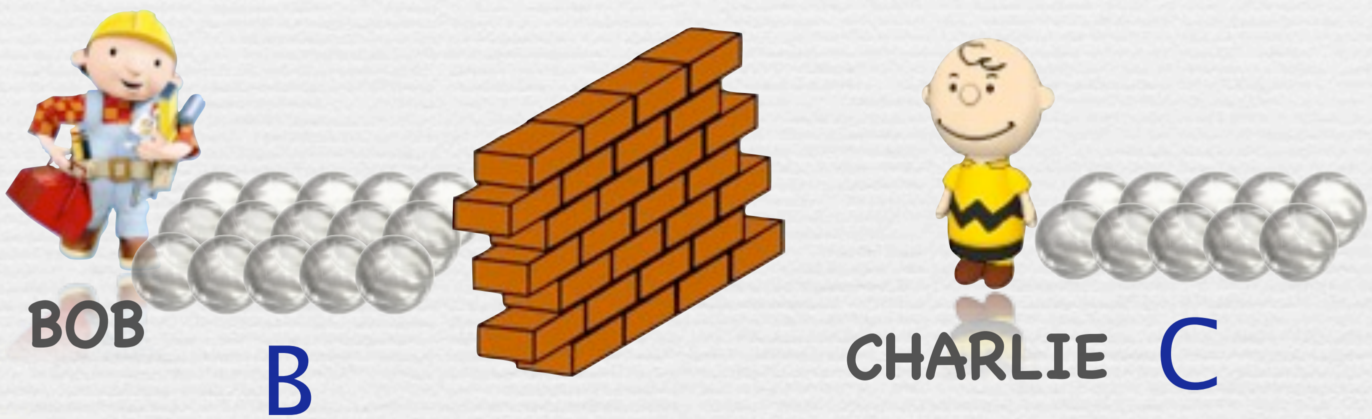


CHARLIE

A Monogamy (of Entanglement) Game

Set up:

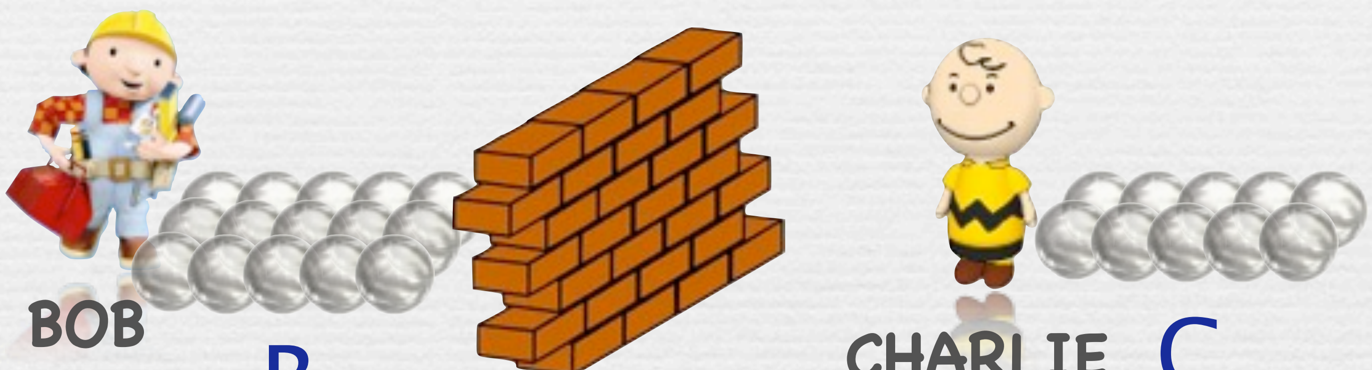
- $A = A_1 \ldots A_n$: n qubits
- B & C : arbitrary many qubits
- joint state of ABC : arbitrary



A Monogamy (of Entanglement) Game

Set up:

- $A = A_1 \ldots A_n$: n qubits
- B & C : arbitrary many qubits
- joint state of ABC : arbitrary



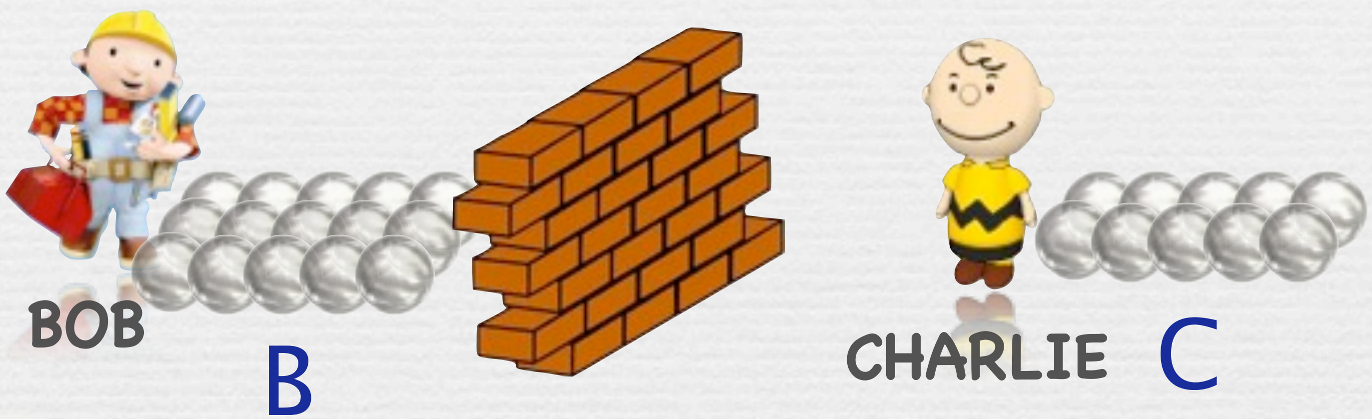
ALICE:

- chooses random $q = (q_1, \ldots, q_n) \in \{+, \times\}^n$,
- measures $A_1 \ldots A_n$ in respective bases $q_1, \ldots, q_n$ -> $x \in \{0,1\}^n$,
- sends q to BOB and CHARLIE

A Monogamy (of Entanglement) Game

Set up:

- $A = A_1 \ldots A_n$: n qubits
- B & C : arbitrary many qubits
- joint state of ABC : arbitrary



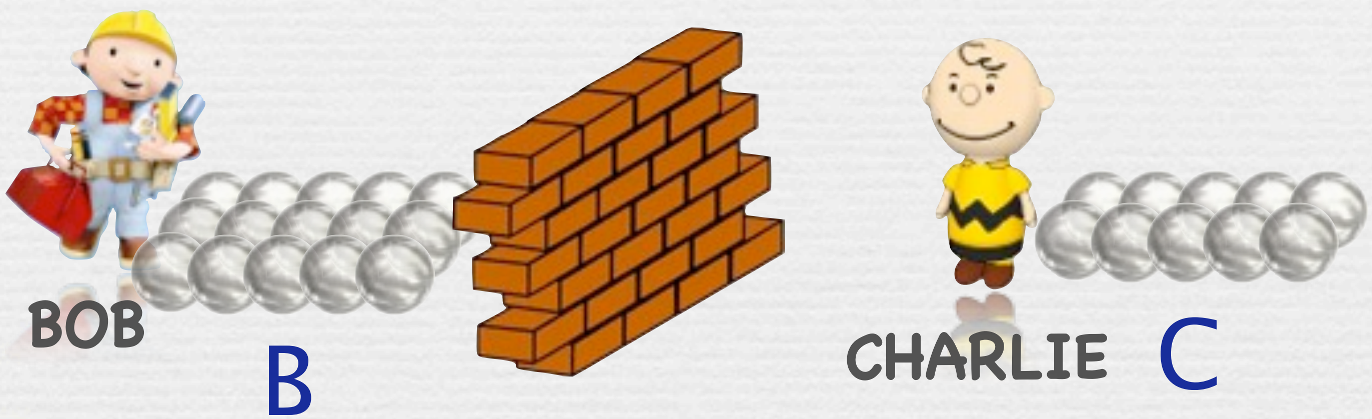
ALICE:

- chooses random $q = (q_1, \ldots, q_n) \in \{+, \times\}^n$,
- measures $A_1 \ldots A_n$ in respective bases $q_1, \ldots, q_n$ -> $x \in \{0,1\}^n$,
- sends q to BOB and CHARLIE

A Monogamy (of Entanglement) Game

Set up:

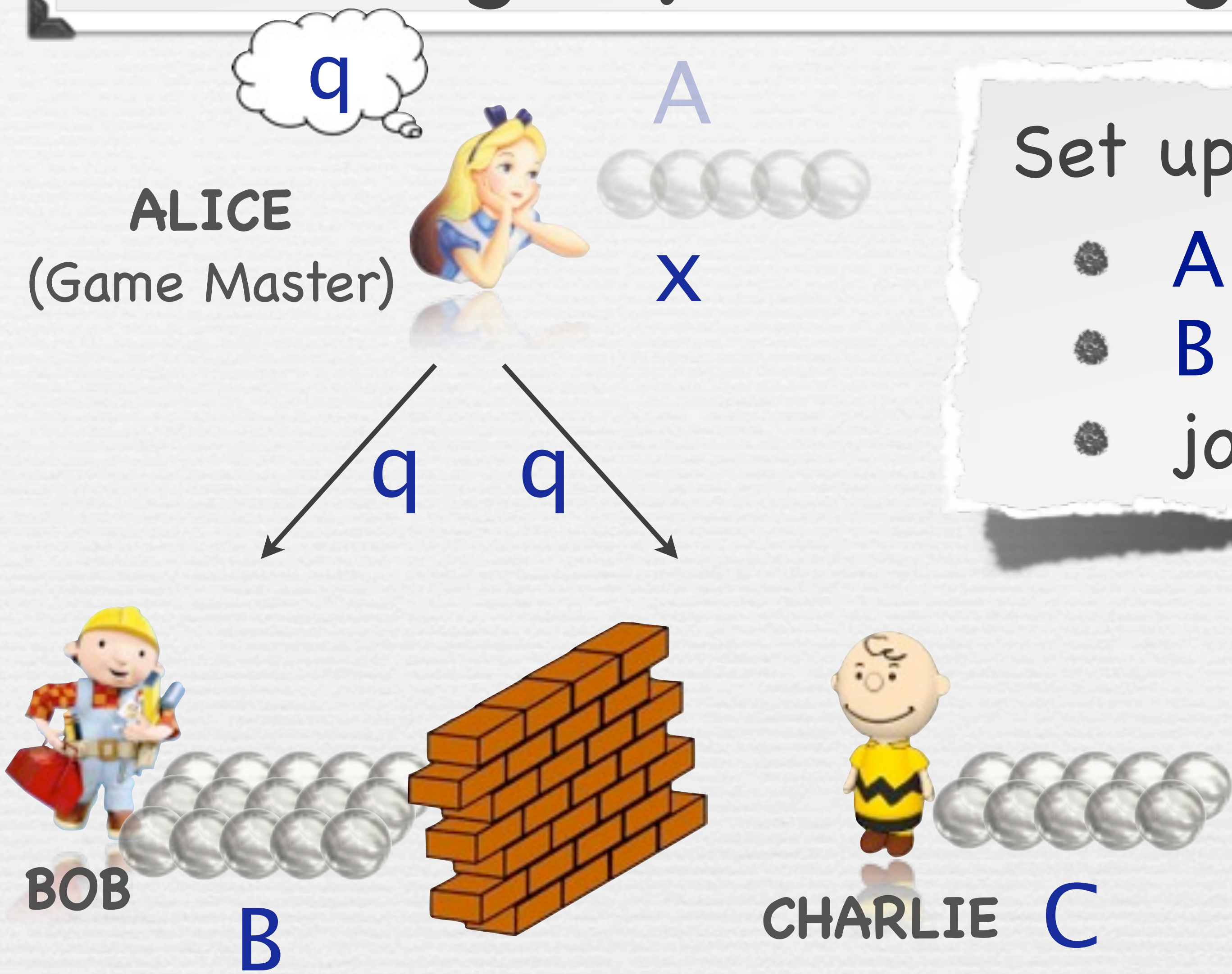
- $A = A_1 \ldots A_n$: n qubits
- B & C : arbitrary many qubits
- joint state of ABC : arbitrary



ALICE:

- chooses random $q = (q_1, \ldots, q_n) \in \{+, \times\}^n$,
- measures $A_1 \ldots A_n$ in respective bases $q_1, \ldots, q_n \rightarrow x \in \{0,1\}^n$,
- sends q to BOB and CHARLIE

A Monogamy (of Entanglement) Game



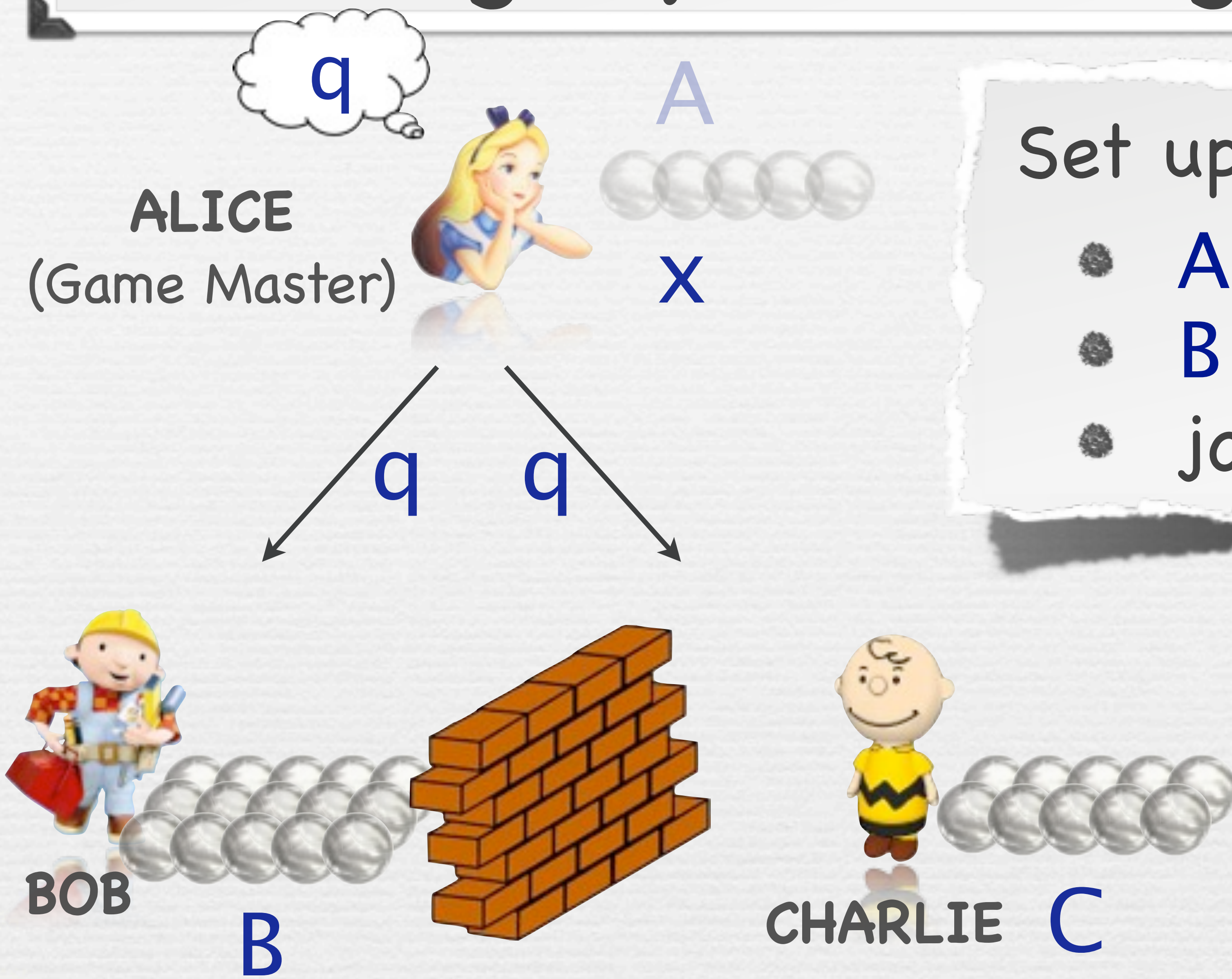
Set up:

- $A = A_1 \ldots A_n$: n qubits
- B & C : arbitrary many qubits
- joint state of ABC : arbitrary

ALICE:

- chooses random $q = (q_1,\ldots,q_n) \in \{+,\times\}^n$,
- measures $A_1 \ldots A_n$ in respective bases $q_1,\ldots,q_n$ -> $x \in \{0,1\}^n$,
- sends q to BOB and CHARLIE

A Monogamy (of Entanglement) Game



Set up:

- $A = A_1 \ldots A_n$: n qubits
- B & C : arbitrary many qubits
- joint state of ABC : arbitrary

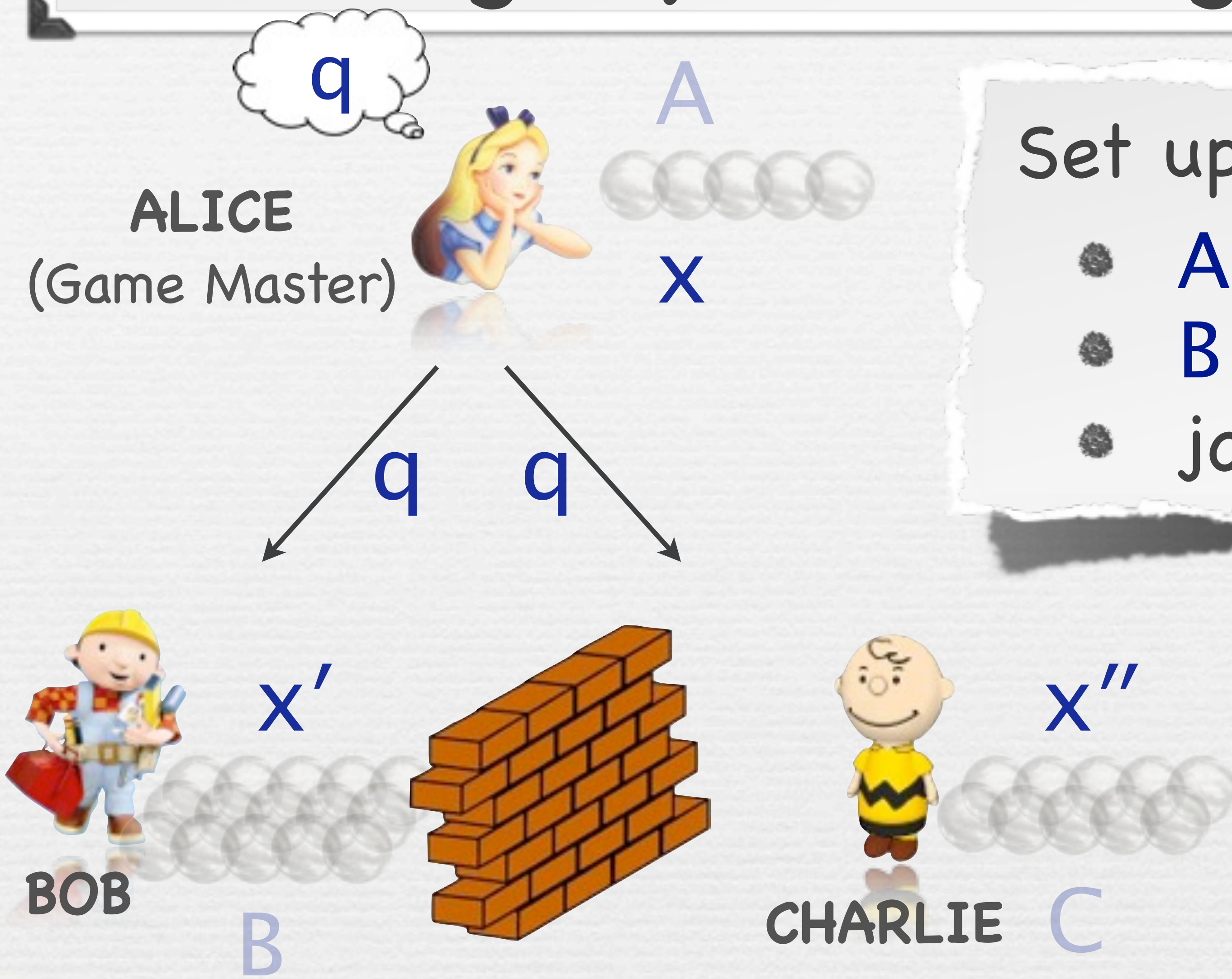
BOB and CHARLIE:

- guess x

ALICE:

- chooses random $q = (q_1,\ldots,q_n) \in \{+,\times\}^n$,
- measures $A_1 \ldots A_n$ in respective bases $q_1,\ldots,q_n$ -> $x \in \{0,1\}^n$,
- sends q to BOB and CHARLIE

A Monogamy (of Entanglement) Game



Set up:

- $A = A_1 \ldots A_n$: n qubits
- B & C : arbitrary many qubits
- joint state of ABC : arbitrary

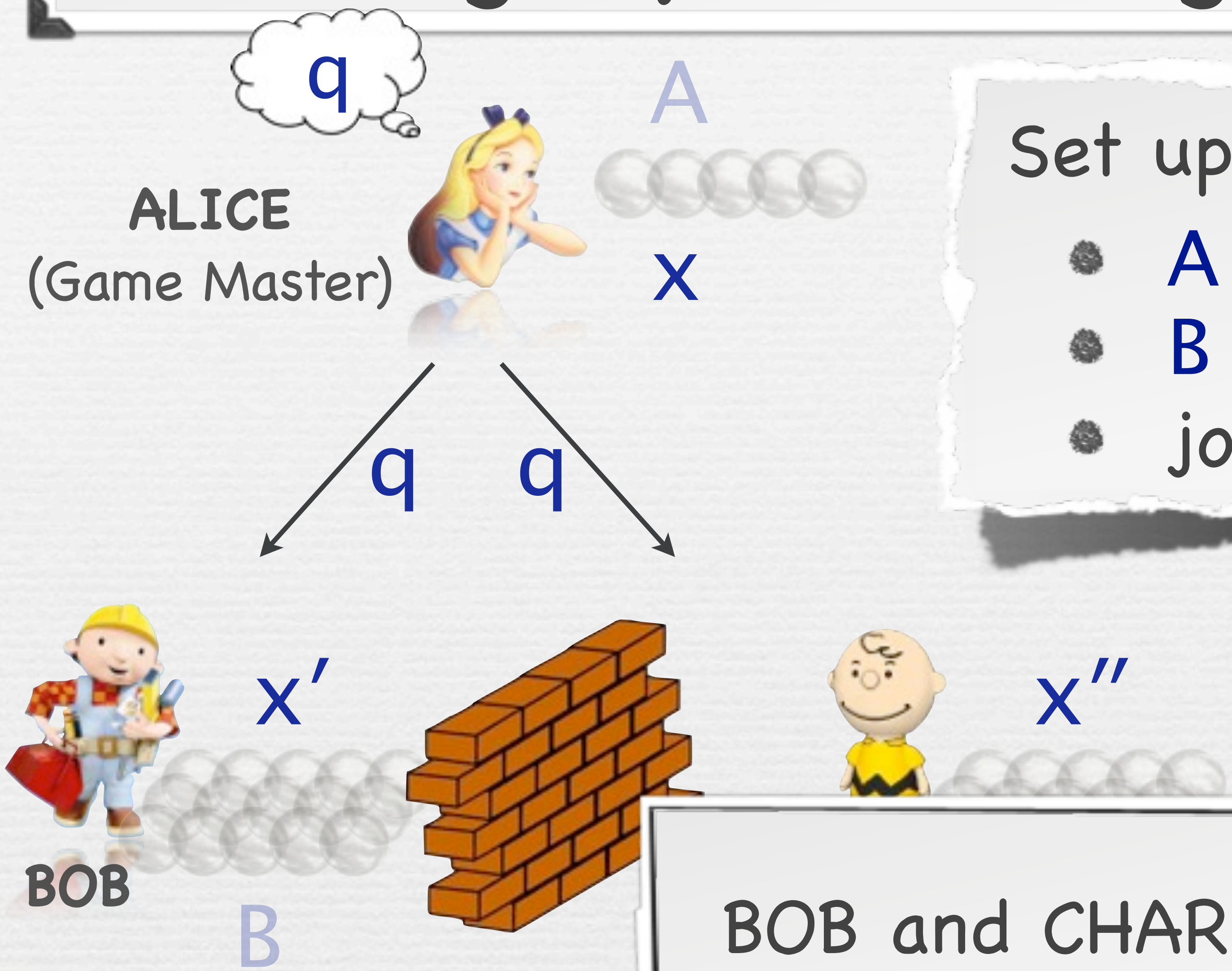
BOB and CHARLIE:

- guess x

ALICE:

- chooses random $q = (q_1, \ldots, q_n) \in \{+, \times\}^n$,
- measures $A_1 \ldots A_n$ in respective bases $q_1, \ldots, q_n$ -> $x \in \{0,1\}^n$,
- sends q to BOB and CHARLIE

A Monogamy (of Entanglement) Game



Set up:

- $A = A_1 \ldots A_n$: n qubits
- B & C : arbitrary many qubits
- joint state of ABC : arbitrary

BOB and CHARLIE:

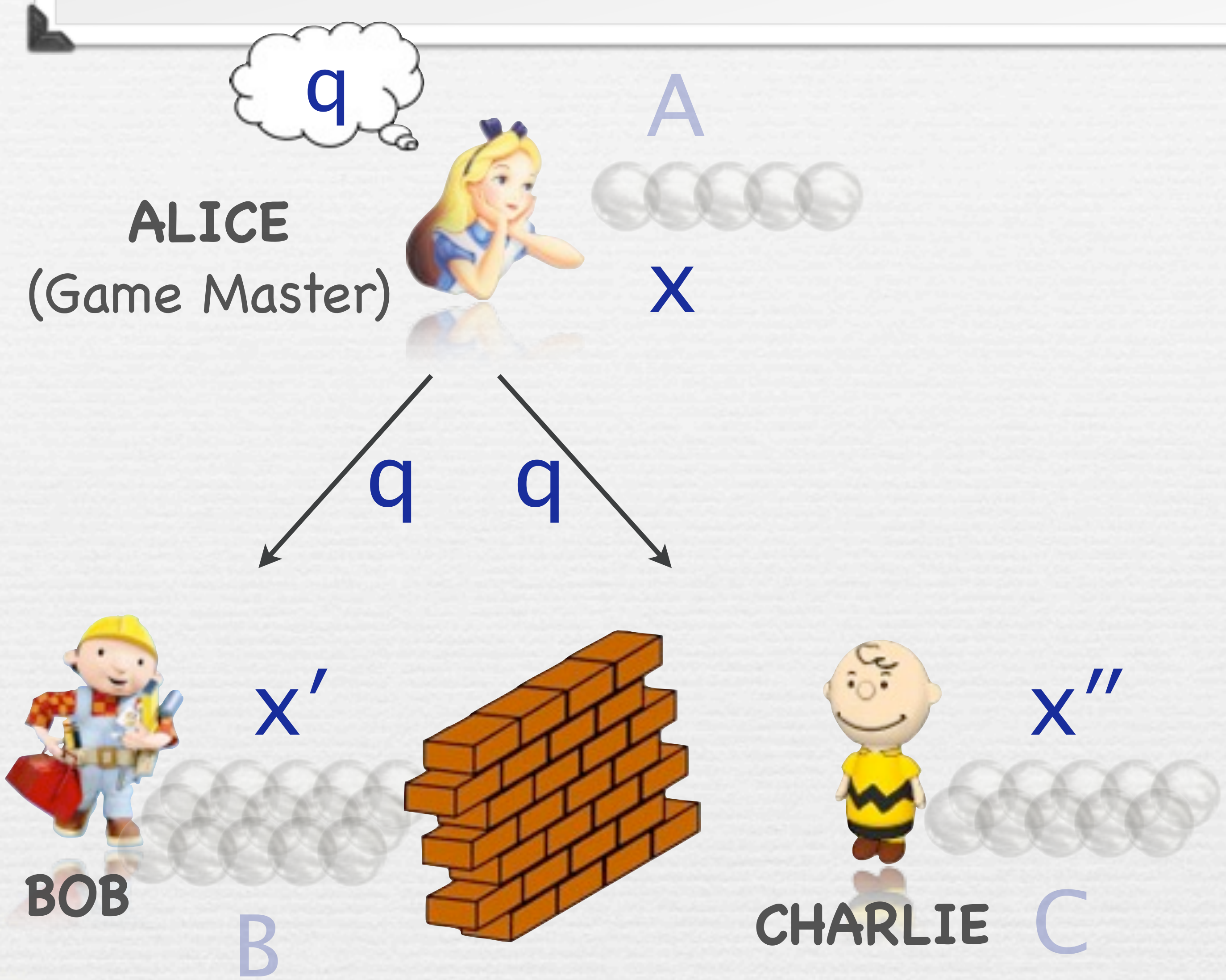
BOB and CHARLIE jointly **win** if:

both $x' = x$ **and** $x'' = x$.

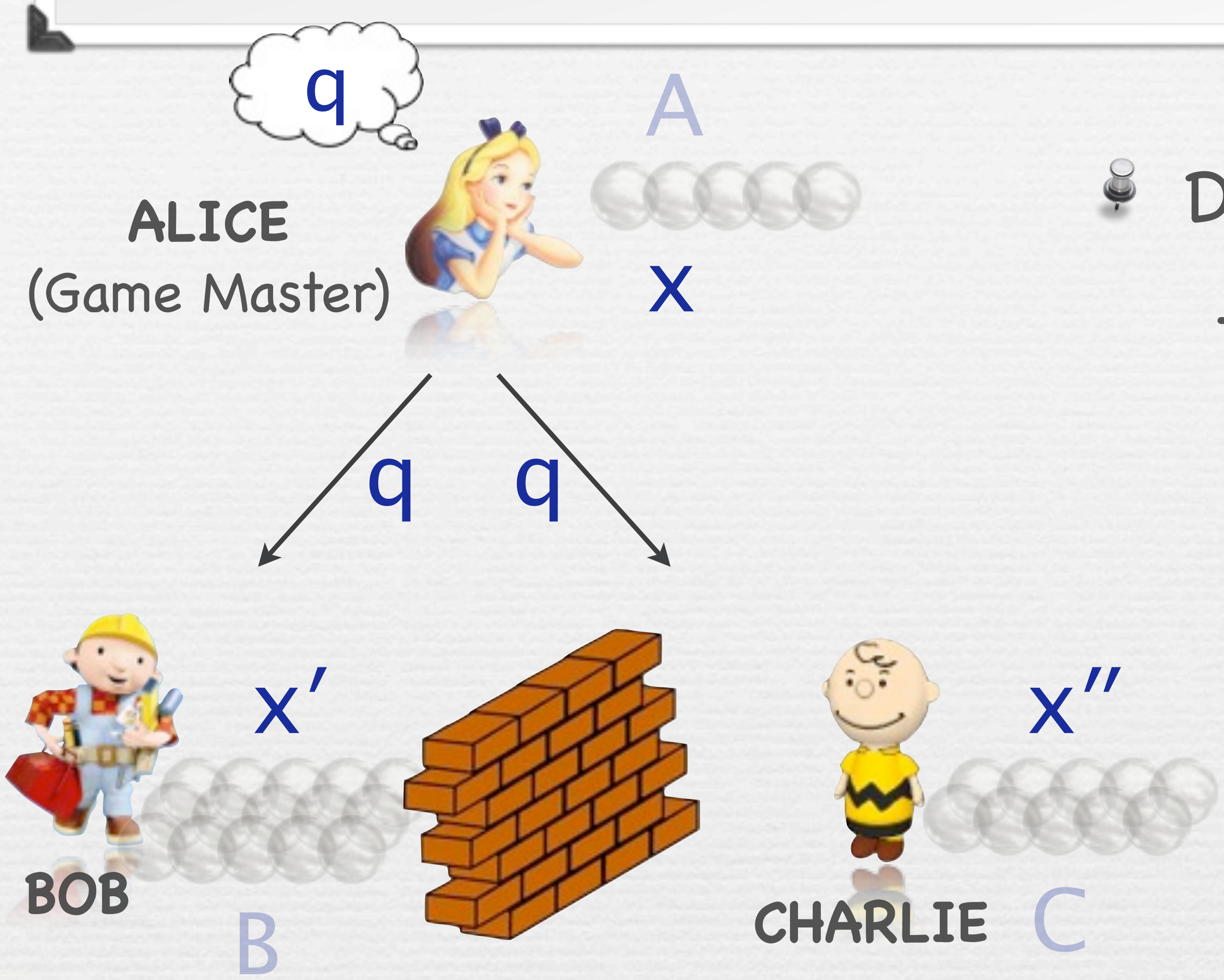
ALICE:

- chooses random $q = (q_1, \ldots, q_n) \in \{+, \times\}^n$,
- measures $A_1 \ldots A_n$ in respective bases $q_1, \ldots, q_n$ -> $x \in \{0,1\}^n$,
- sends q to BOB and CHARLIE

Intuition

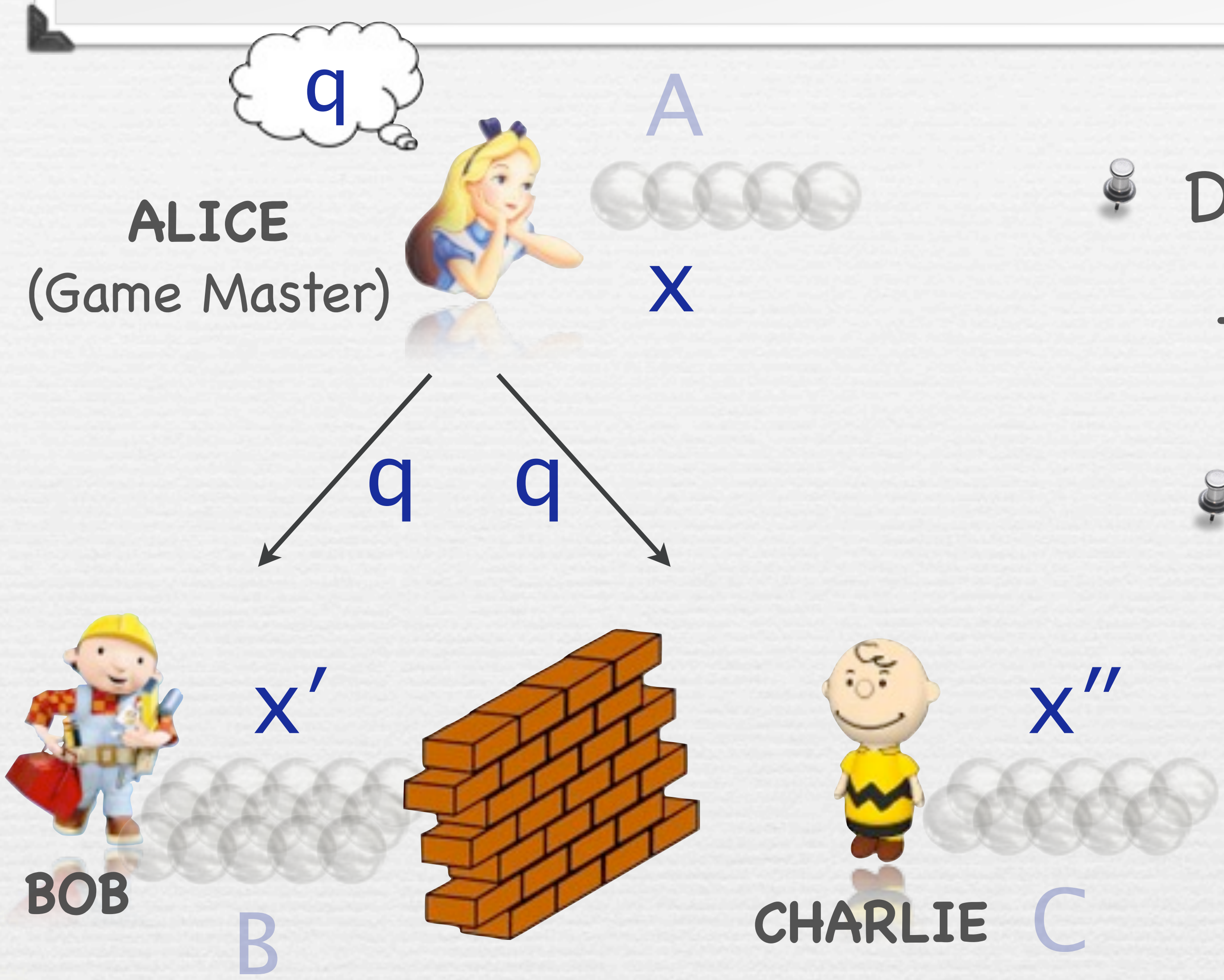


Intuition



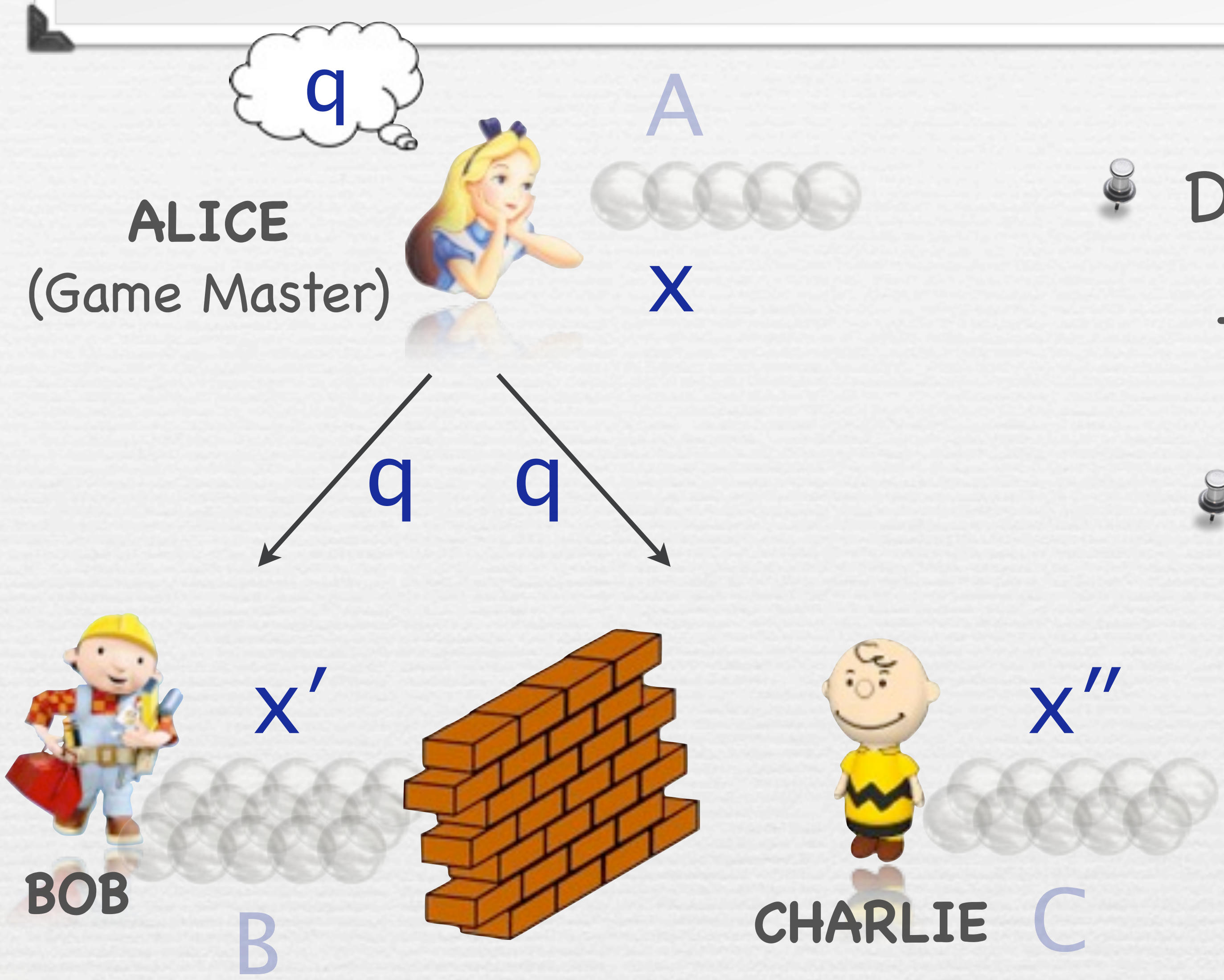
- Due to **uncertainty principle:**
  - **fresh randomness** in x

Intuition



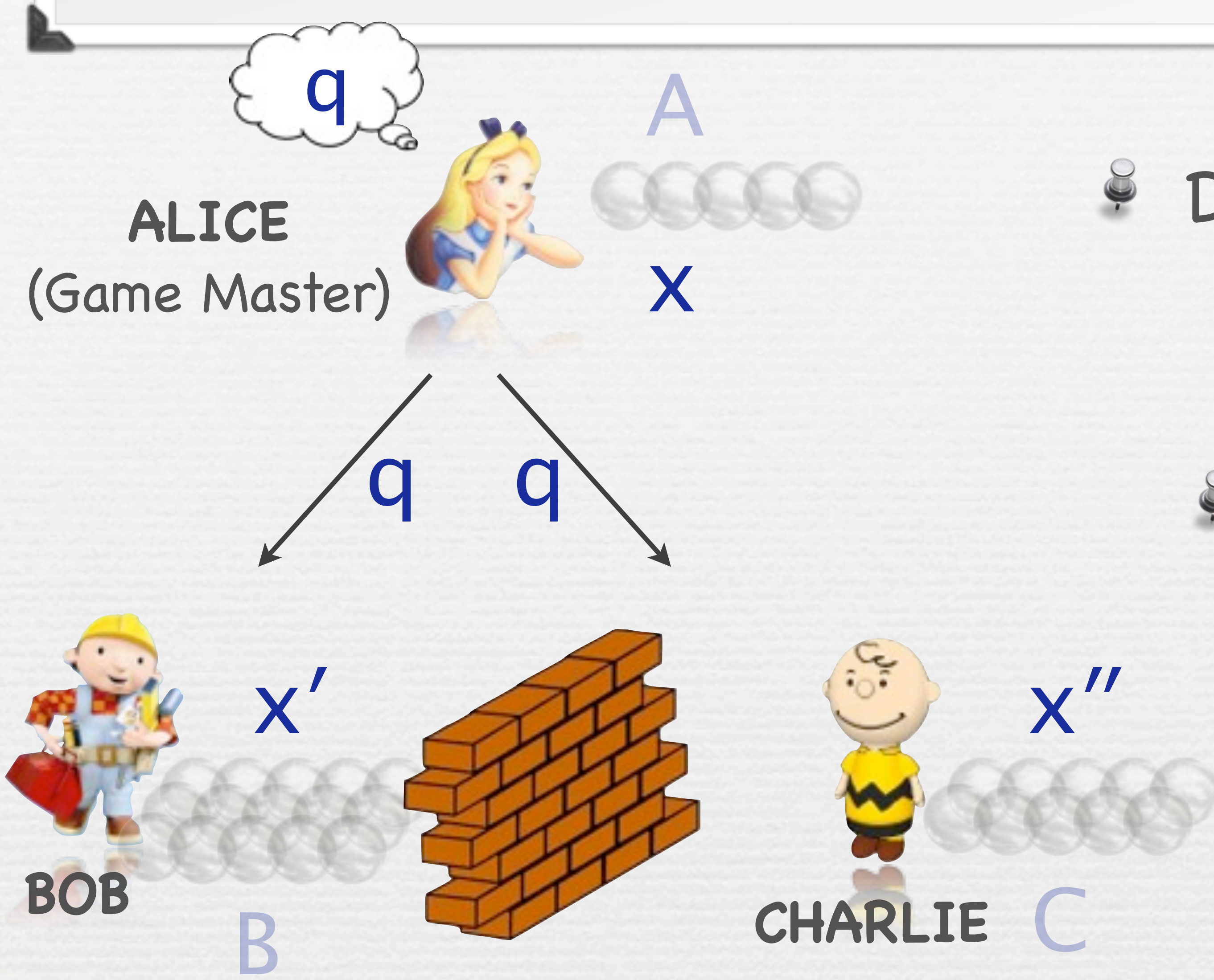
- Due to **uncertainty principle**:
  - **fresh randomness** in x
- If A & B are fully **entangled**:
  - can achieve $x' = x$

Intuition



- Due to **uncertainty principle**:
  - **fresh randomness** in x
- If A & B are fully **entangled**:
  - can achieve $x' = x$
- By **monogamy**:
  - A & C are not entangled
  - CHARLIE has a hard time

Intuition



- Due to **uncertainty principle**:
  - **fresh randomness** in x
- If A & B are fully **entangled**:
  - can achieve $x' = x$
- By **monogamy**:
  - A & C are not entangled
  - CHARLIE has a hard time

Thus, we expect:

$$p_{\mathrm{win}}(n) := \max_{\substack{\text{initial states} \\ \& \\ \text{measurements}}} P[X' = X \wedge X'' = X] \approx 0$$

Our Main Technical Result

Formally: $$p_{\text{win}}(n) := \max_{\{P_x^\theta\},\{Q_x^\theta\}} \frac{1}{2^n} \left\| \sum_{\theta,x} H^\theta |x\rangle\langle x| H^\theta \otimes P_x^\theta \otimes Q_x^\theta \right\|$$

Theorem:

$$p_{\text{win}}(n) \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^n \approx 0.85^n$$

Our Main Technical Result

Formally: $$p_{\text{win}}(n) := \max_{\{P_x^\theta\},\{Q_x^\theta\}} \frac{1}{2^n} \left\| \sum_{\theta,x} H^\theta |x\rangle\langle x| H^\theta \otimes P_x^\theta \otimes Q_x^\theta \right\|$$

Theorem:

$$p_{\text{win}}(n) \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^n \approx 0.85^n$$

Remarks:

- Bound is **tight** (i.e., $p_{\text{win}}(n)$ = ...)
- Strong parallel repetition: $p_{\text{win}}(n) = p_{\text{win}}(1)^n$
- Is attained **without any entanglement**
  => monogamy completely kills power of entanglement

Our Main Technical Result

Formally: $$p_{\mathrm{win}}(n) := \max_{\{P_x^\theta\},\{Q_x^\theta\}} \frac{1}{2^n} \left\| \sum_{\theta,x} H^\theta |x\rangle\langle x| H^\theta \otimes P_x^\theta \otimes Q_x^\theta \right\|$$

Theorem:

$$p_{\mathrm{win}}(n) \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^n \approx 0.85^n$$

Our Main Technical Result

Formally: $p_{\text{win}}(n) := \max_{\{P_x^\theta\},\{Q_x^\theta\}} \frac{1}{2^n} \left\| \sum_{\theta,x} H^\theta |x\rangle\langle x| H^\theta \otimes P_x^\theta \otimes Q_x^\theta \right\|$

Theorem:

$$p_{\text{win}}(n) \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^n \approx 0.85^n$$

Proof:

- very simple
- New **operator-norm inequality**: bounds $||\sum_i O_i||$ for positive operators $O_1,\dots,O_n$ in terms of $||\sqrt{O_i}\sqrt{O_j}||$.

Generalizations

- **Arbitrary** (and arbitrary many) **measurements** for Alice

Generalizations

- **Arbitrary** (and arbitrary many) **measurements** for Alice
- **Relaxed winning condition** for Bob and/or Charlie, i.e., $x' \approx x$ and $x'' \approx x$, or $x' \approx x$ and $x'' = x$.

Main Application Result

Theorem (informal): Standard BB84 QKD remains secure even if Bob's measurement device is **malicious**.

Main Application Result

Theorem (informal): Standard BB84 QKD remains secure even if Bob's measurement device is **malicious**.

Remarks:

- Referred to as: one-sided device-independent security
- Was claimed before, but no correct proof was given

Main Application Result

Theorem (informal): Standard BB84 QKD remains secure even if Bob's measurement device is **malicious**.

Remarks:

- Referred to as: one-sided device-independent security
- Was claimed before, but no correct proof was given

In the proof:

- We analyze EPR-pair bases version of BB84
- Well known to imply security for standard BB84 QKD

EPR-Pair Based BB84 QKD

ALICE

BOB

CHARLIE

EPR-Pair Based BB84 QKD

ALICE

BOB

EVE

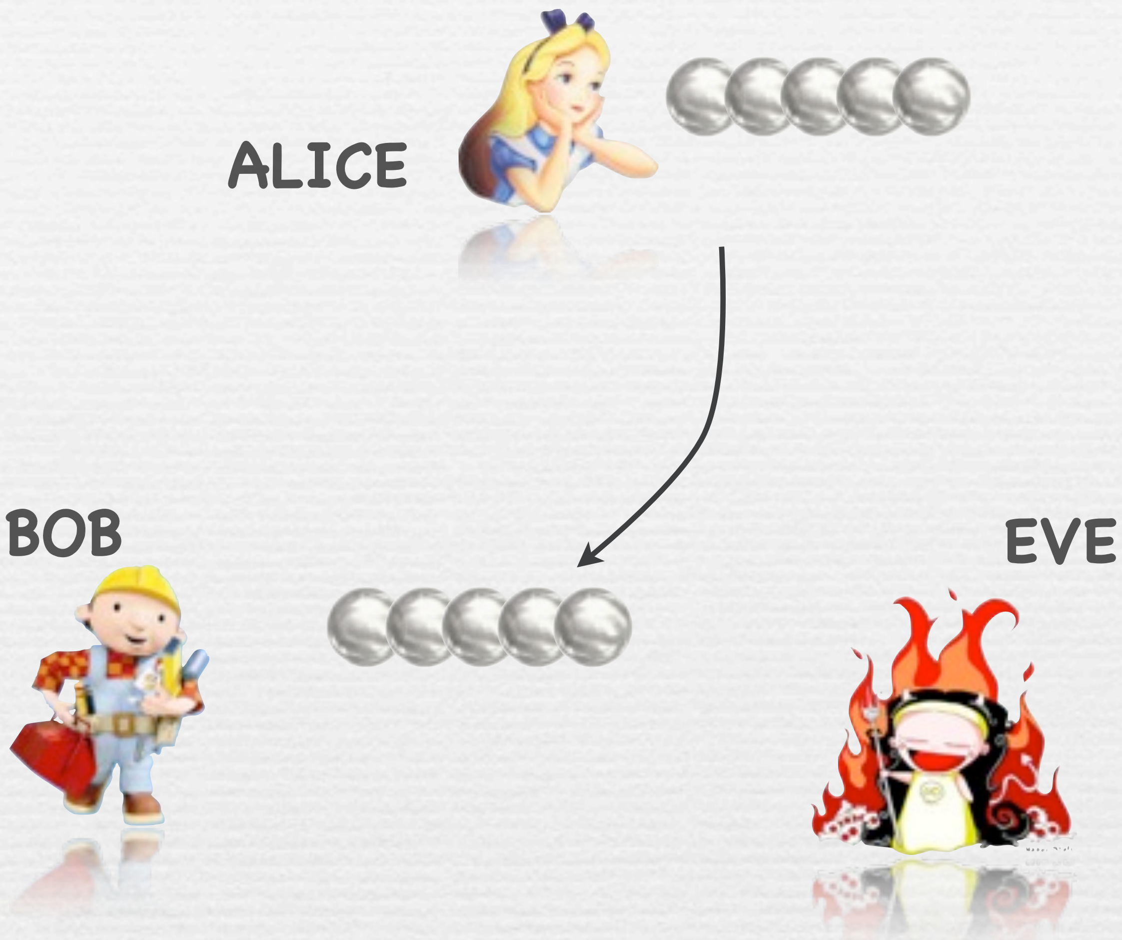
EPR-Pair Based BB84 QKD

ALICE

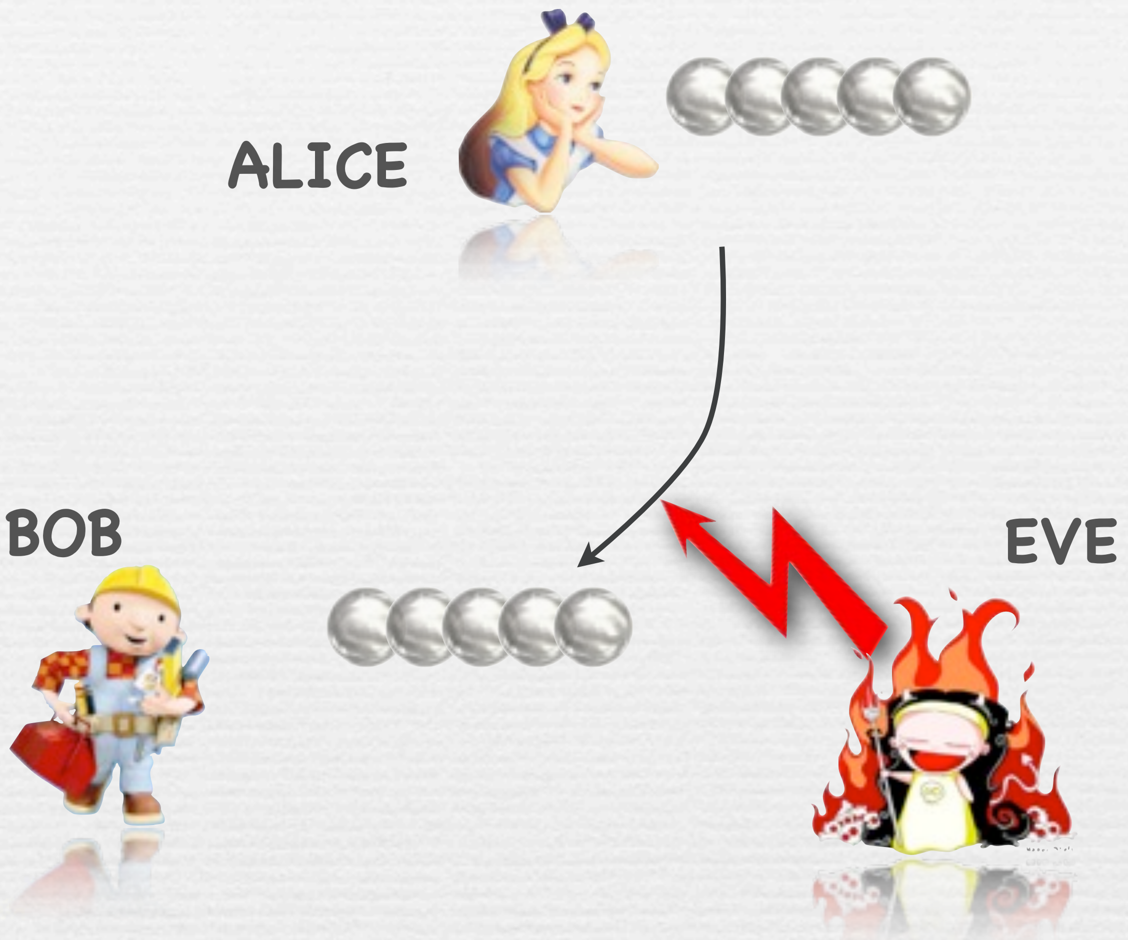
BOB

EVE

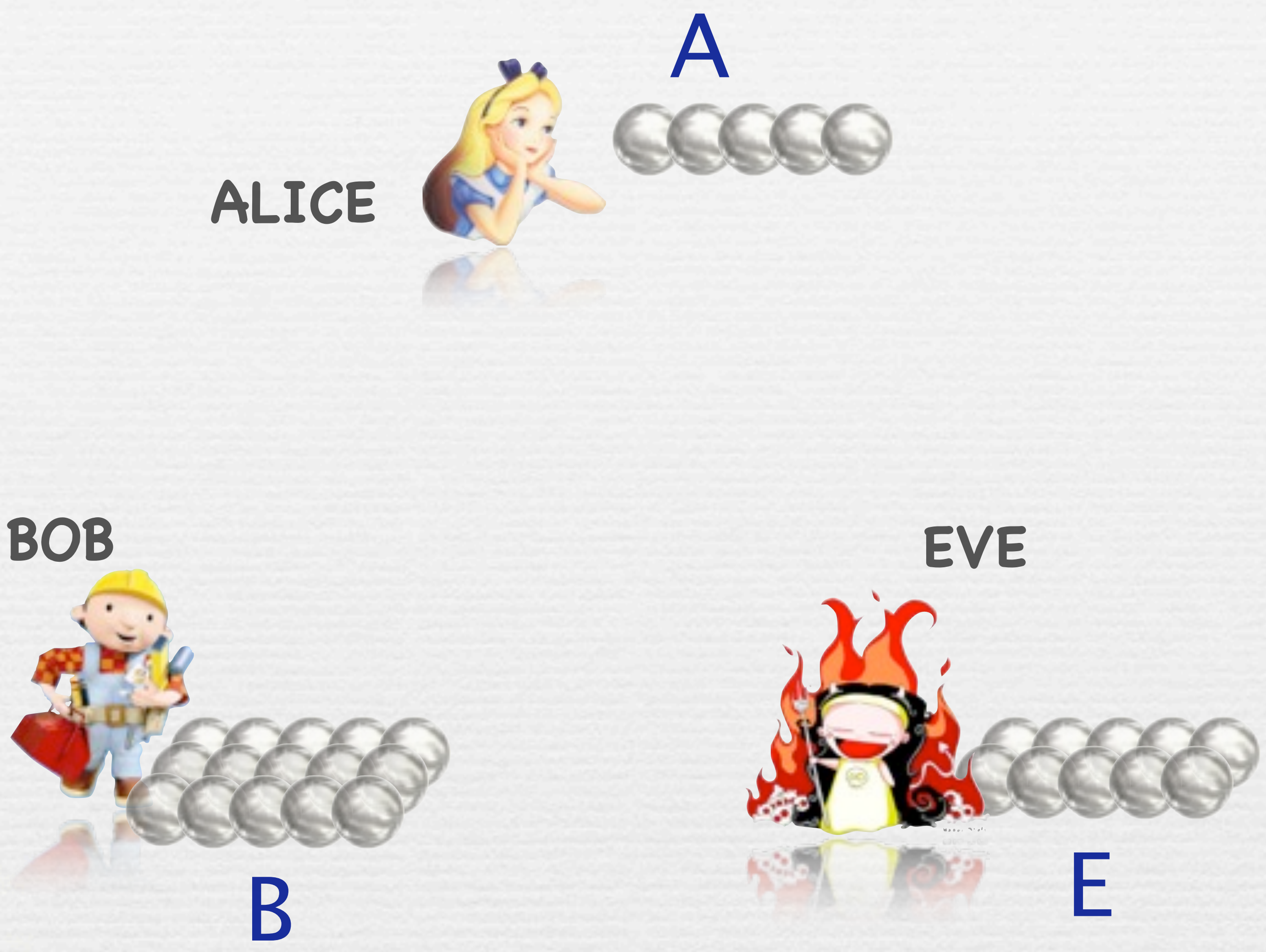
EPR-Pair Based BB84 QKD



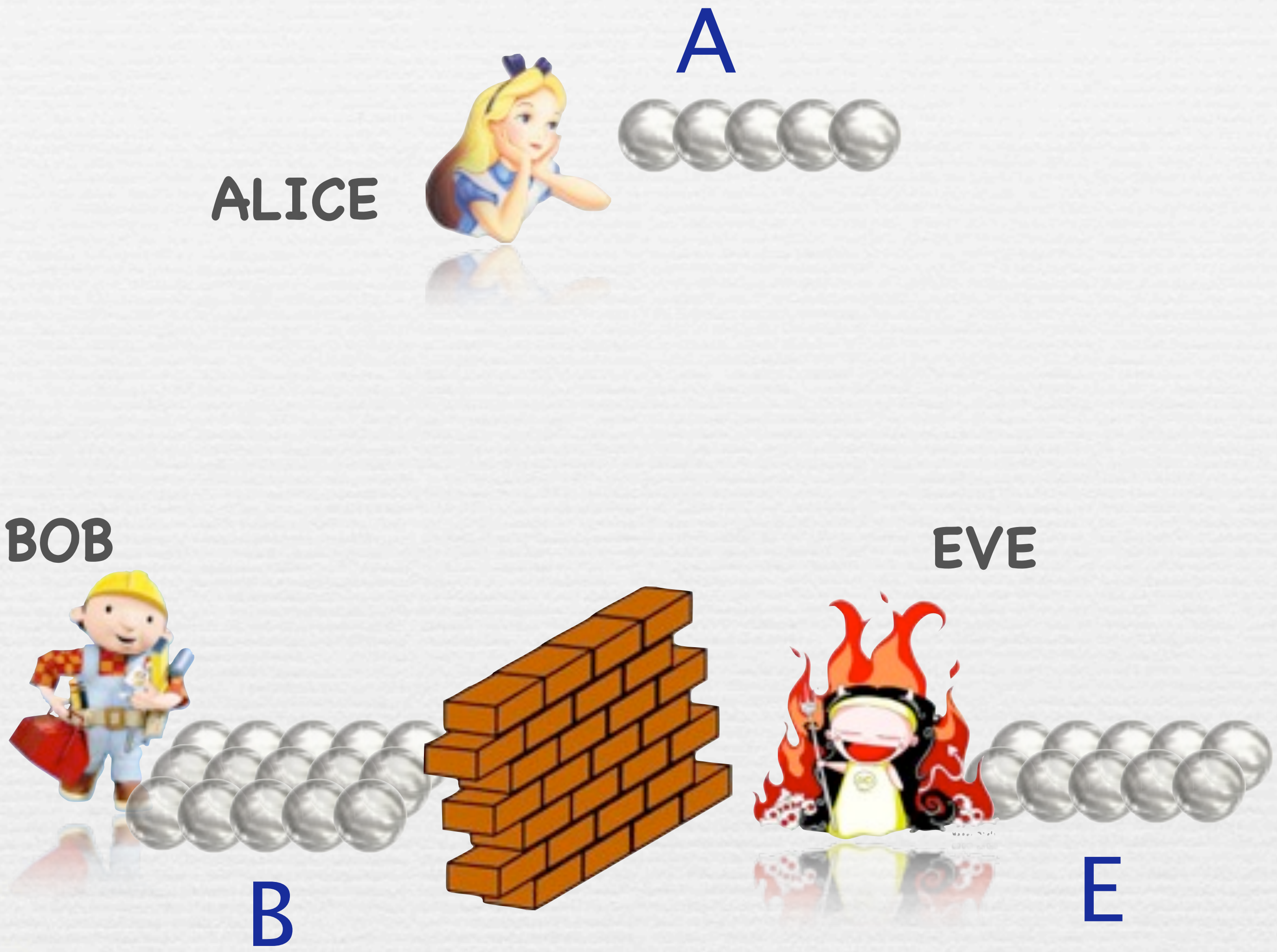
EPR-Pair Based BB84 QKD



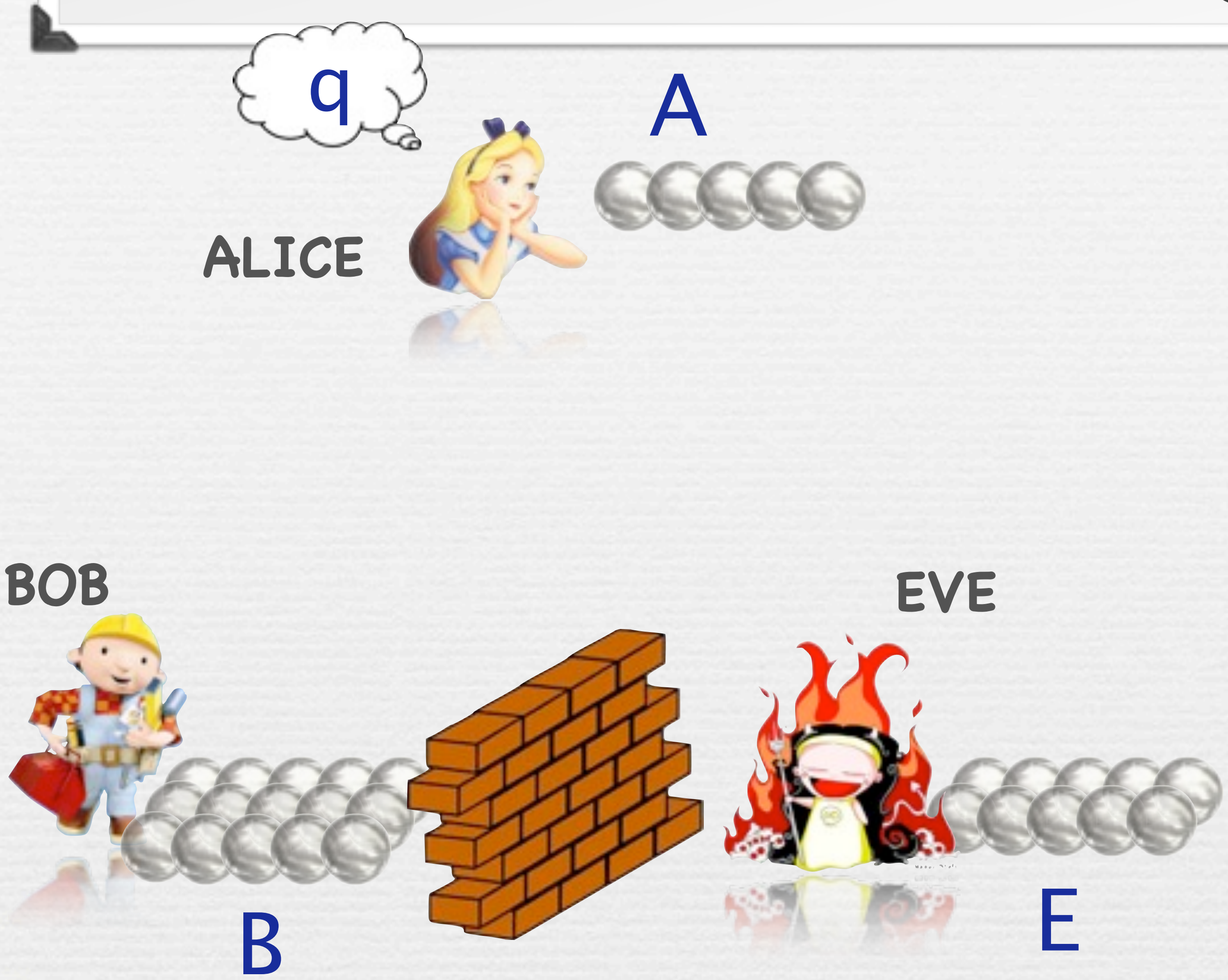
EPR-Pair Based BB84 QKD



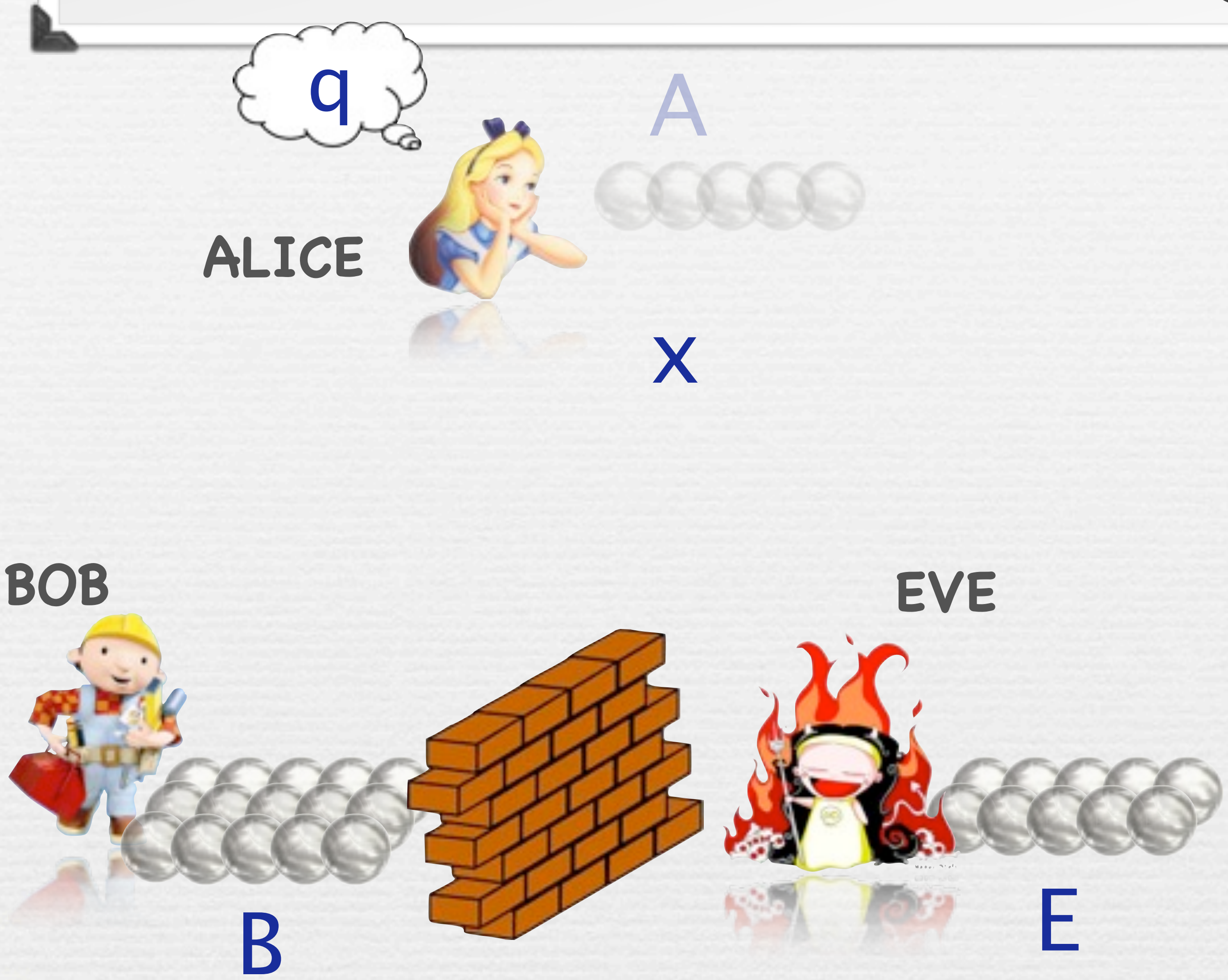
EPR-Pair Based BB84 QKD



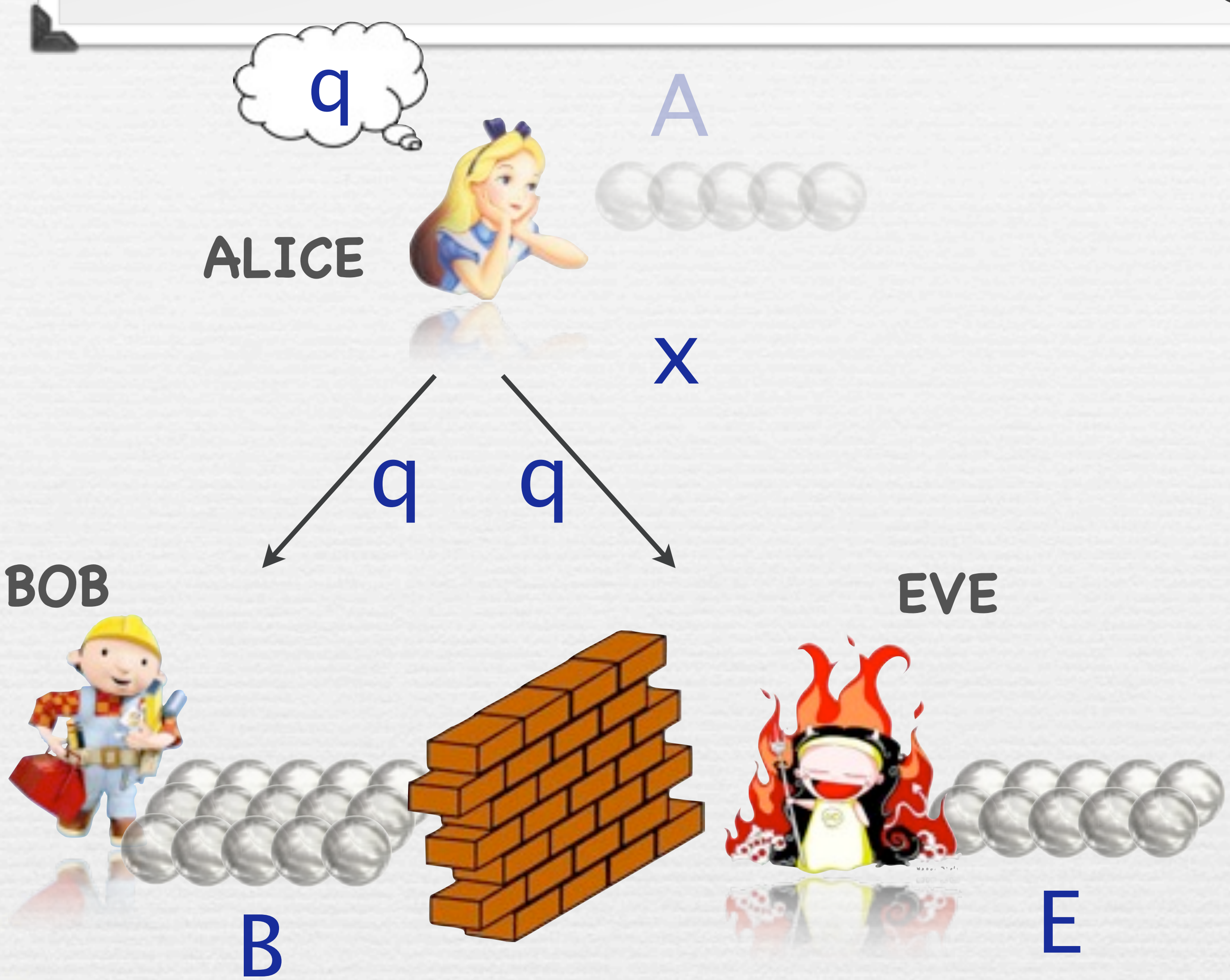
EPR-Pair Based BB84 QKD



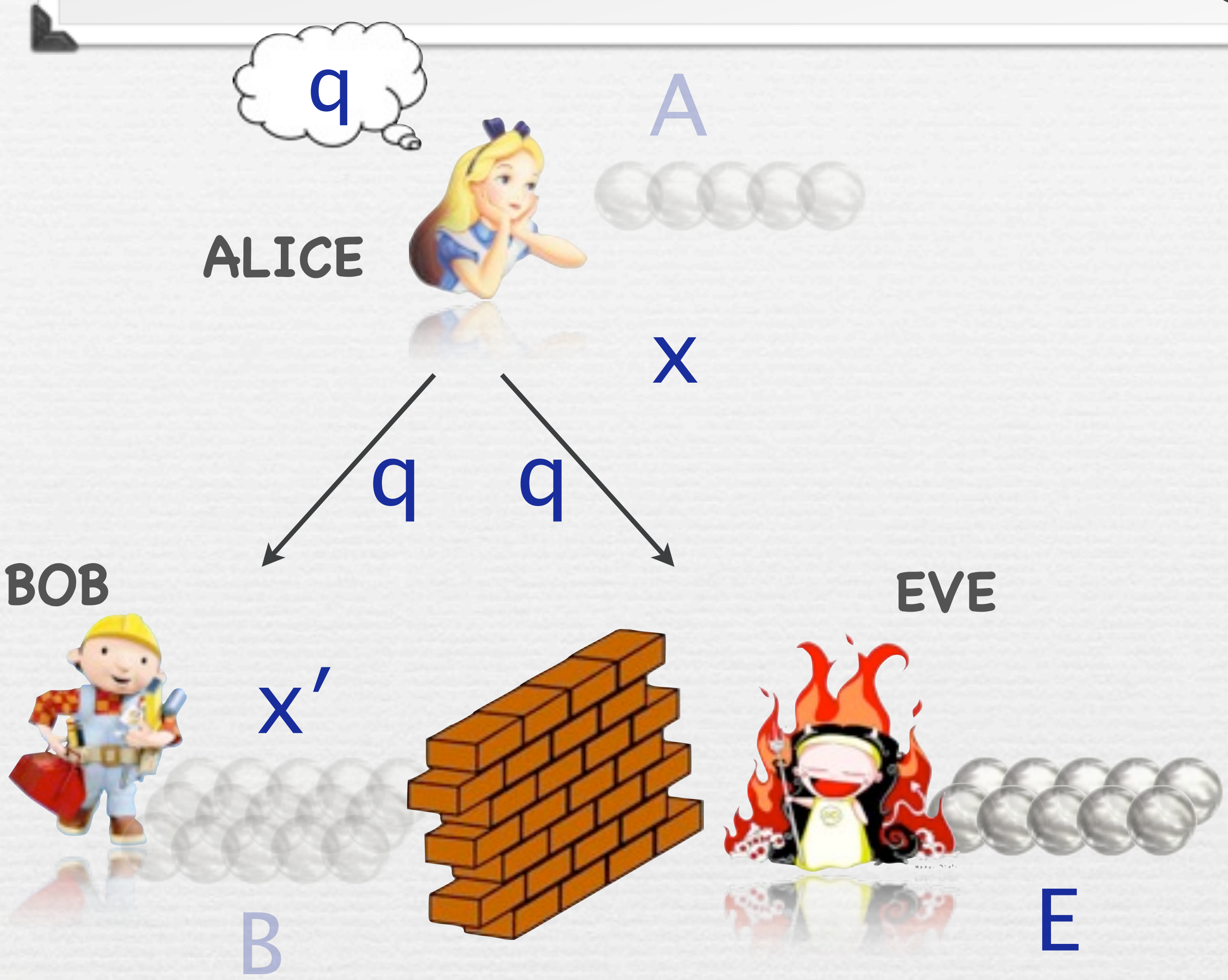
EPR-Pair Based BB84 QKD



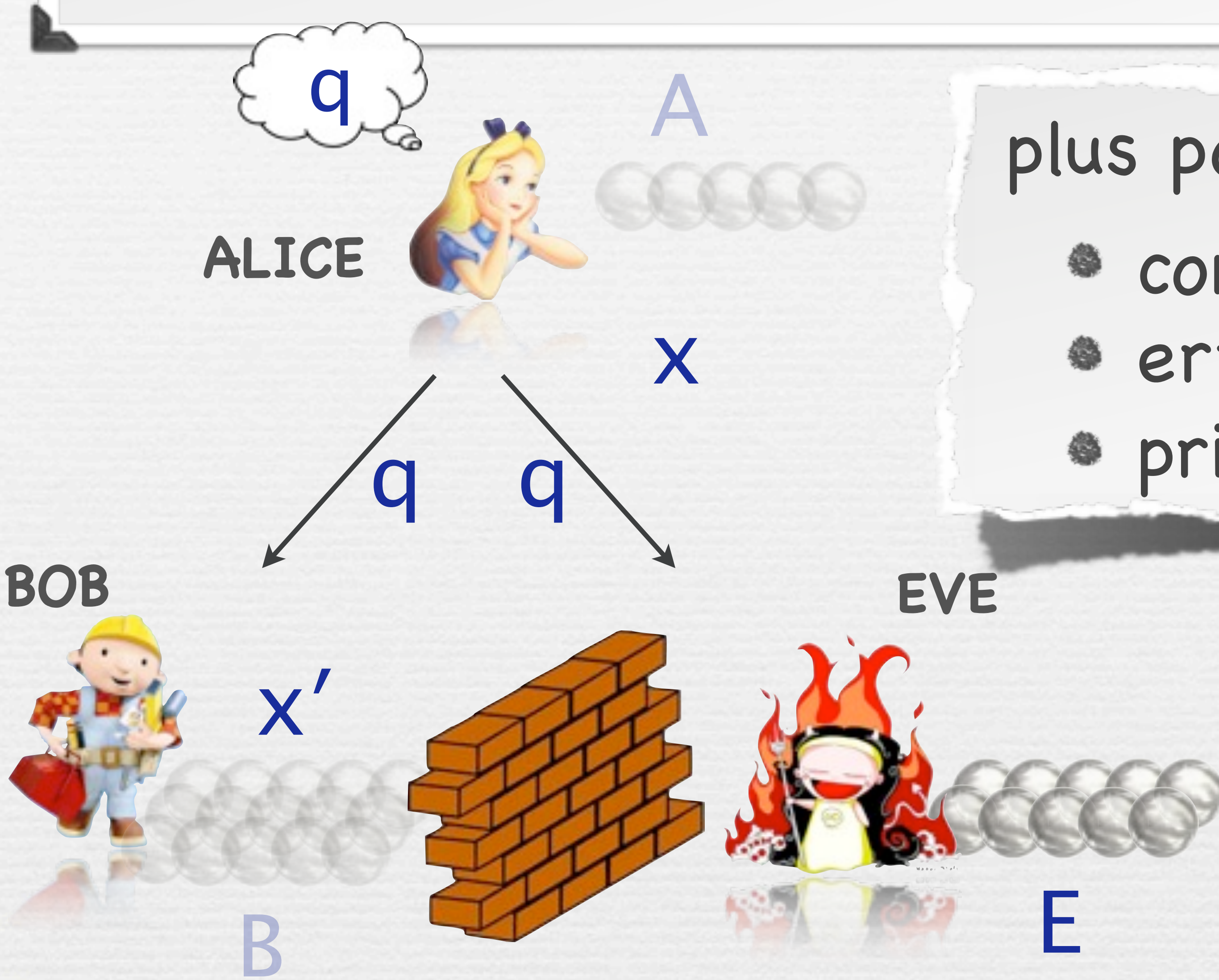
EPR-Pair Based BB84 QKD



EPR-Pair Based BB84 QKD



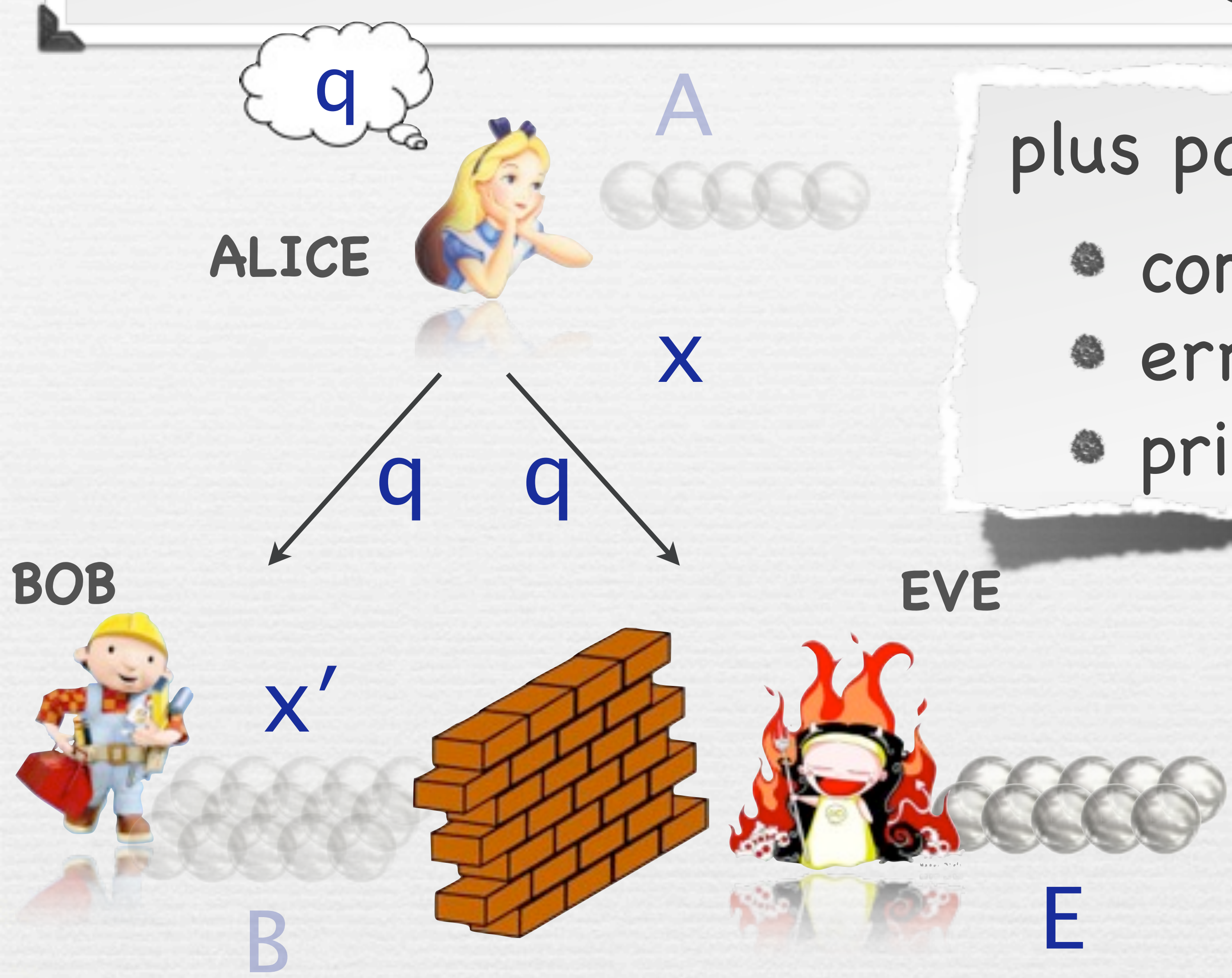
EPR-Pair Based BB84 QKD



plus post-processing:

- comparing x & x' on random subset
- error correction
- privacy amplification

EPR-Pair Based BB84 QKD



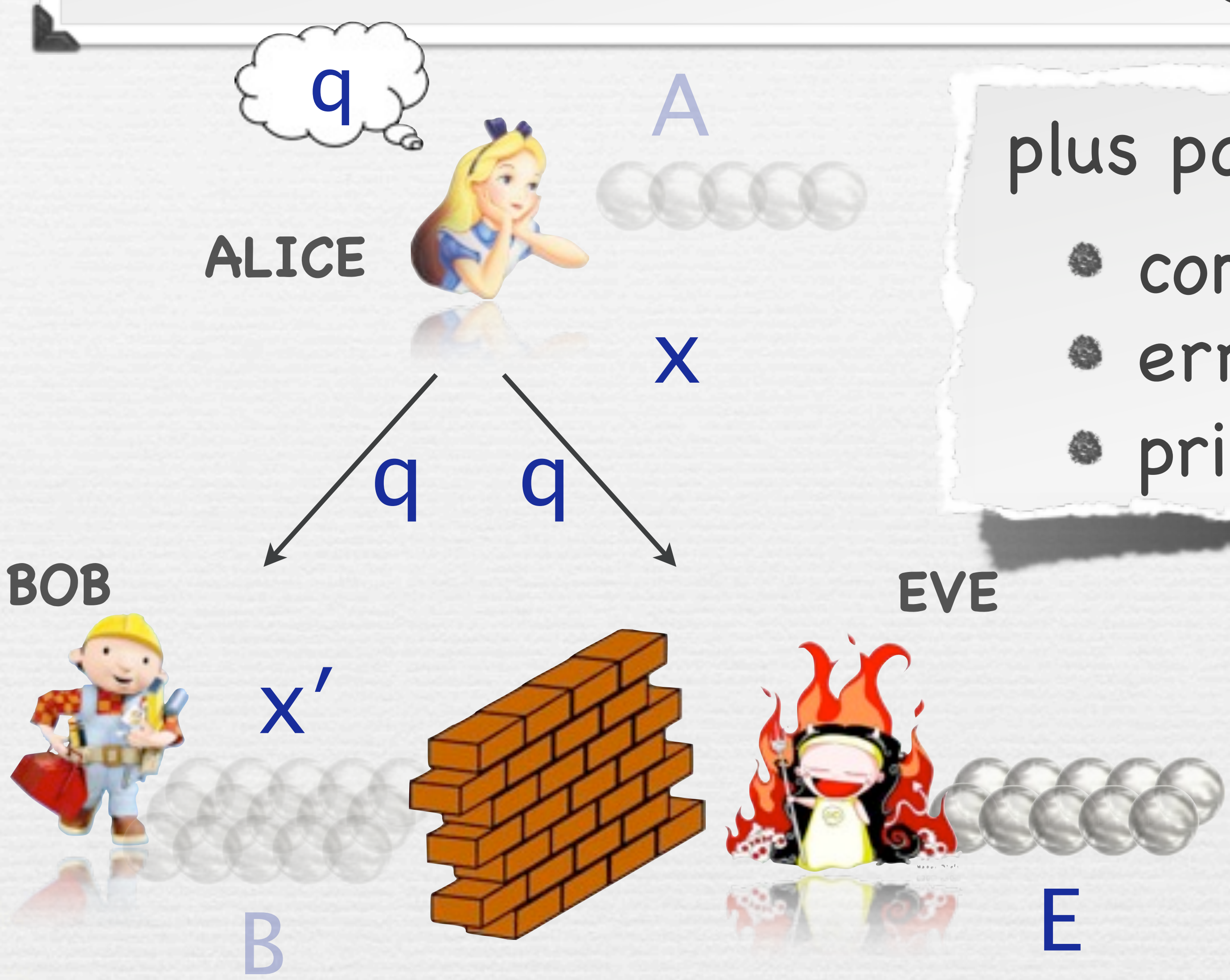
plus post-processing:

- comparing x & x' on random subset
- error correction
- privacy amplification

To prove:

$H_\infty(X|QE, \text{not abort}) \geq t$

EPR-Pair Based BB84 QKD



plus post-processing:

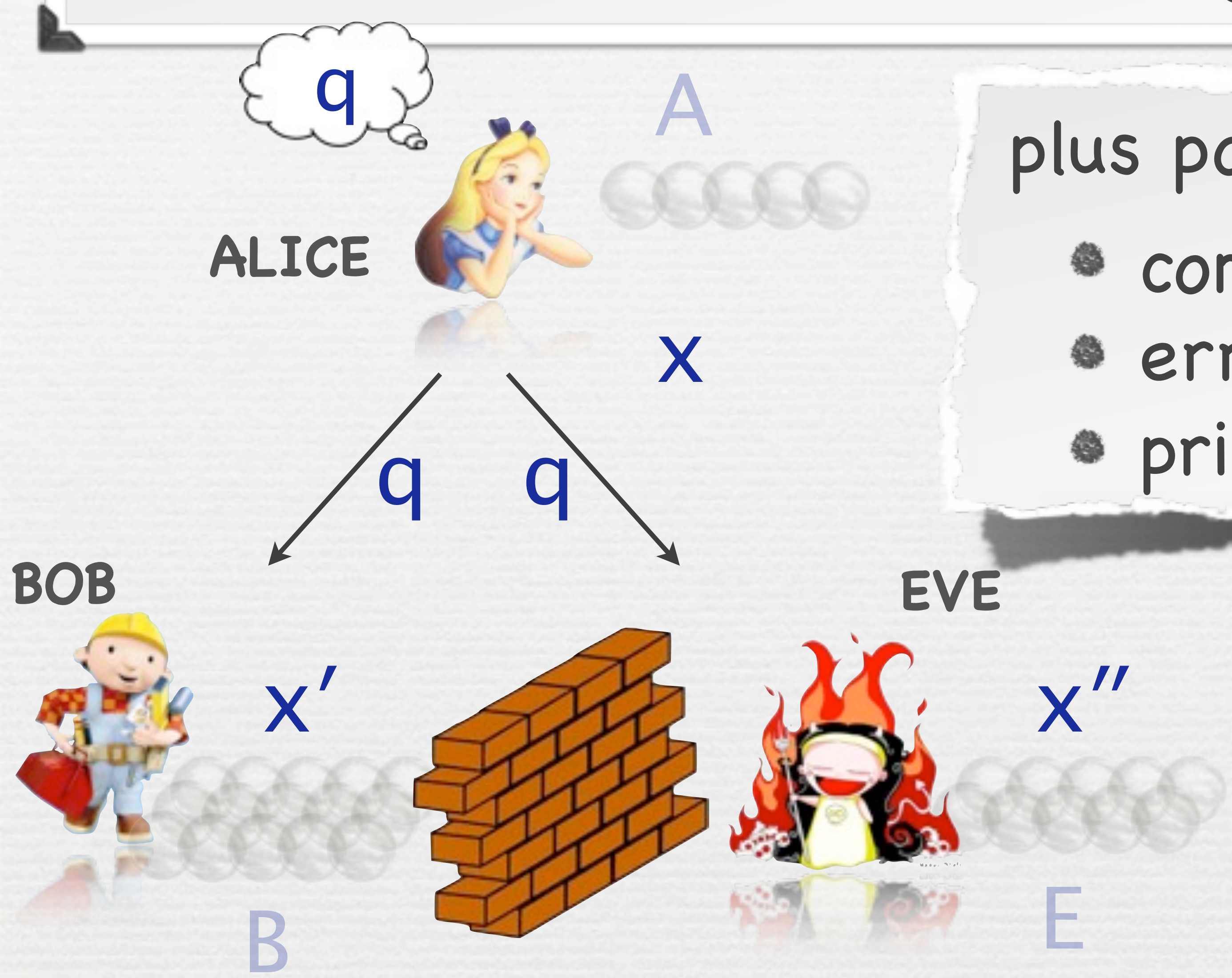
- comparing x & x' on random subset
- error correction
- privacy amplification

To prove:

$H_\infty(X|QE, \text{not abort}) \geq t$

- For sake of argument: say that Eve measures E

EPR-Pair Based BB84 QKD



plus post-processing:

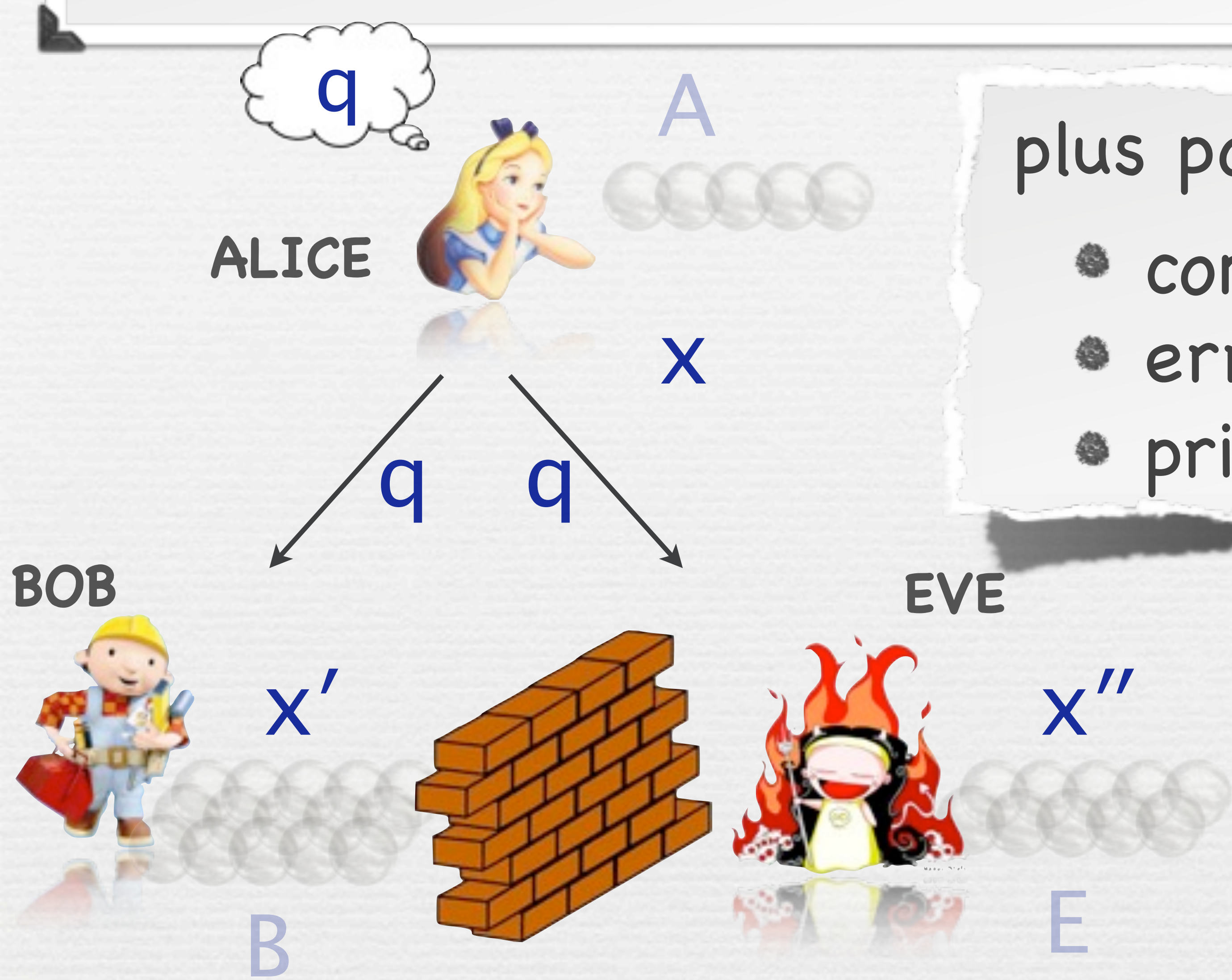
- comparing x & x' on random subset
- error correction
- privacy amplification

To prove:

$H_\infty(X|QE, \text{not abort}) \geq t$

- For sake of argument: say that Eve measures E

EPR-Pair Based BB84 QKD



plus post-processing:

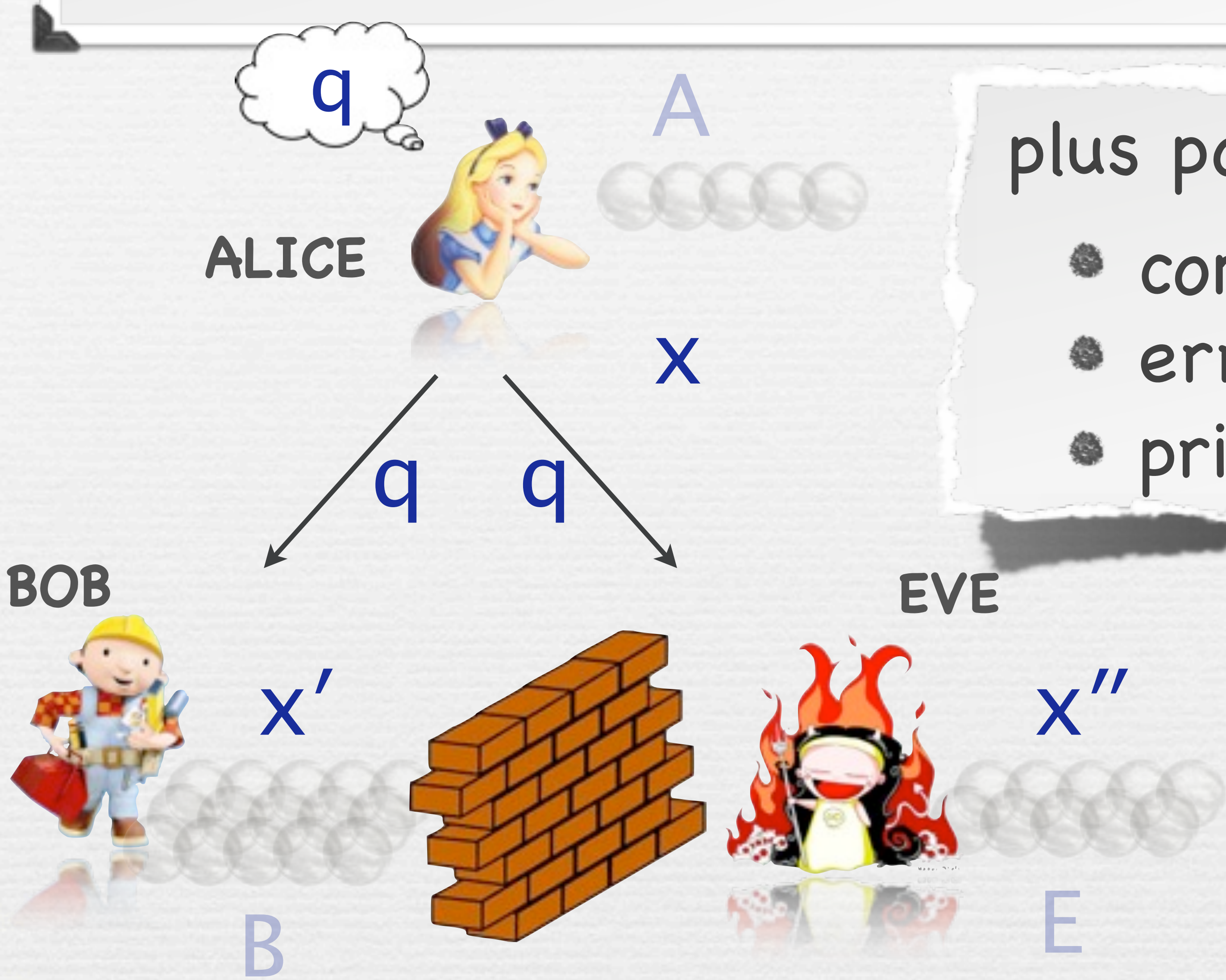
- comparing x & x' on random subset
- error correction
- privacy amplification

To prove:

$H_\infty(X|QE, \text{not abort}) \geq t$

- For sake of argument: say that Eve measures E
- Monogamy game ⇒ $P[X' \approx X \wedge X'' = X] \leq e^n$

EPR-Pair Based BB84 QKD



plus post-processing:

- comparing x & x' on random subset
- error correction
- privacy amplification

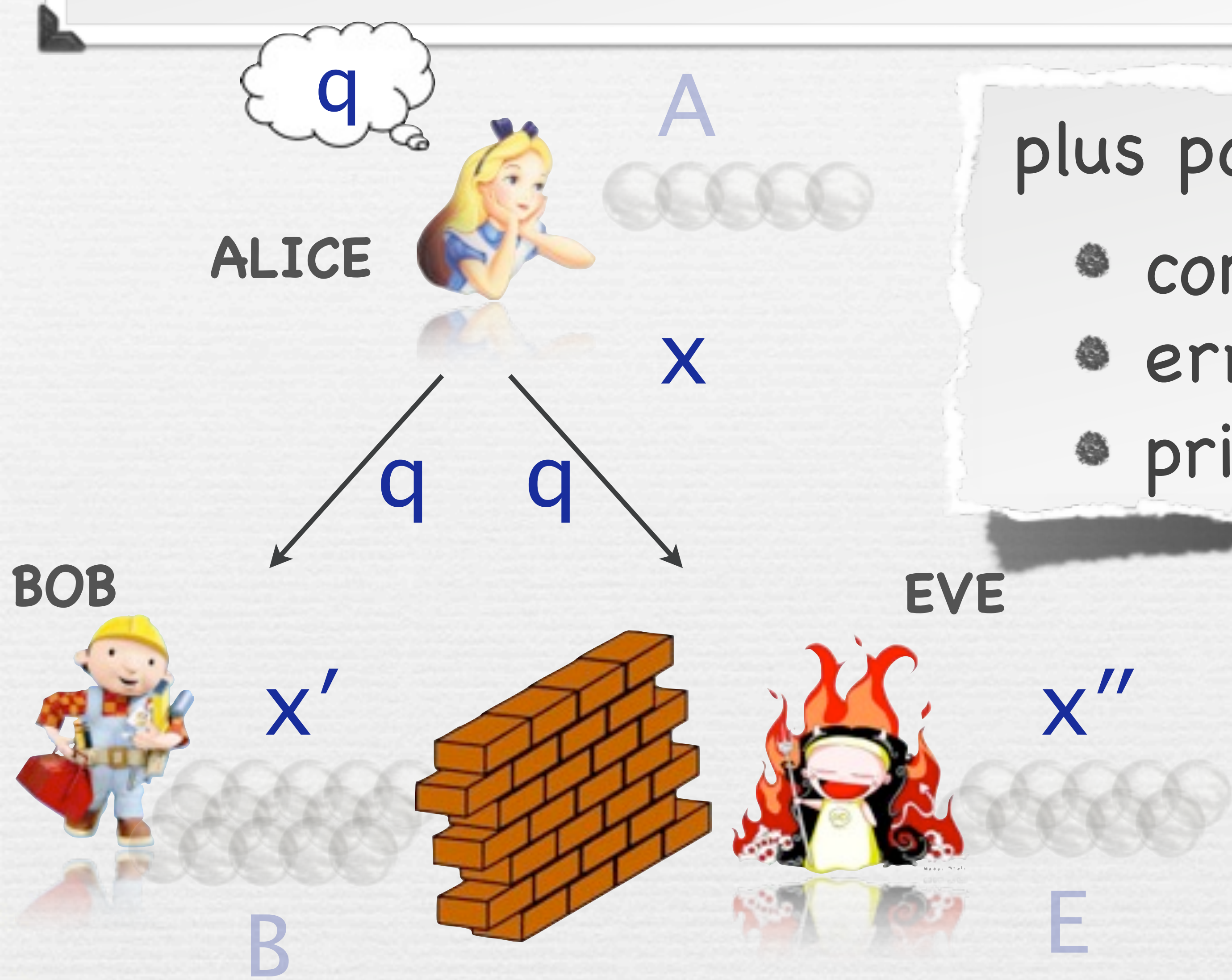
To prove:

$H_\infty(X|QE, \text{not abort}) \geq t$

- For sake of argument: say that Eve measures E
- Monogamy game $\Rightarrow P[X' \approx X \wedge X'' = X] \leq e^n$

  $\Rightarrow P[X' \approx X] \leq e^{n/2}$ (and thus $P[\text{abort}] \approx 1$)

EPR-Pair Based BB84 QKD



plus post-processing:

- comparing x & x' on random subset
- error correction
- privacy amplification

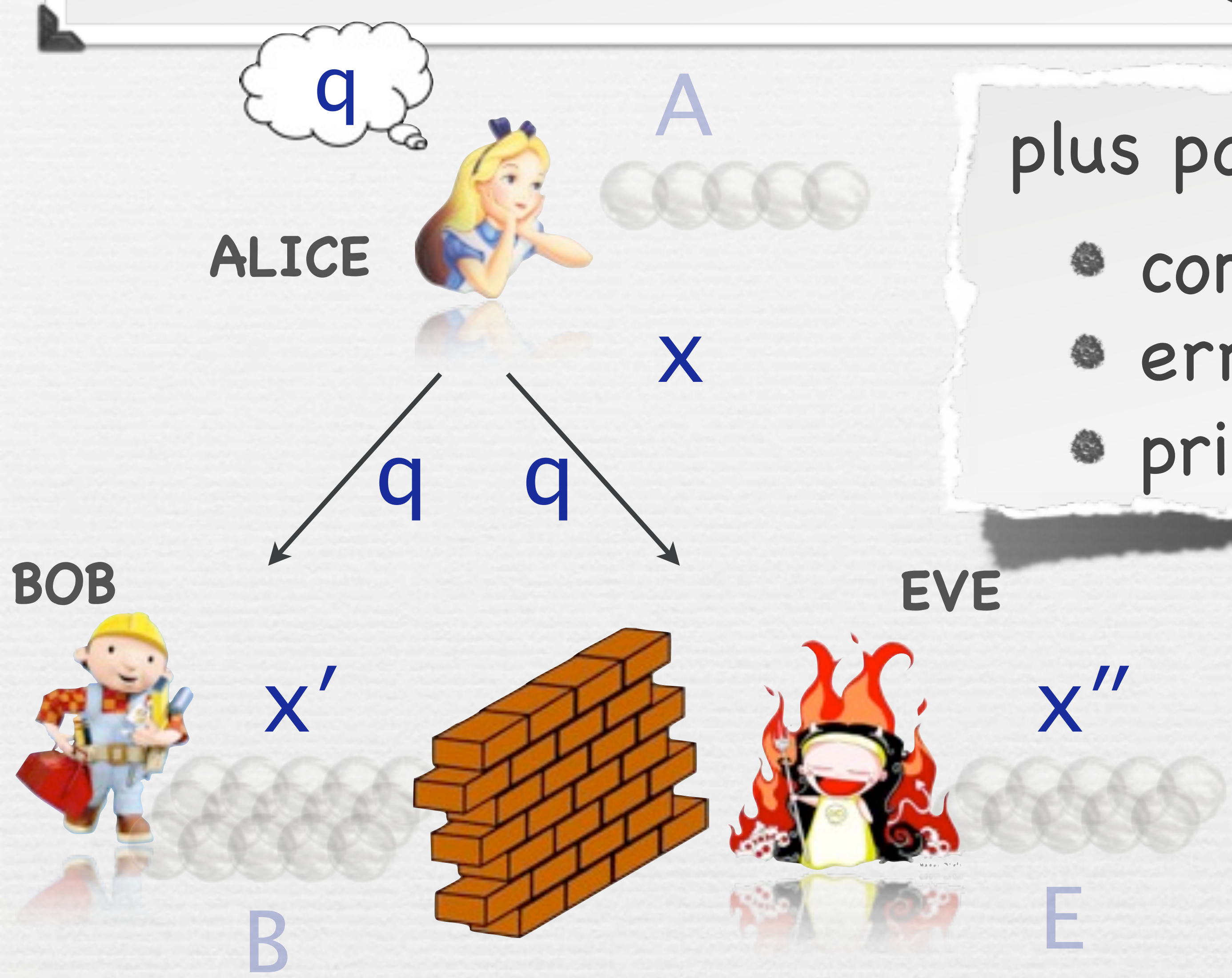
To prove:

$H_\infty(X|QE, \text{not abort}) \geq t$

- For sake of argument: say that Eve measures E
- Monogamy game $\Rightarrow P[X' \approx X \wedge X'' = X] \leq e^n$

  $\Rightarrow P[X' \approx X] \leq e^{n/2}$ (and thus $P[\text{abort}] \approx 1$) ✓

EPR-Pair Based BB84 QKD



plus post-processing:

- comparing x & x' on random subset
- error correction
- privacy amplification

To prove:

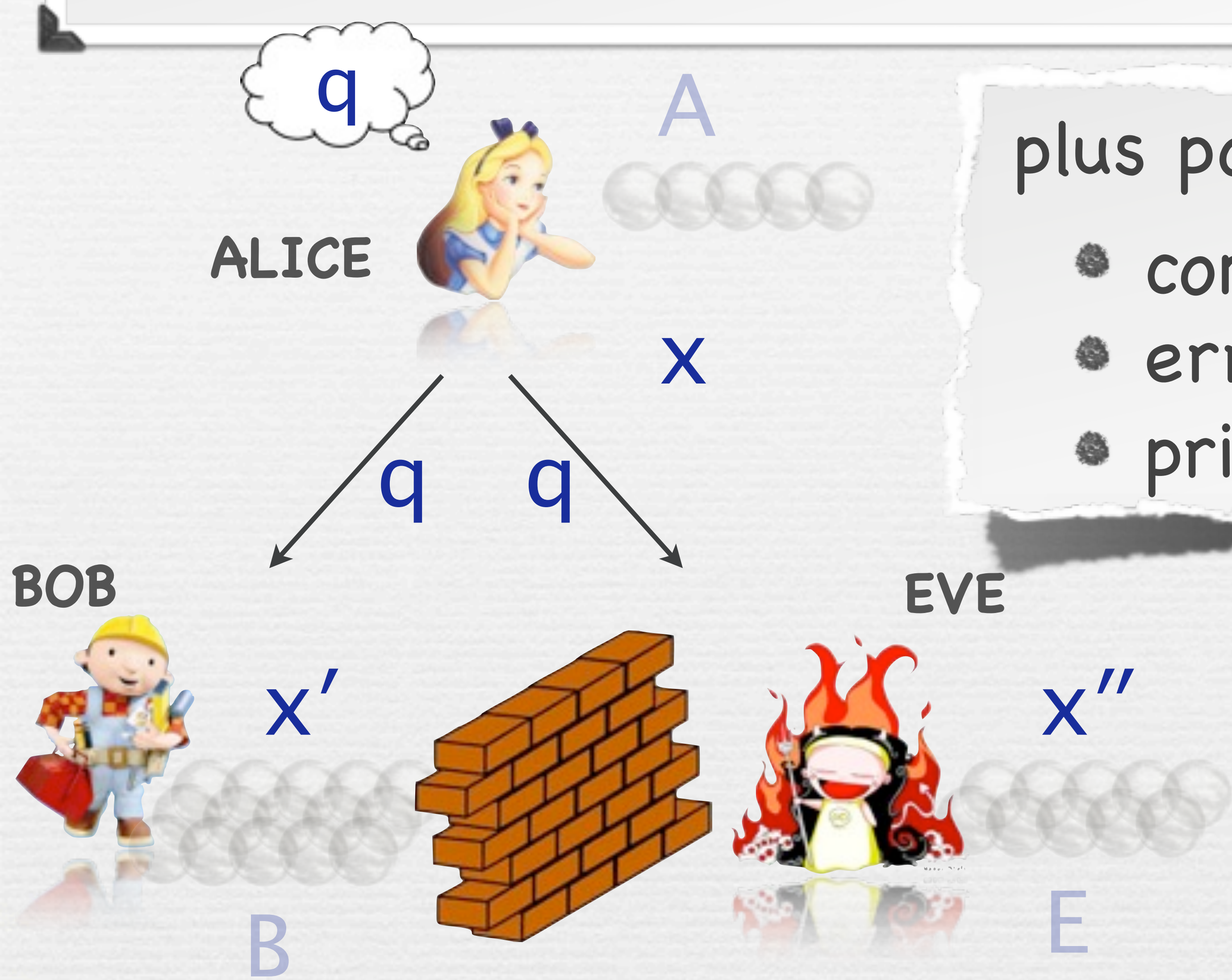
$H_\infty(X|QE, \text{not abort}) \geq t$

- For sake of argument: say that Eve measures E
- Monogamy game $\Rightarrow P[X' \approx X \wedge X'' = X] \leq e^n$

  $\Rightarrow P[X' \approx X] \leq e^{n/2}$ (and thus $P[\text{abort}] \approx 1$) ✓

  or $P[X'' = X \mid X' \approx X] \leq e^{n/2}$ $\forall$ measurement of E

EPR-Pair Based BB84 QKD



plus post-processing:

- comparing x & x' on random subset
- error correction
- privacy amplification

To prove:

$H_\infty(X|QE, \text{not abort}) \geq t$

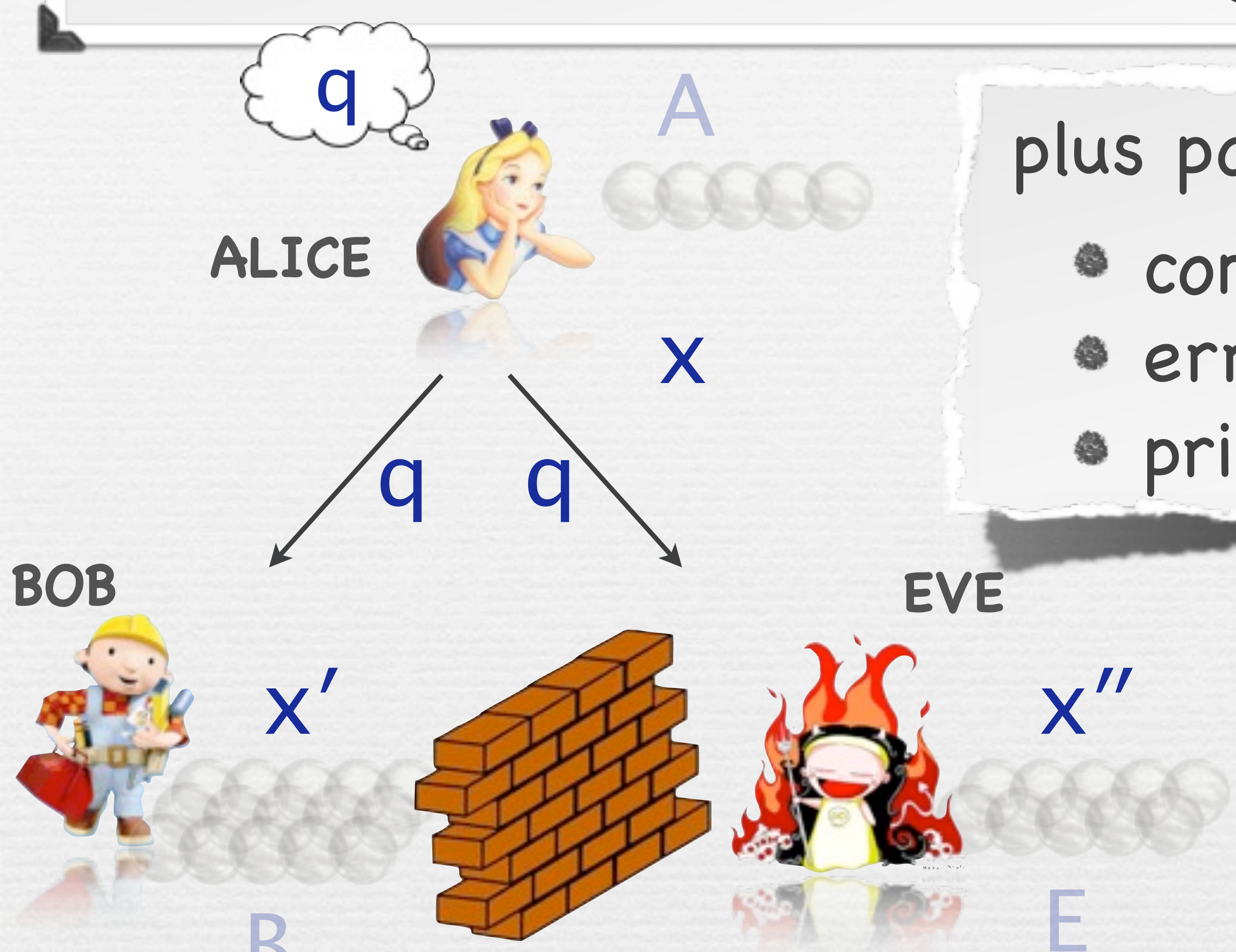
- For sake of argument: say that Eve measures E
- Monogamy game $\Rightarrow$ $P[X' \approx X \wedge X'' = X] \leq e^n$

  $\Rightarrow$ $P[X' \approx X] \leq e^{n/2}$ (and thus $P[\text{abort}] \approx 1$) ✓

  or $P[X'' = X \,|\, X' \approx X] \leq e^{n/2}$ $\forall$ measurement of E

  $\Rightarrow$ $H_\infty(X \,|\, QE, X' \approx X) \geq n/2 \cdot \log(1/e)$

EPR-Pair Based BB84 QKD



plus post-processing:

- comparing x & x' on random subset
- error correction
- privacy amplification

To prove:

$H_\infty(X|QE, \text{not abort}) \geq t$

- For sake of argument: say that Eve measures E
- Monogamy game $\Rightarrow P[X' \approx X \wedge X'' = X] \leq e^n$

$\Rightarrow P[X' \approx X] \leq e^{n/2}$ (and thus $P[\text{abort}] \approx 1$) ✓

or $P[X'' = X \mid X' \approx X] \leq e^{n/2}$ $\forall$ measurement of E

$\Rightarrow H_\infty(X \mid QE, \overset{\text{not abort}}{\cancel{X' \approx X}}) \geq n/2 \cdot \log(1/e)$ ✓

Comparison with other protocols

	Reichhardt et al. (E91)	Vazirani/ Viddick (E91)	this work (BB84/BBM92)
device assumptions	none	none	trusted Alice (source)
noise tolerance	0%	1.2%	1.5% (11%)
key rate	0%	2.5%	22.8% (100%)
finite key analysis	×	×	✓

Summary

- Capture "monogamy of entanglement" by a game
- Analyze this monogamy game, and show:
  - winning probability is exponentially small
  - strong parallel repetition in some cases

Summary

- Capture "monogamy of entanglement" by a game
- Analyze this monogamy game, and show:
  - winning probability is exponentially small
  - strong parallel repetition in some cases
- Application I: to BB84 QKD
  - allow a malicious measurement device for Bob
  - extremely simple proof

Summary

- Capture "monogamy of entanglement" by a game
- Analyze this monogamy game, and show:
  - winning probability is exponentially small
  - strong parallel repetition in some cases
- Application I: to BB84 QKD
  - allow a malicious measurement device for Bob
  - extremely simple proof
- Application II: to position-based quantum crypto
  - first 1-round position-verification scheme

- Post-Doc and PhD positions are available at CQT in Singapore: http://www.quantumlah.org/openings/

- Our group homepage: http://quantuminfo.quantumlah.org/contact.html

- Post-Doc and PhD positions are available at CQT in Singapore: http://www.quantumlah.org/openings/

- Our group homepage: http://quantuminfo.quantumlah.org/contact.html

THANK YOU