Complete Insecurity of Quantum Protocols for Classical Two-Party Computation

Matthias Christandl (ETH Zurich)
joint work with
Harry Buhrman (CWI, University of Amsterdam)
Christian Schaffner (University of Amsterdam, CWI)

arXiv:1201.0849, Phys. Rev. Lett. 109, 160501 (2012)

Complete Insecurity of Quantum Protocols for Classical Two-Party Computation

Matthias Christandl (ETH Zurich)
joint work with
Harry Buhrman (CWI, University of Amsterdam)
Christian Schaffner (University of Amsterdam, CWI)

thanks for reuse of slides :)

arXiv:1201.0849, Phys. Rev. Lett. 109, 160501 (2012)

Motivation

- ideally

Motivation

- ideally

f

Motivation

- ideally

$$x \longrightarrow \boxed{f} \longleftarrow y$$

Motivation

- ideally

x	$\longrightarrow$	f	$\longleftarrow$	y
$f(x,y)$	$\longleftarrow$		$\longrightarrow$	$f(x,y)$

Motivation

- ideally

x → f ← y

f(x,y) ← f → f(x,y)

e.g.: Yao's millionaires' problem: ≤

Motivation

- ideally

x → f ← y

f(x,y) ← f → f(x,y)

e.g.: Yao's millionaires' problem: ≤

- reality

Motivation

- ideally

x → f ← y

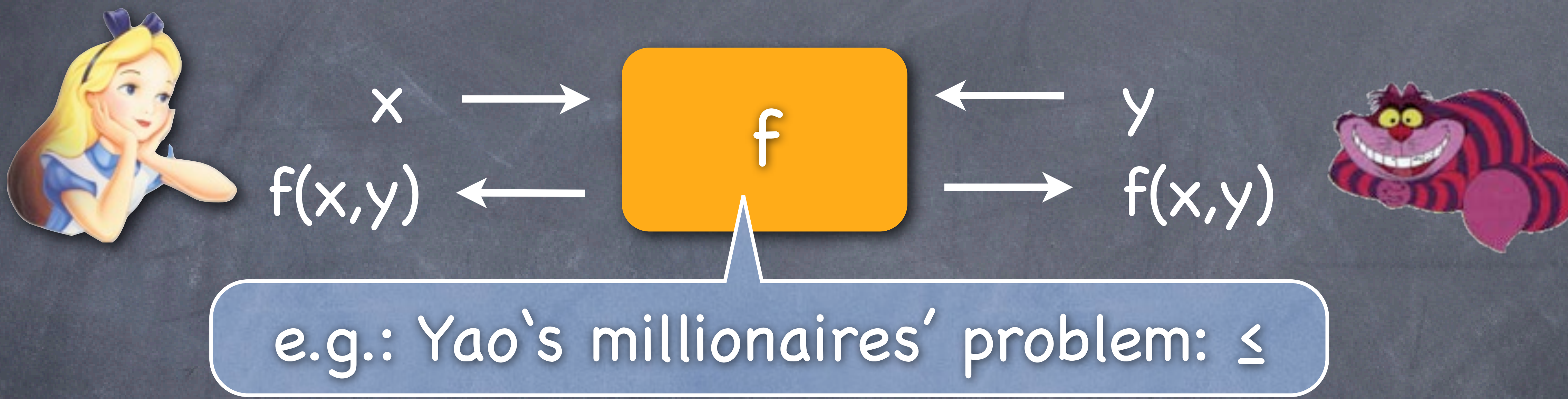
f(x,y) ← f → f(x,y)

e.g.: Yao's millionaires' problem: ≤

- reality

Motivation

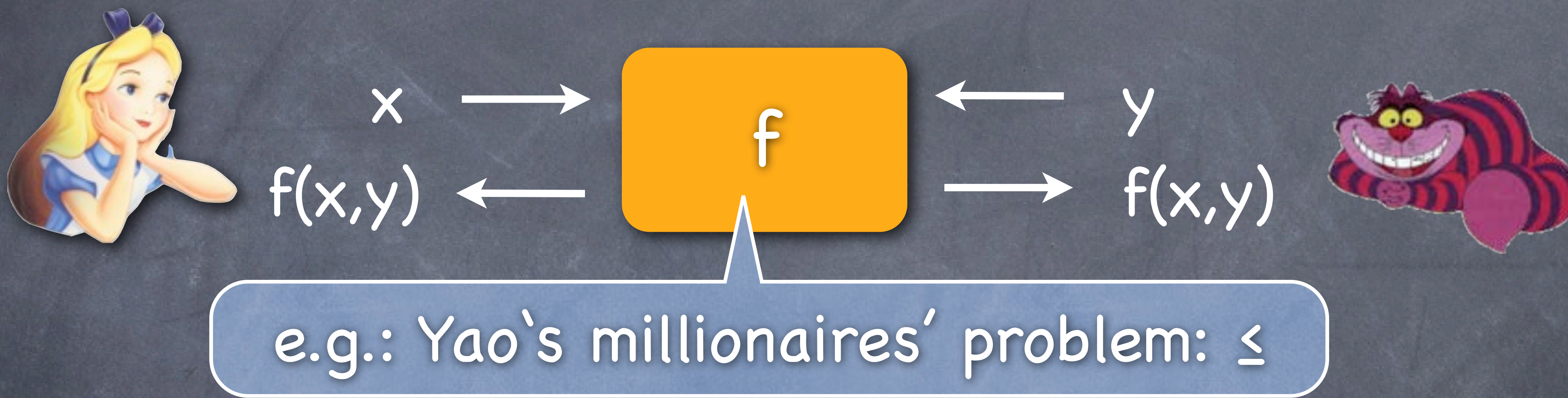
- ideally



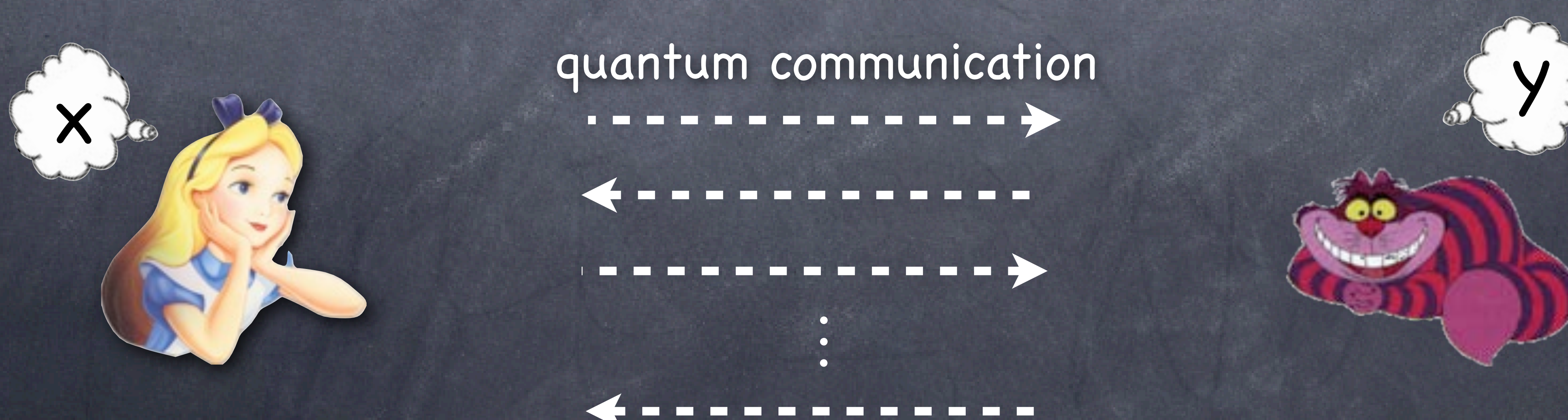
- reality

Motivation

- ideally

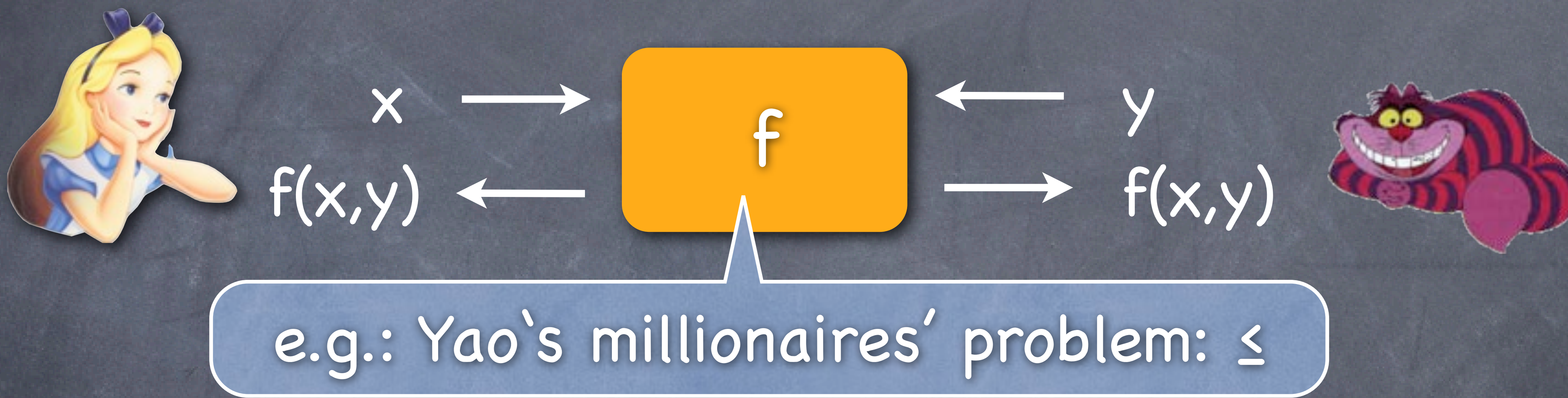


- reality

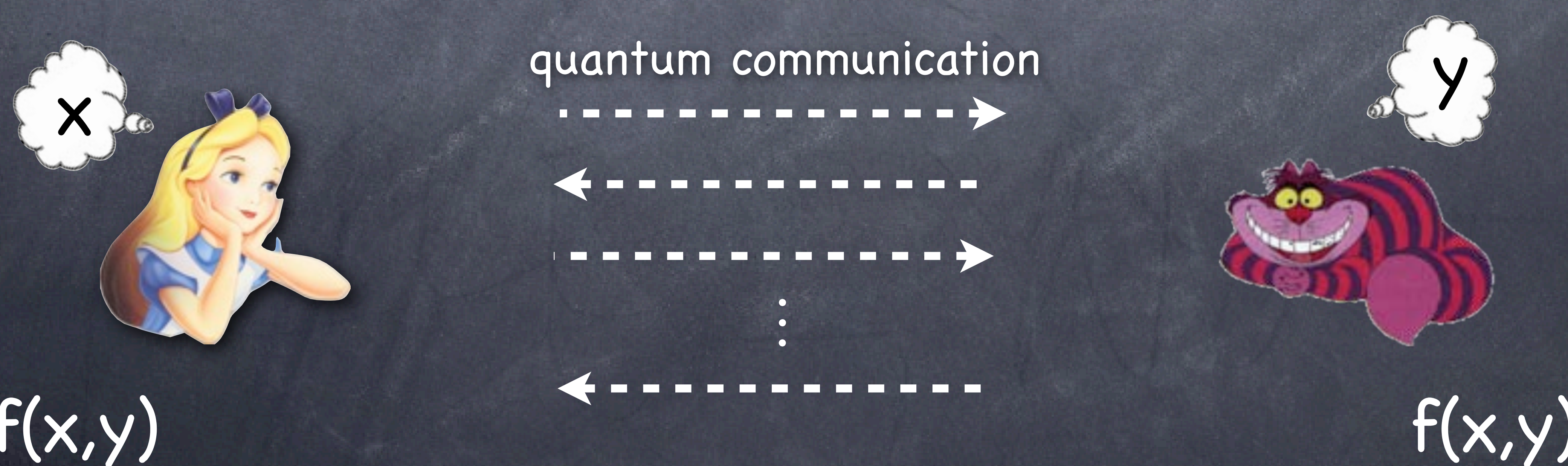


Motivation

- ideally



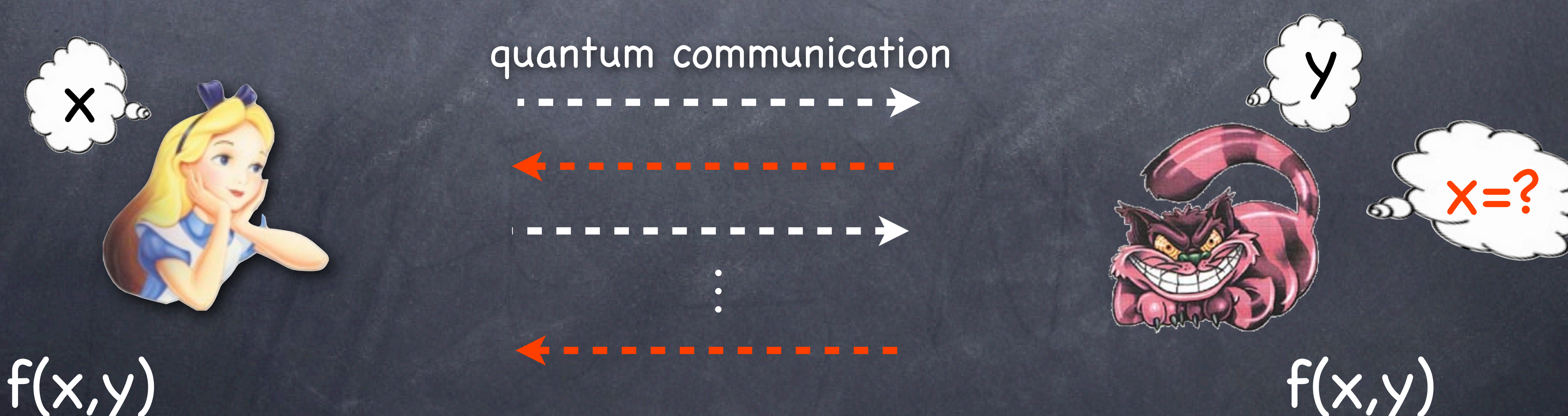
- reality



Motivation

- ideally

- reality



Secure Function Evaluation

- ideally

Secure Function Evaluation

- ideally

x $\longrightarrow$ **f** $\longleftarrow$ y

f(x,y) $\longleftarrow$ **f** $\longrightarrow$ f(x,y)

- goal: come up with protocols that are

Secure Function Evaluation

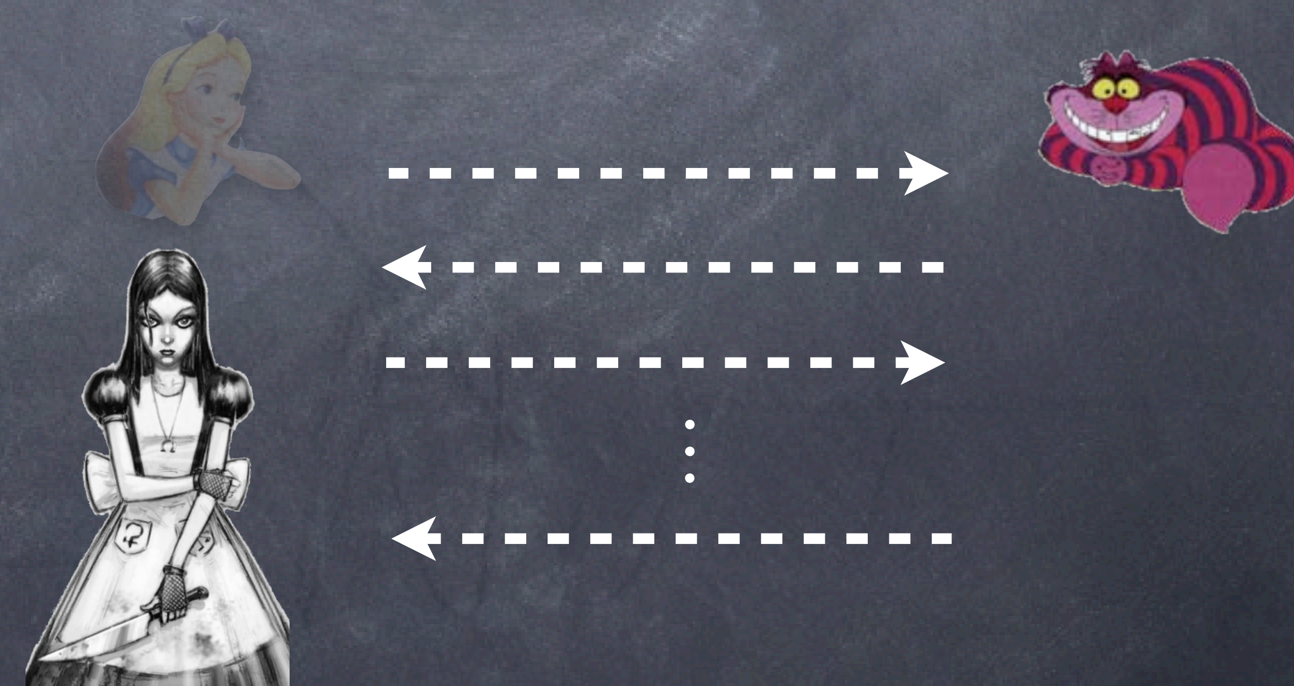
- ideally

- goal: come up with protocols that are
  - correct

Secure Function Evaluation

- ideally

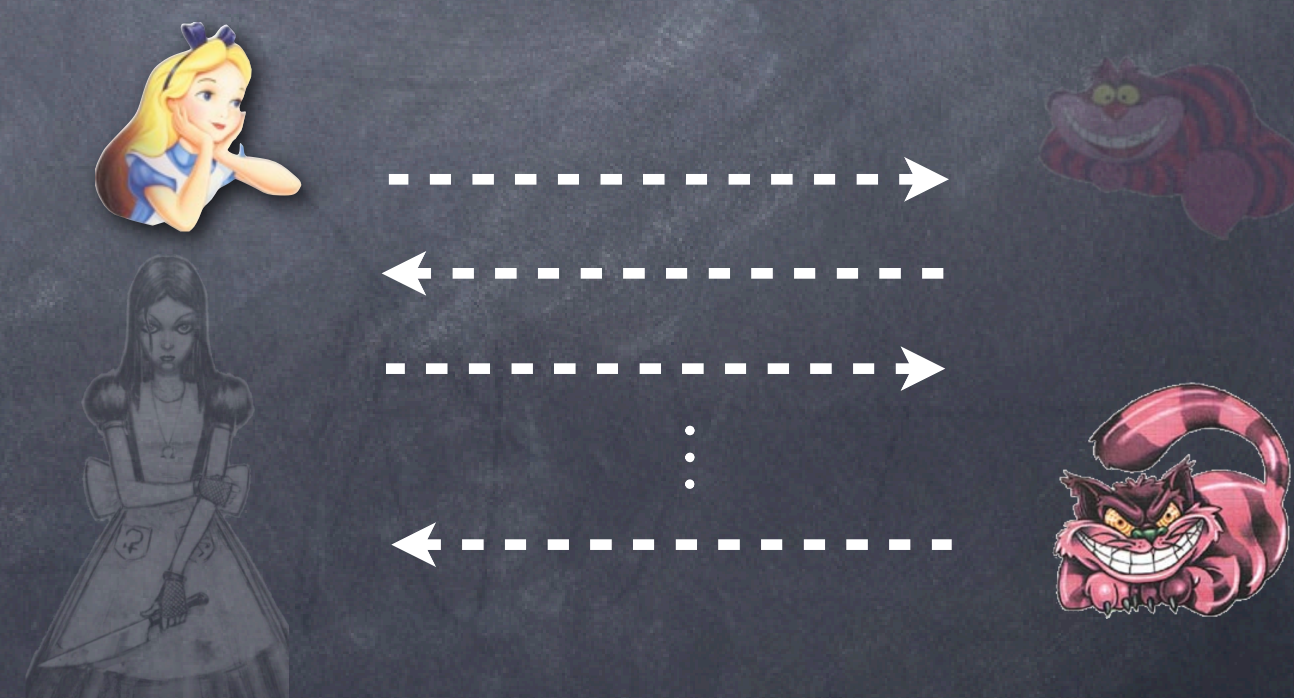
- goal: come up with protocols that are
  - correct
  - secure against dishonest Alice



Secure Function Evaluation

- ideally

- goal: come up with protocols that are
  - correct
  - secure against dishonest Alice
  - secure against dishonest Bob

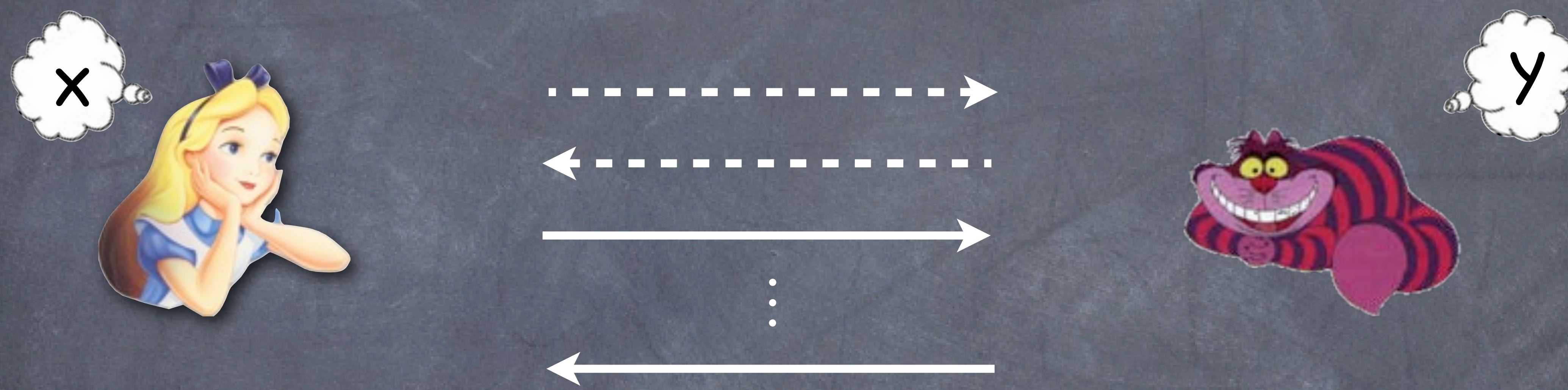


Main Result

- **Theorem**: If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.

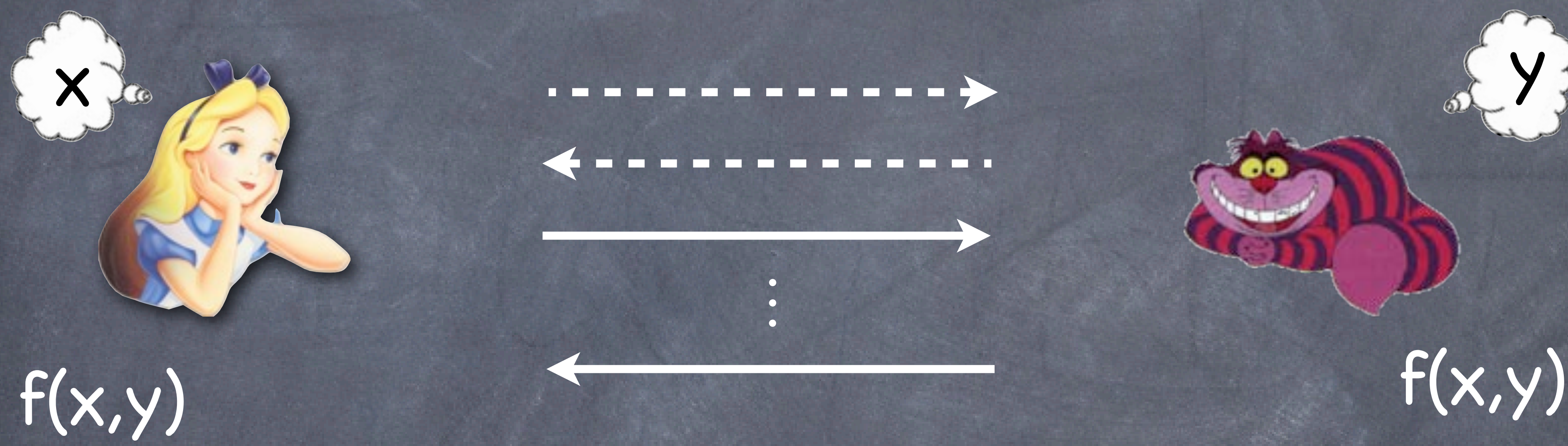
Main Result

- **Theorem:** If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



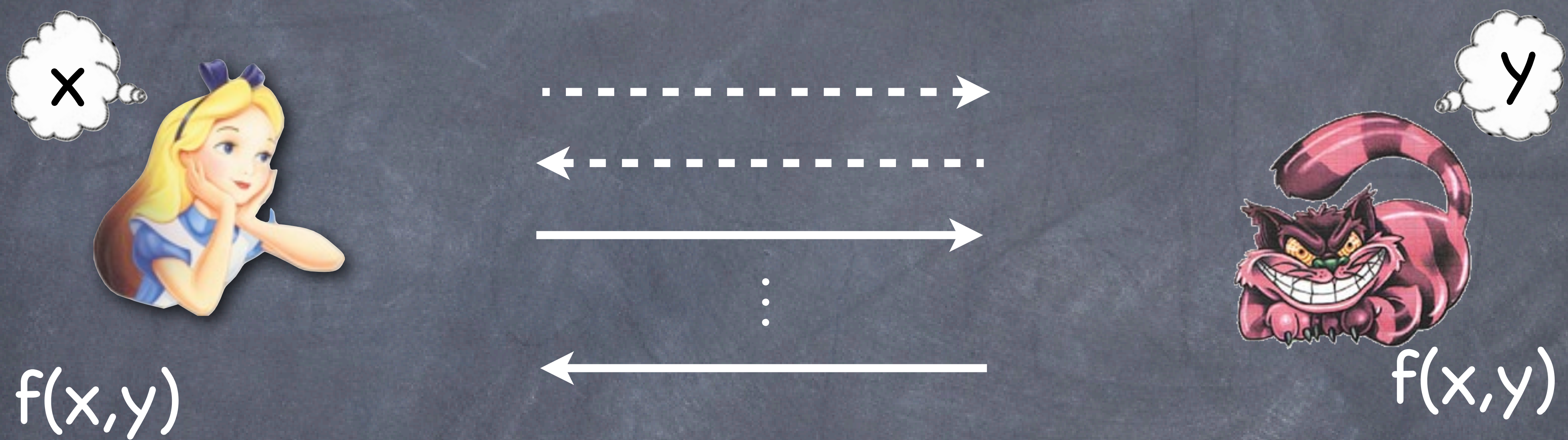
Main Result

- **Theorem**: If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



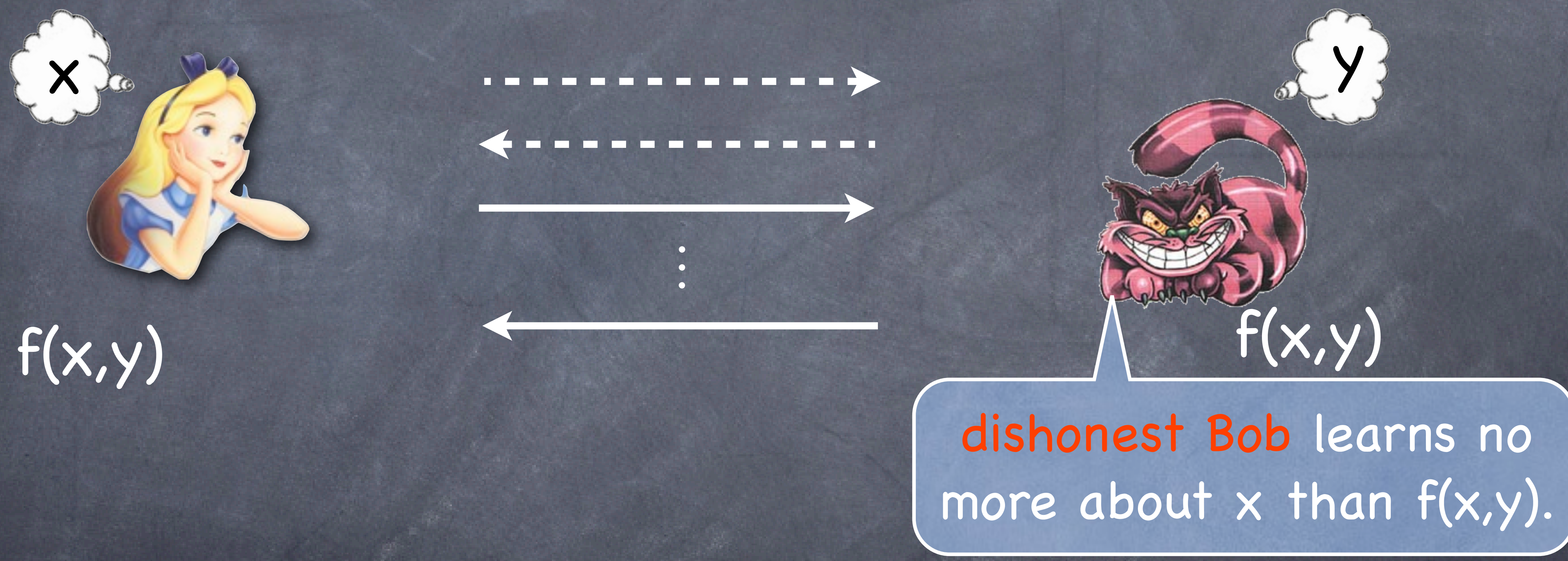
Main Result

- **Theorem**: If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



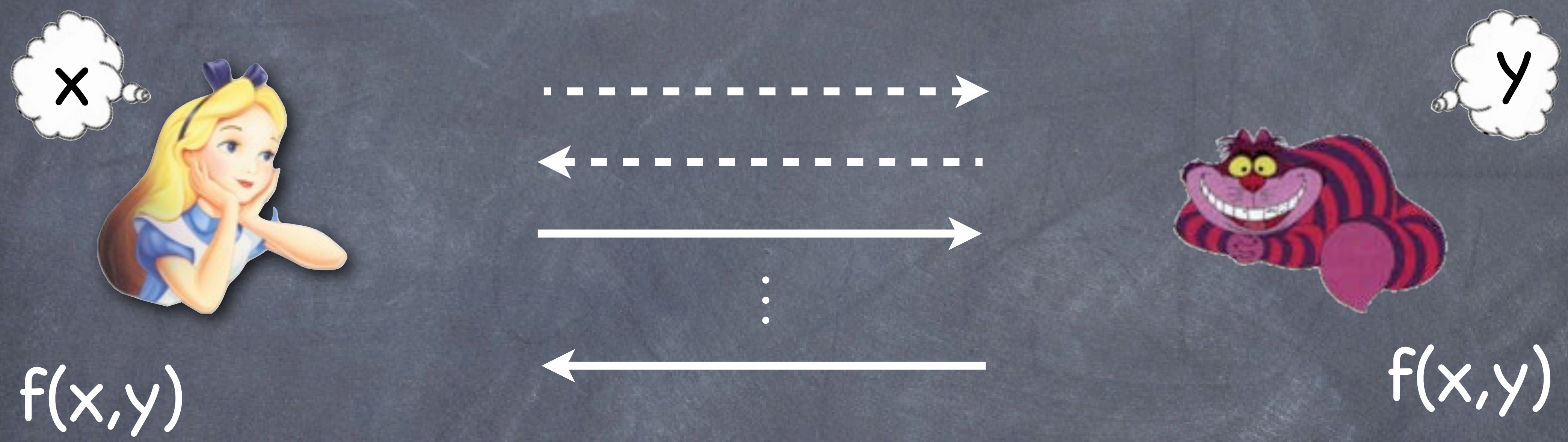
Main Result

- **Theorem:** If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



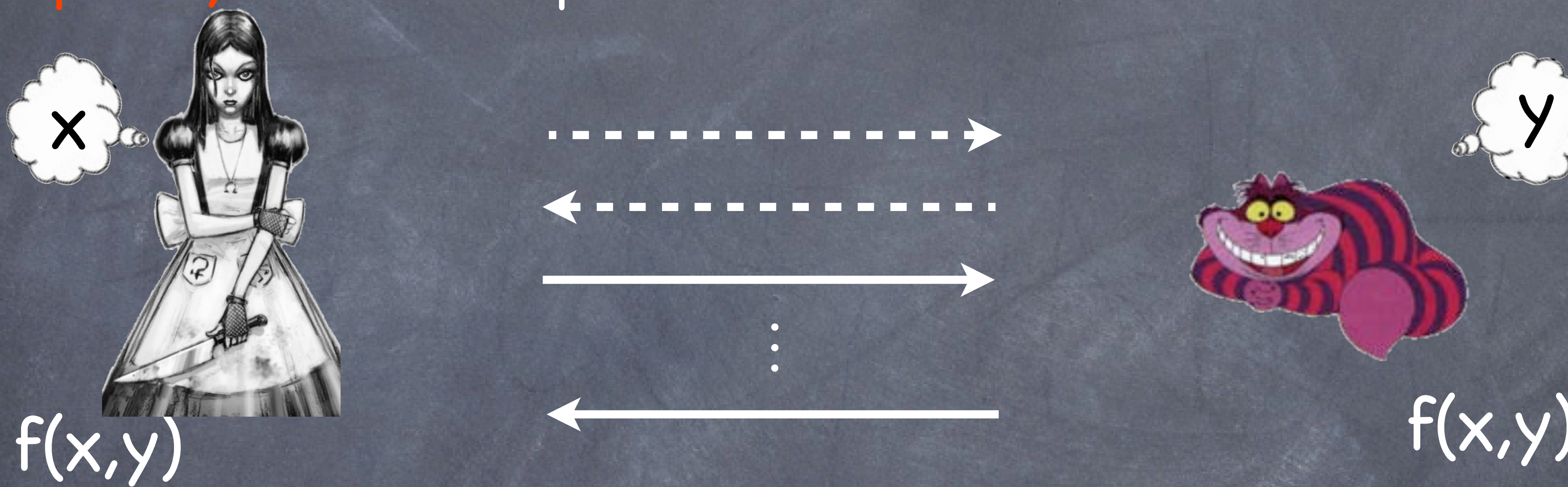
Main Result

- **Theorem**: If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



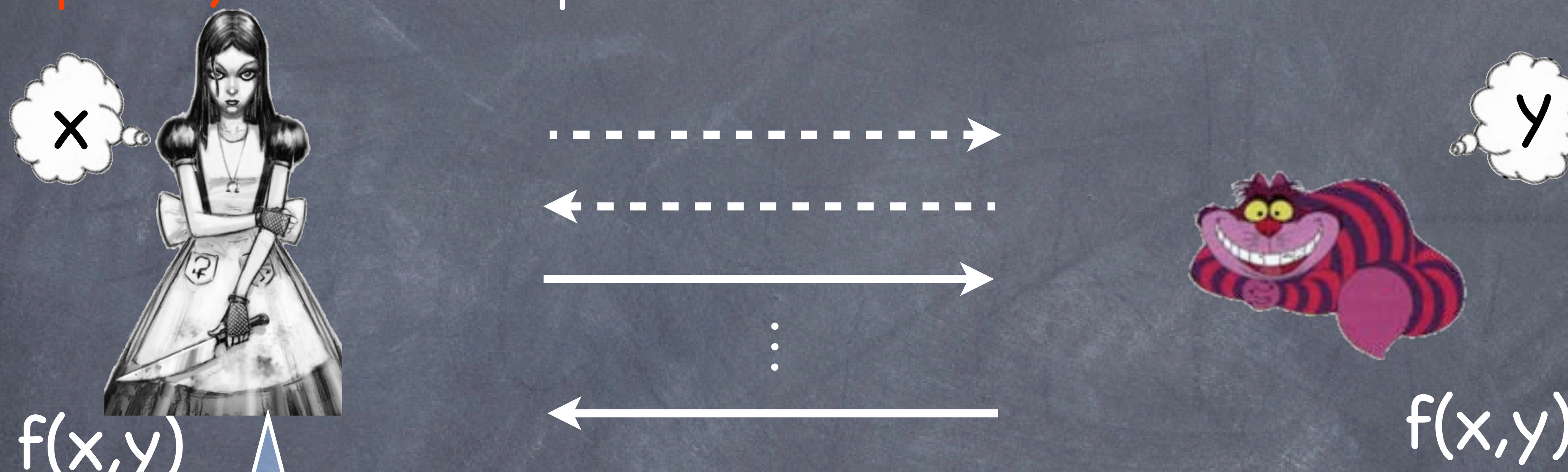
Main Result

- **Theorem**: If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



Main Result

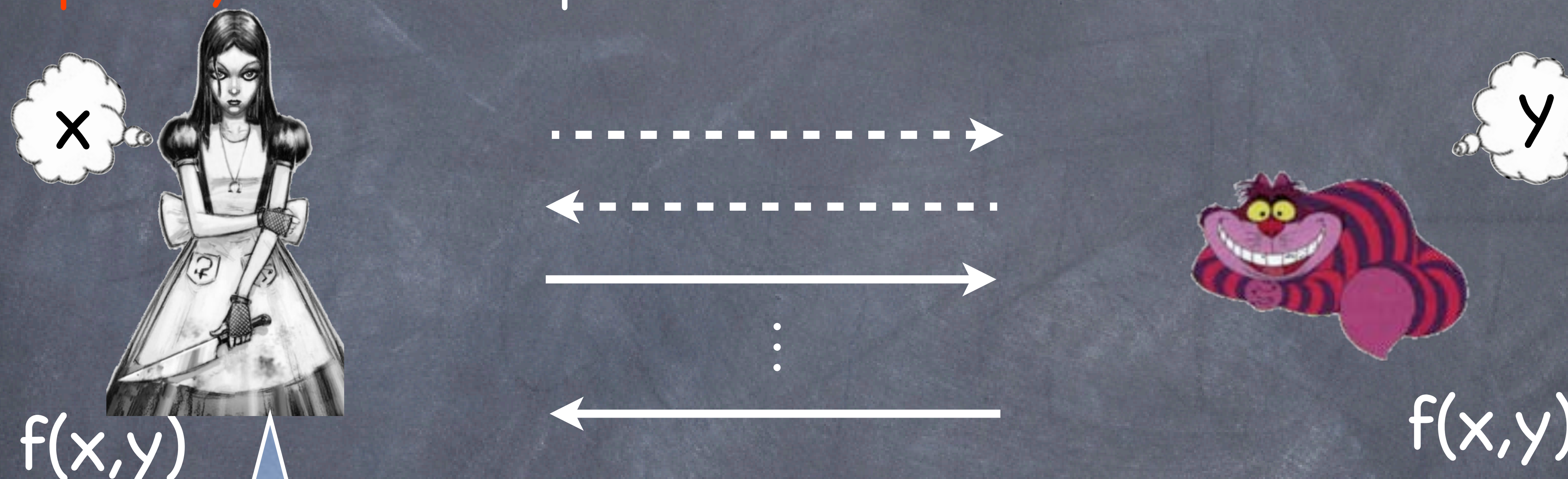
- **Theorem**: If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



dishonest Alice can compute
f(x,y) not just for one x, but for all x.
Equivalently, she obtains y‘ s.th.
f(x,y‘)=f(x,y) for all x

Main Result

- **Theorem:** If a quantum protocol for the evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



dishonest Alice can compute
f(x,y) not just for one x, but for all x.
Equivalently, she obtains y` s.th.
f(x,y`)=f(x,y) for all x

- **Theorem:** If a quantum protocol for the evaluation of f is ε-correct and ε-secure against Bob, then Alice can break the protocol with probability 1-O(ε).

History

History

- ~1970: Conjugate Coding [Wiesner]

History

- ~1970: Conjugate Coding [Wiesner]
- 1984: Quantum Key Distribution [Bennett Brassard]
  Bit Commitment and Oblivious Transfer?

History

- ~1970: Conjugate Coding [Wiesner]
- 1984: Quantum Key Distribution [Bennett Brassard]
  Bit Commitment and Oblivious Transfer?
- 1997: No Bit Commitment [Lo Chau, Mayers]

History

- ~1970: Conjugate Coding [Wiesner]
- 1984: Quantum Key Distribution [Bennett Brassard]
  Bit Commitment and Oblivious Transfer?
- 1997: No Bit Commitment [Lo Chau, Mayers]
- 1997: No One-Sided Secure Computation [Lo]

History

- ~1970: Conjugate Coding [Wiesner]
- 1984: Quantum Key Distribution [Bennett Brassard]
  Bit Commitment and Oblivious Transfer?
- 1997: No Bit Commitment [Lo Chau, Mayers]
- 1997: No One-Sided Secure Computation [Lo]
- 2007, 2009: Quantum Protocols leak more than allowed [Colbeck], [Salvail Sotakova Schaffner]

History

- ~1970: Conjugate Coding [Wiesner]
- 1984: Quantum Key Distribution [Bennett Brassard]
  Bit Commitment and Oblivious Transfer?
- 1997: No Bit Commitment [Lo Chau, Mayers]
- 1997: No One-Sided Secure Computation [Lo]
- 2007, 2009: Quantum Protocols leak more than allowed [Colbeck], [Salvail Sotakova Schaffner]
- this work: Complete Insecurity of Two-Sided Secure Function Evaluation (also with finite error)

Talk Outline

Talk Outline

- explain Lo's impossibility proof

Talk Outline

- explain Lo's impossibility proof
- problem with two-sided computation

Talk Outline

- explain Lo's impossibility proof
- problem with two-sided computation
- security definition

Talk Outline

- explain Lo's impossibility proof
- problem with two-sided computation
- security definition
- impossibility proof

Talk Outline

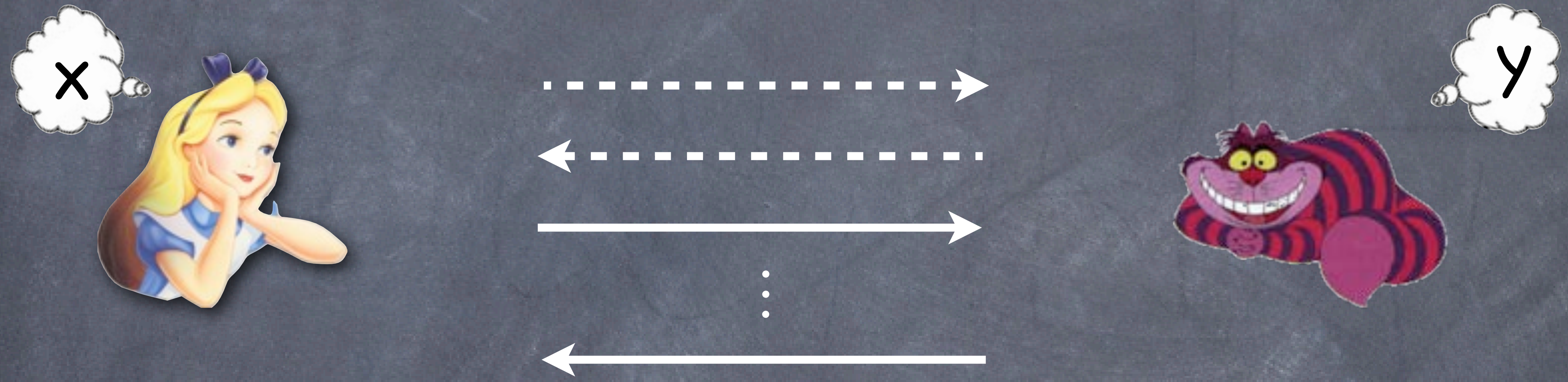
- explain Lo's impossibility proof
- problem with two-sided computation
- security definition
- impossibility proof
- conclusion

Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.

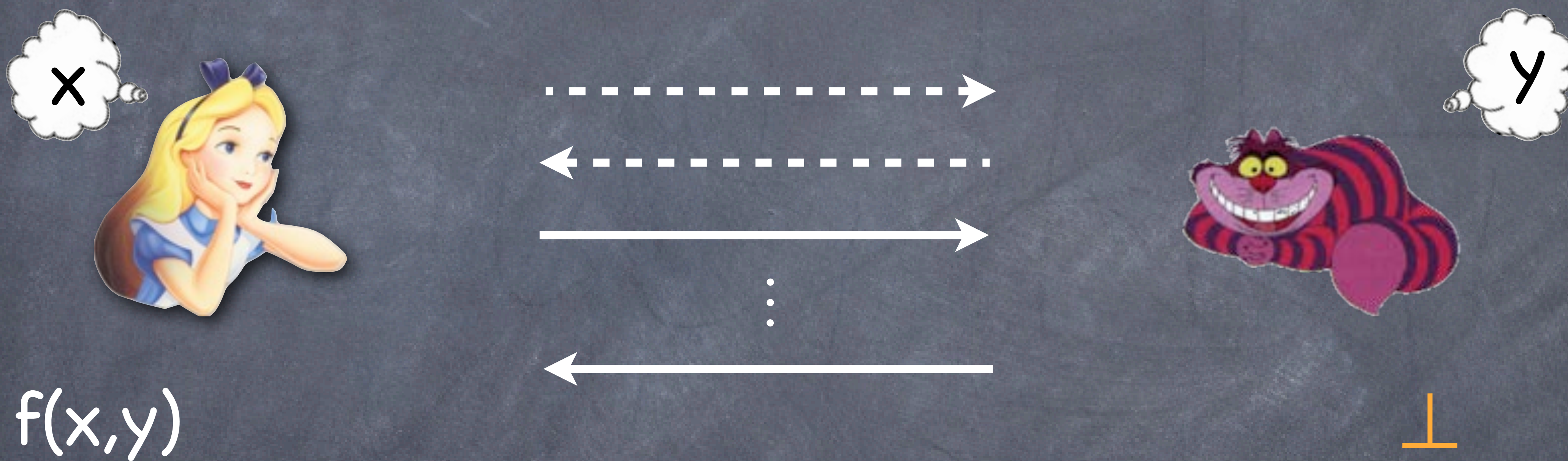
Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



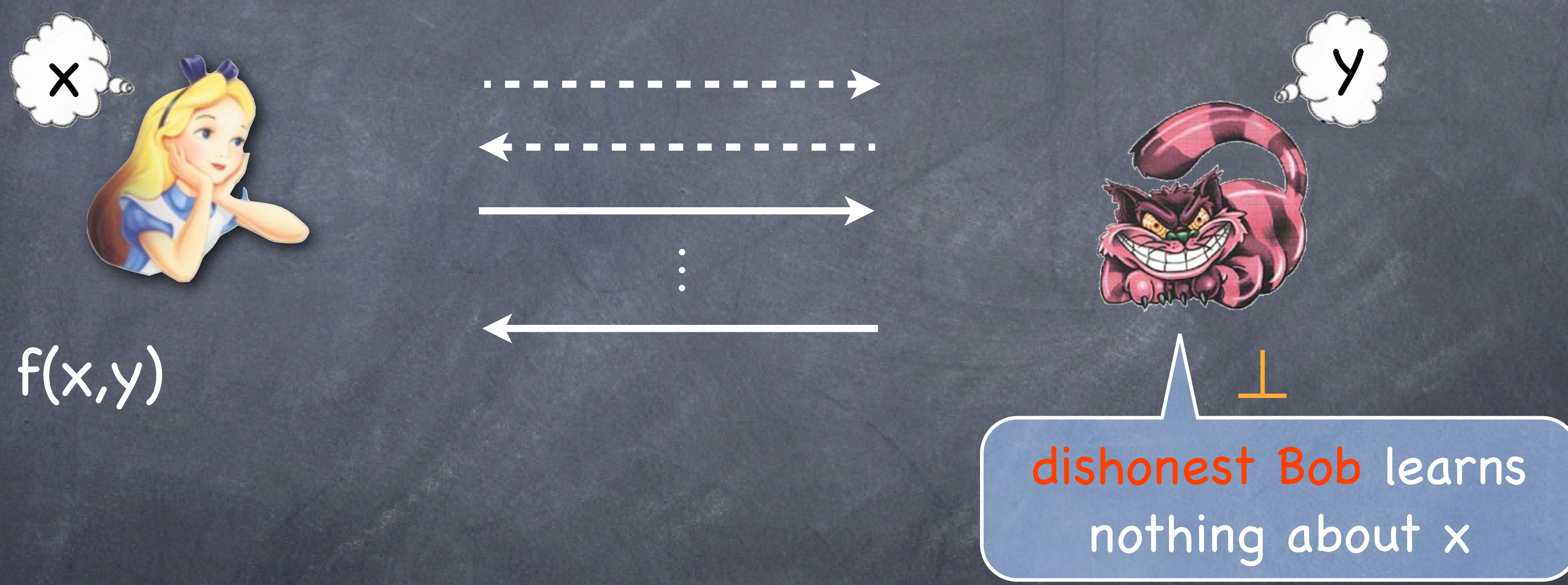
Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



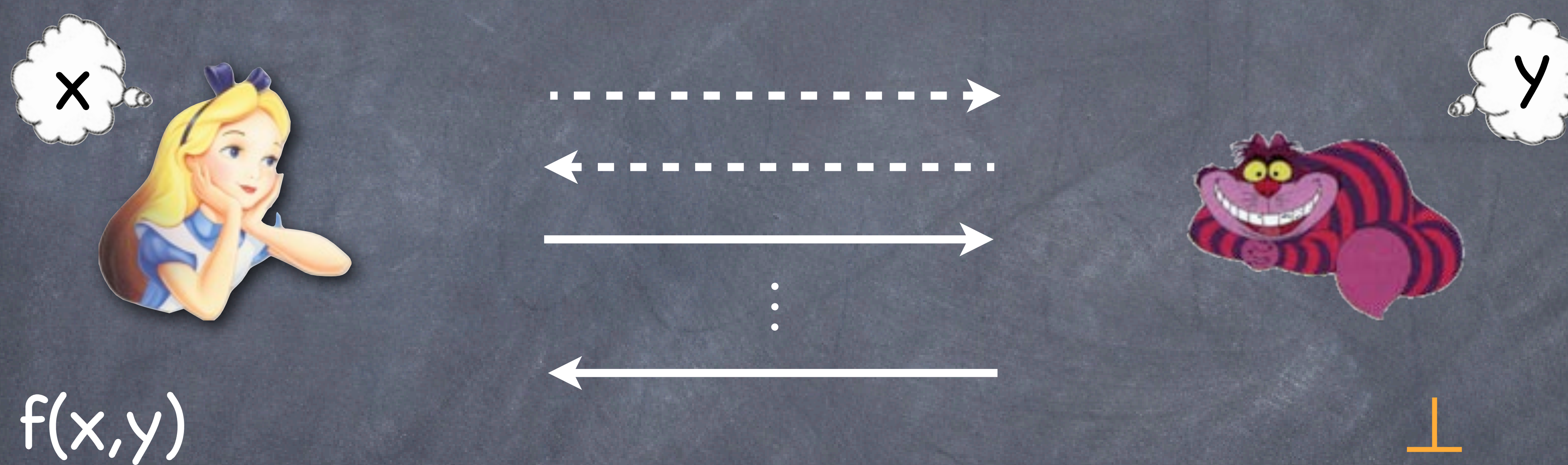
Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



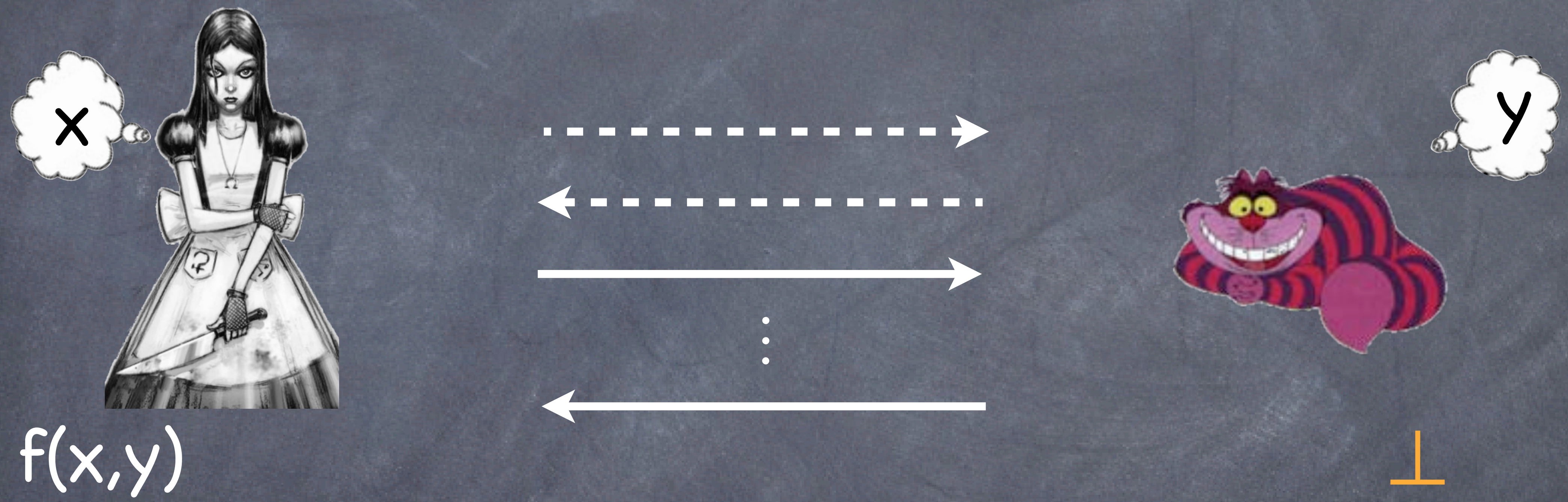
Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



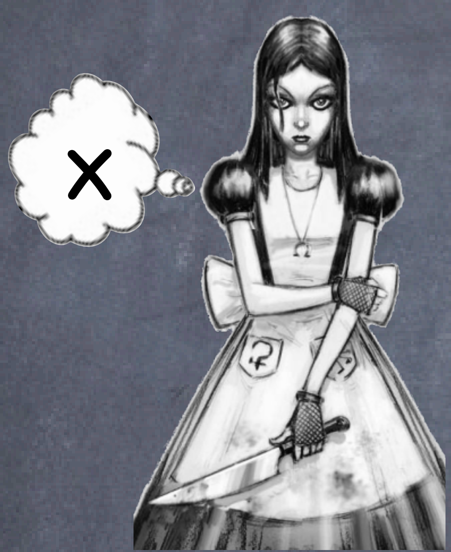
Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



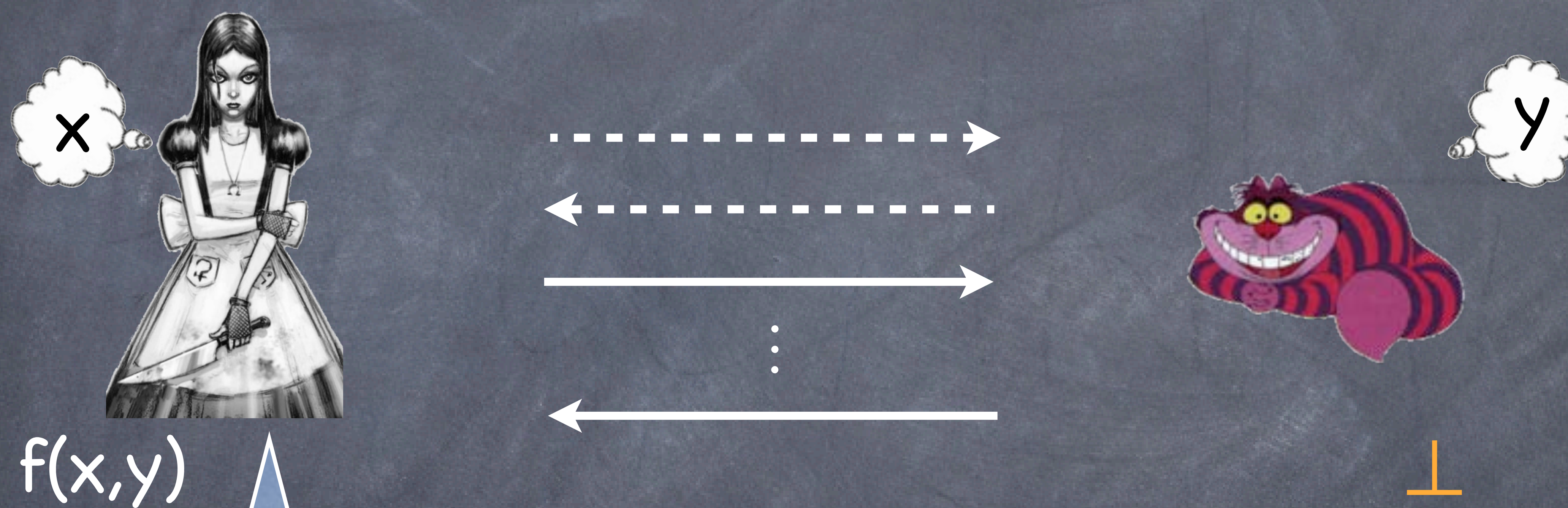
f(x,y)

$\perp$

dishonest Alice can compute f(x,y) not just for one x, but for all x.

Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.

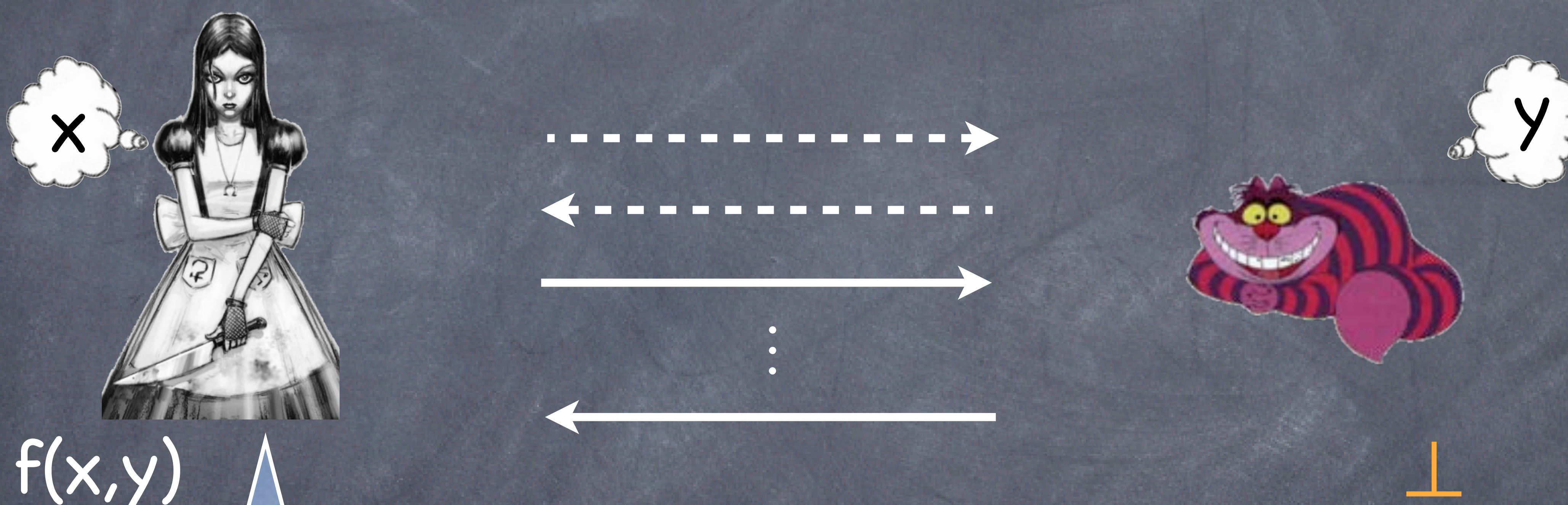


dishonest Alice can compute f(x,y) not just for one x, but for all x.

- proof fails for two-sided computations

Lo's Result

- **Theorem**: If a quantum protocol for the one-sided evaluation of f is correct and perfectly secure against Bob, then Alice can completely break the protocol.



dishonest Alice can compute f(x,y) not just for one x, but for all x.

- proof fails for two-sided computations
- error increases with number of inputs

Lo's Proof

Lo's Proof

Lo's Proof

$f(x,y)$ $\perp$

- only Alice gets output

Lo's Proof

f(x,y) $\quad|\psi^{x,y}\rangle_{AB}\quad$ $\perp$

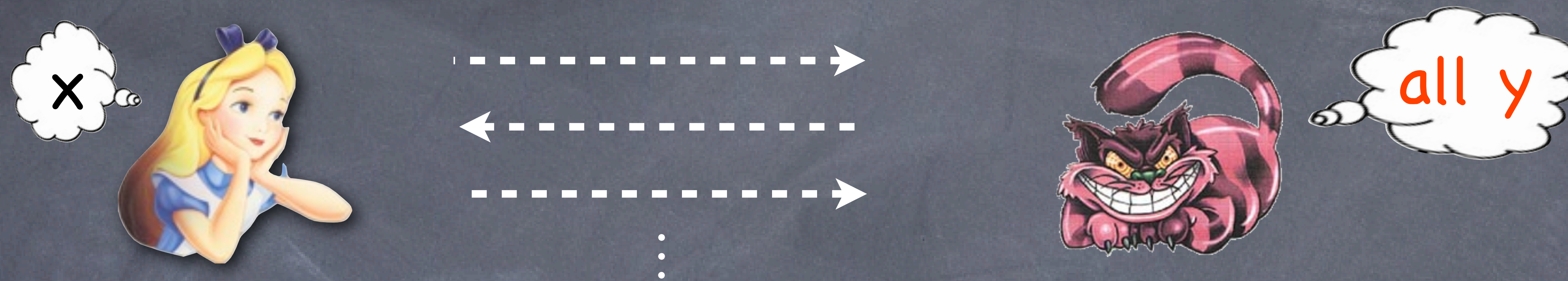
- only Alice gets output
- wlog measurements are moved to the end, final state is pure

Lo's Proof

f(x,y) $\qquad |\psi^{x,y}\rangle_{AB} \qquad \perp$

- only Alice gets output
- wlog measurements are moved to the end, final state is pure

Lo's Proof



f(x,y) $\quad |\psi^{x,y}\rangle_{AB} \quad \perp$

- only Alice gets output
- wlog measurements are moved to the end, final state is pure
- dishonest Bob inputs superposition

$$|\psi^{x_0}\rangle_{AB} = \sum_y |\psi^{x_0,y}\rangle_{AB_1} |y\rangle_{B_2}$$

Lo's Proof

f(x,y) $\qquad |\psi^{x,y}\rangle_{AB} \qquad \perp$

- only Alice gets output
- wlog measurements are moved to the end, final state is pure
- dishonest Bob inputs superposition

$$|\psi^{x_0}\rangle_{AB} = \sum_y |\psi^{x_0,y}\rangle_{AB_1} |y\rangle_{B_2}$$

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

Lo's Proof

f(x,y) $\qquad |\psi^{x,y}\rangle_{AB} \qquad \perp$

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

Lo's Proof

f(x,y) $\qquad |\psi^{x,y}\rangle_{AB} \qquad \perp$

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

- implies existence of cheating unitary for Alice: (not dep on y)

$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0}\rangle_{AB} = |\psi^{x_1}\rangle_{AB}$$

Lo's Proof

f(x,y) $\quad |\psi^{x,y}\rangle_{AB} \quad \perp$

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

$$|\psi^{x_0}\rangle_{AB} = \sum_y |\psi^{x_0,y}\rangle_{AB_1} |y\rangle_{B_2}$$

- implies existence of cheating unitary for Alice: (not dep on y)

$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0}\rangle_{AB} = |\psi^{x_1}\rangle_{AB}$$

Lo's Proof

$\vdots$

f(x,y) $\qquad |\psi^{x,y}\rangle_{AB} \qquad \perp$

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

$$|\psi^{x_0}\rangle_{AB} = \sum_y |\psi^{x_0,y}\rangle_{AB_1}|y\rangle_{B_2}$$

- implies existence of cheating unitary for Alice: (not dep on y)

$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0}\rangle_{AB} = |\psi^{x_1}\rangle_{AB}$$

$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0,y}\rangle_{AB} = |\psi^{x_1,y}\rangle_{AB}$$

Lo's Proof

$\vdots$

f(x,y) $\quad |\psi^{x,y}\rangle_{AB} \quad \perp$

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

$$|\psi^{x_0}\rangle_{AB} = \sum_y |\psi^{x_0,y}\rangle_{AB_1} |y\rangle_{B_2}$$

- implies existence of cheating unitary for Alice: (not dep on y)

$$(U_A \otimes \mathbb{I}_B)\, |\psi^{x_0}\rangle_{AB} = |\psi^{x_1}\rangle_{AB}$$

$$(U_A \otimes \mathbb{I}_B)\, |\psi^{x_0,y}\rangle_{AB} = |\psi^{x_1,y}\rangle_{AB}$$

Lo's Proof

$\vdots$

f(x,y) $\qquad |\psi^{x,y}\rangle_{AB} \qquad \perp$

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

$$|\psi^{x_0}\rangle_{AB} = \sum_y |\psi^{x_0,y}\rangle_{AB_1} |y\rangle_{B_2}$$

- implies existence of cheating unitary for Alice: (not dep on y)

$$(U_A \otimes \mathbb{I}_B)\, |\psi^{x_0}\rangle_{AB} = |\psi^{x_1}\rangle_{AB}$$
$$(U_A \otimes \mathbb{I}_B)\, |\psi^{x_0,y}\rangle_{AB} = |\psi^{x_1,y}\rangle_{AB}$$

- dishonest Alice: input x_0 -> f(x_0,y), switches to x_1 -> f(x_1,y) ...

Lo's Proof

$\vdots$

f(x_0,y), f(x_1,y), ... $|\psi^{x,y}\rangle_{AB}$ f(x,y)

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

$$|\psi^{x_0}\rangle_{AB} = \sum_y |\psi^{x_0,y}\rangle_{AB_1}|y\rangle_{B_2}$$

- implies existence of cheating unitary for Alice: (not dep on y)

$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0}\rangle_{AB} = |\psi^{x_1}\rangle_{AB}$$
$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0,y}\rangle_{AB} = |\psi^{x_1,y}\rangle_{AB}$$

- dishonest Alice: input x_0 -> f(x_0,y), switches to x_1 -> f(x_1,y) ...

Lo's Proof

$f(x_0,y)$, $f(x_1,y)$, ... $\quad |\psi^{x,y}\rangle_{AB} \quad$ $f(x,y)$

- security against dishonest Bob:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

$$|\psi^{x_0}\rangle_{AB} = \sum_y |\psi^{x_0,y}\rangle_{AB_1}|y\rangle_{B_2}$$

- implies existence of cheating unitary for Alice: (not dep on y)

$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0}\rangle_{AB} = |\psi^{x_1}\rangle_{AB}$$

$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0,y}\rangle_{AB} = |\psi^{x_1,y}\rangle_{AB}$$

- dishonest Alice: input x_0 -> $f(x_0,y)$, switches to x_1 -> $f(x_1,y)$ ...

$\square$

Lo's Proof

f(x,y) $\quad |\psi^{x,y}\rangle_{AB} \quad \perp$

- security against dishonest Bob without output:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

Lo's Proof

f(x,y) $\quad |\psi^{x,y}\rangle_{AB} \quad \perp$

- security against dishonest Bob without output:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

crucial step!

Lo's Proof

f(x,y) $\quad |\psi^{x,y}\rangle_{AB}$ $\quad$ f(x,y)

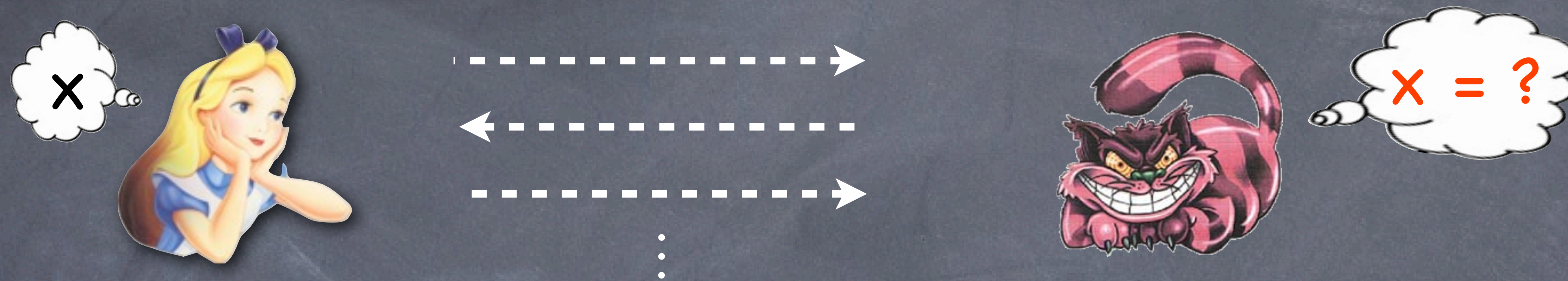
- security against dishonest Bob without output:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

crucial step!

- what if Bob has f(x,y) ? In general $\rho_B^{x_0} \neq \rho_B^{x_1}$

Lo's Proof



f(x,y) $\quad |\psi^{x,y}\rangle_{AB}$ $\quad$ f(x,y)

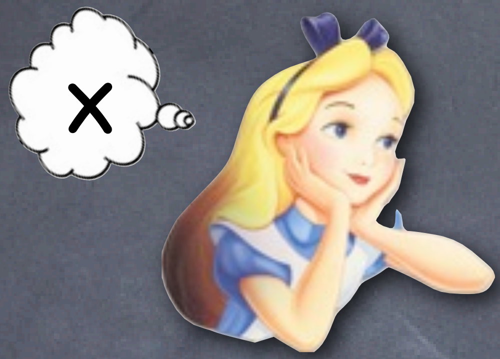
- security against dishonest Bob without output:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

crucial step!

- what if Bob has f(x,y) ? In general $\rho_B^{x_0} \neq \rho_B^{x_1}$
- precise formalisation of "not learning more about x than f(x,y)" ?

Lo's Proof



f(x,y) $\quad |\psi^{x,y}\rangle_{AB} \quad$ f(x,y)

- security against dishonest Bob without output:

$$\mathrm{tr}_A(|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = \rho_B^{x_1} = \mathrm{tr}_A(|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})$$

crucial step!

- what if Bob has f(x,y) ? In general $\rho_B^{x_0} \neq \rho_B^{x_1}$
- precise formalisation of
  "not learning more about x than f(x,y)" ?

use the real/ideal paradigm

Informal Security Definition

- we want

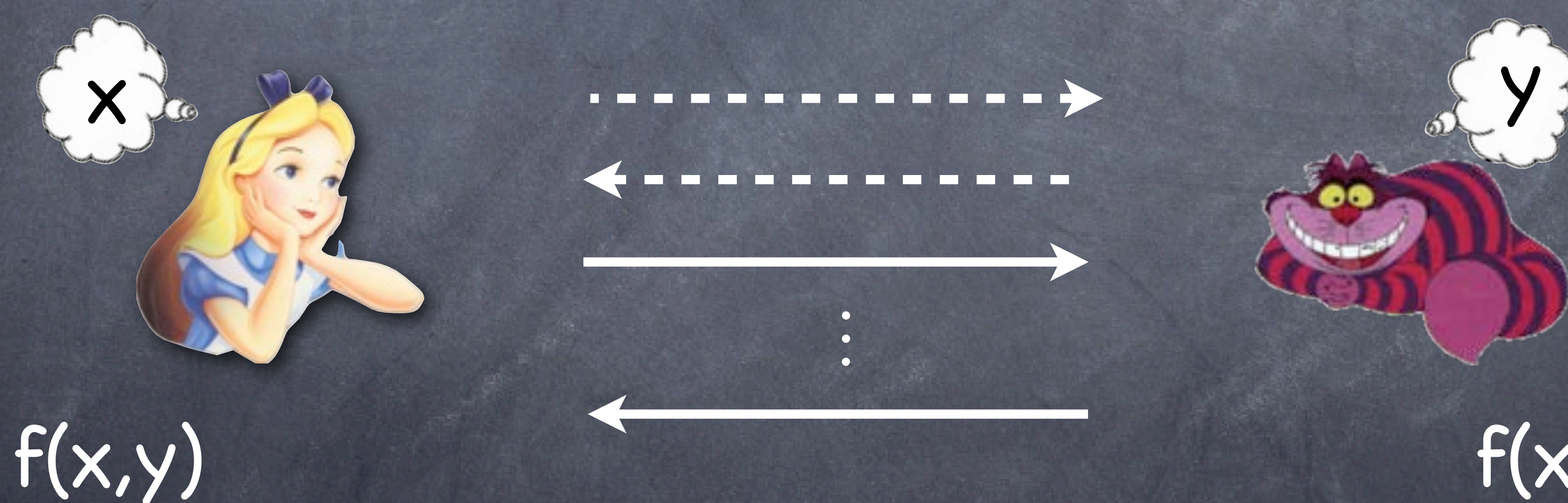
Informal Security Definition

- we want

Informal Security Definition

- we want

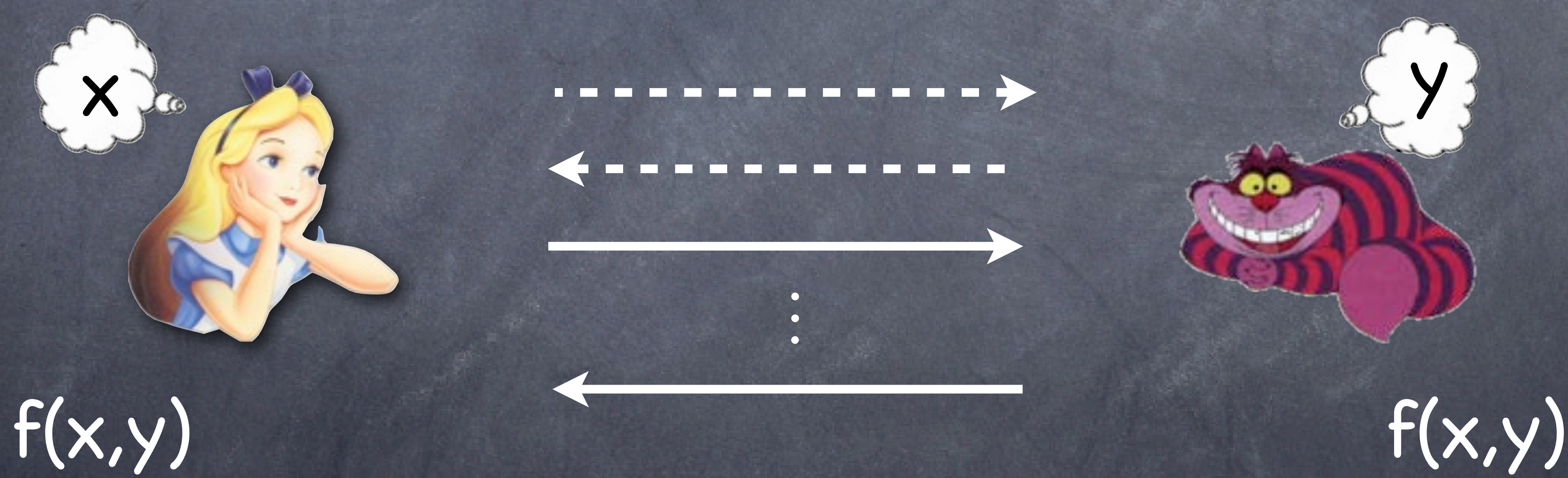
- we have



Informal Security Definition

- we want

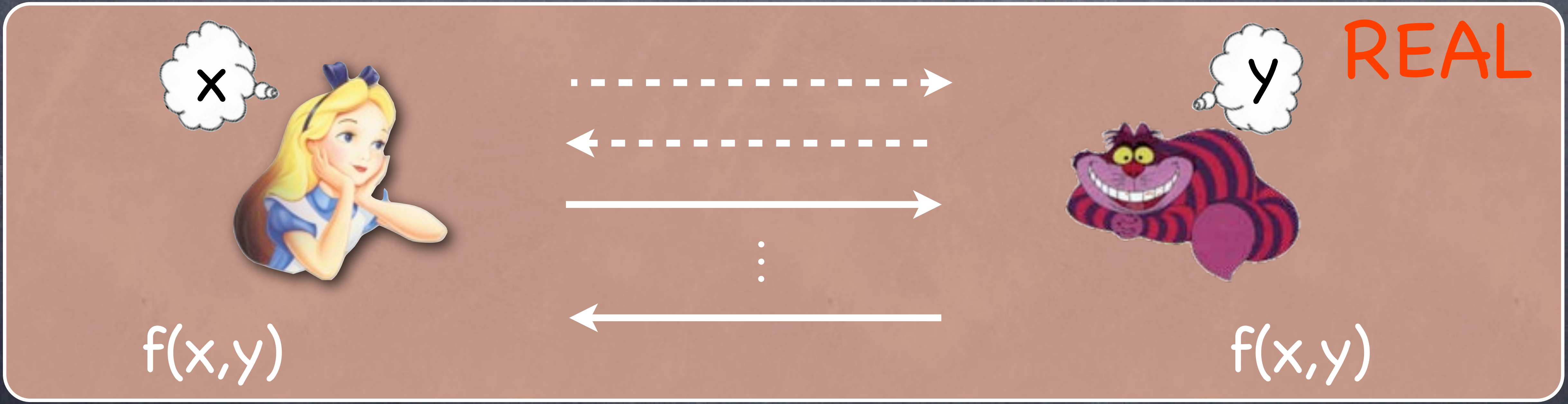
- we have



Informal Security Definition

- we want

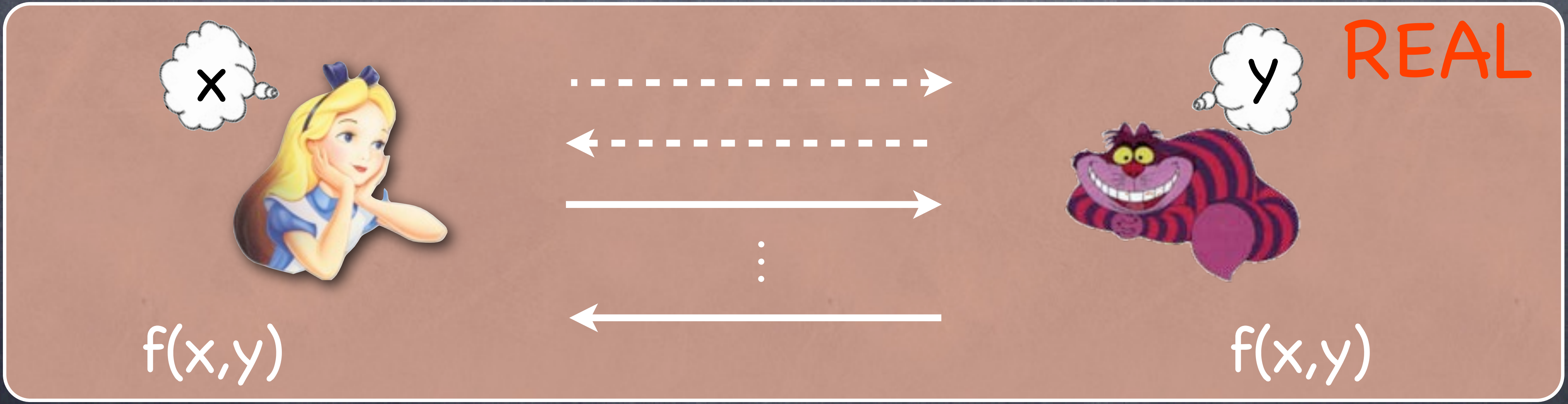
- we have



Informal Security Definition

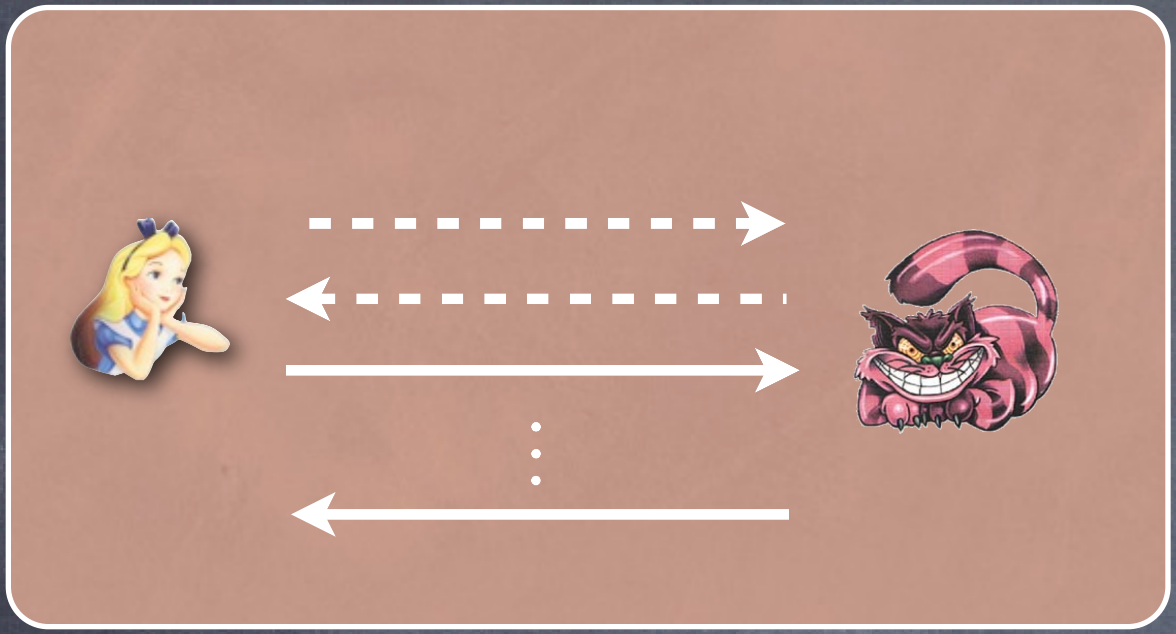
- we want

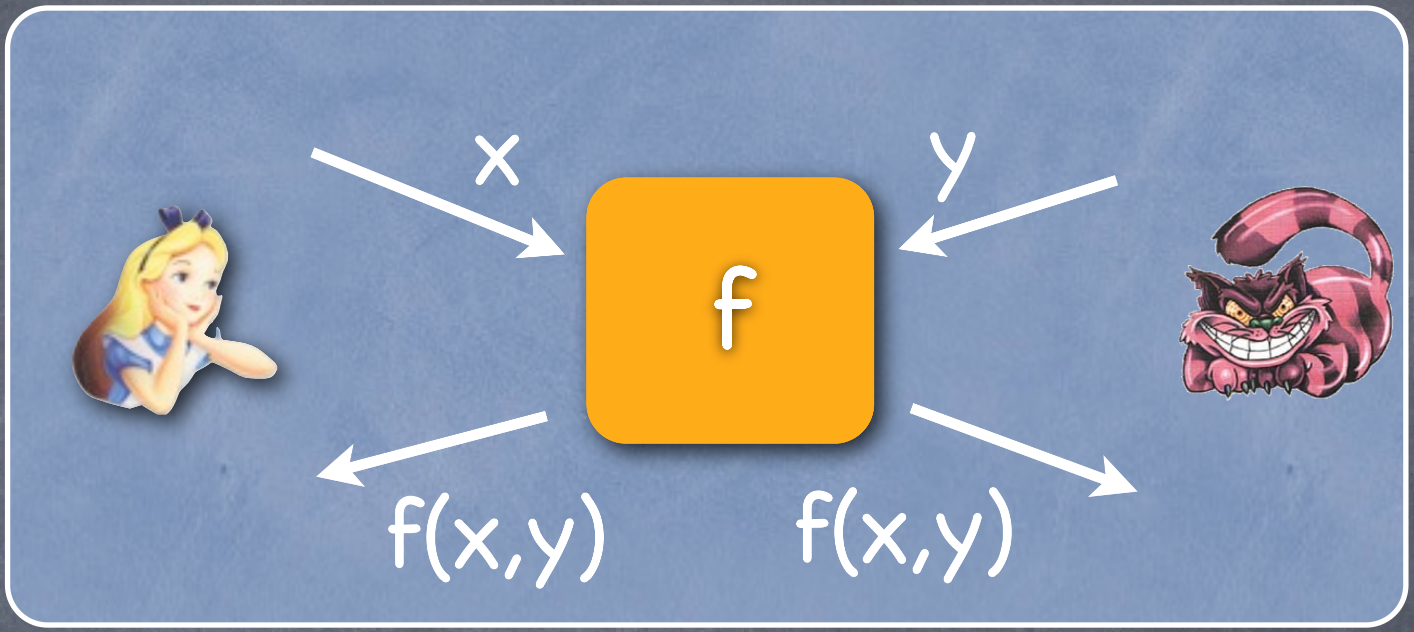
- we have



security holds if REAL looks like IDEAL to the outside world

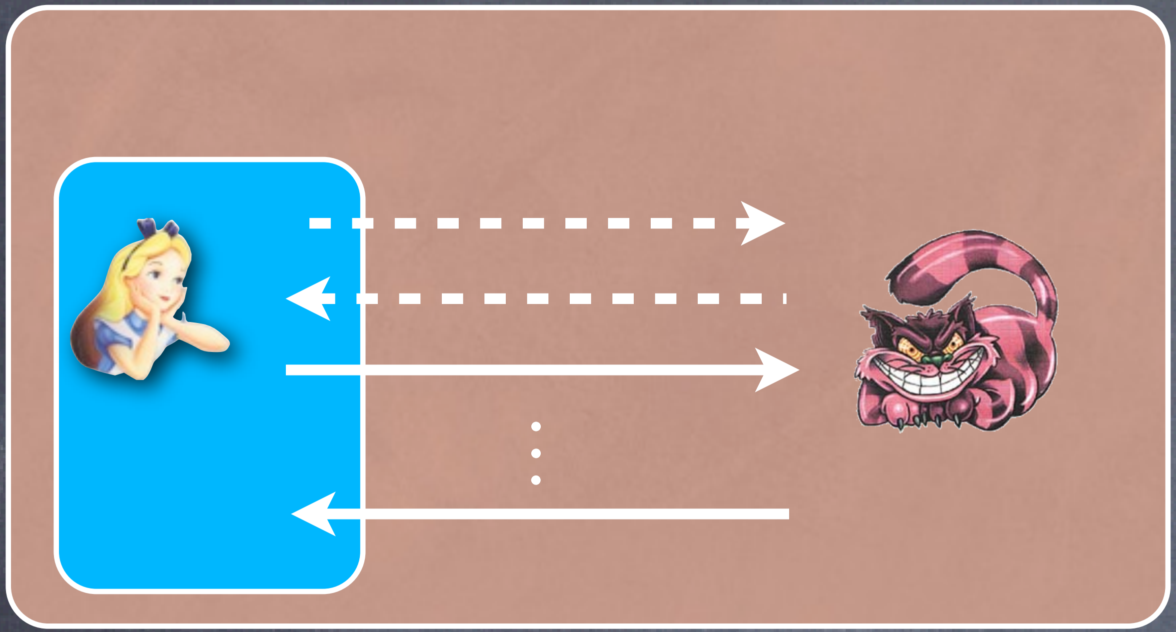
Formal Security Definition

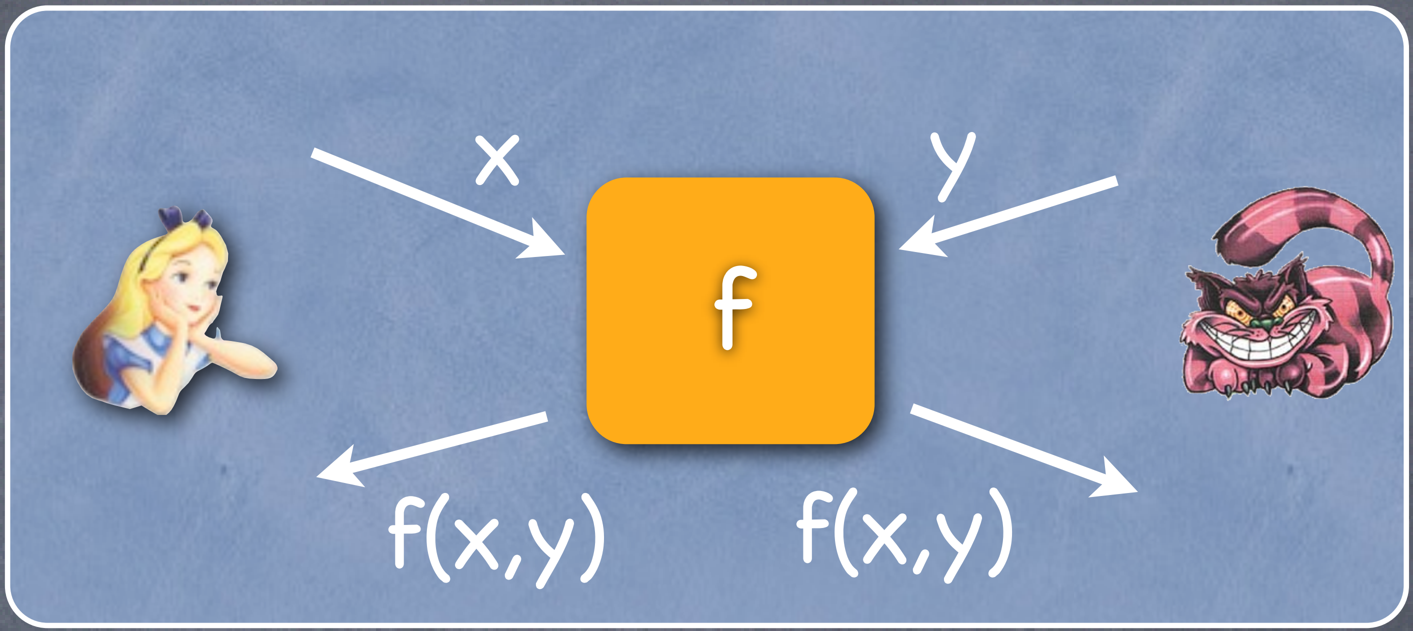




security holds if REAL looks like IDEAL to the outside world

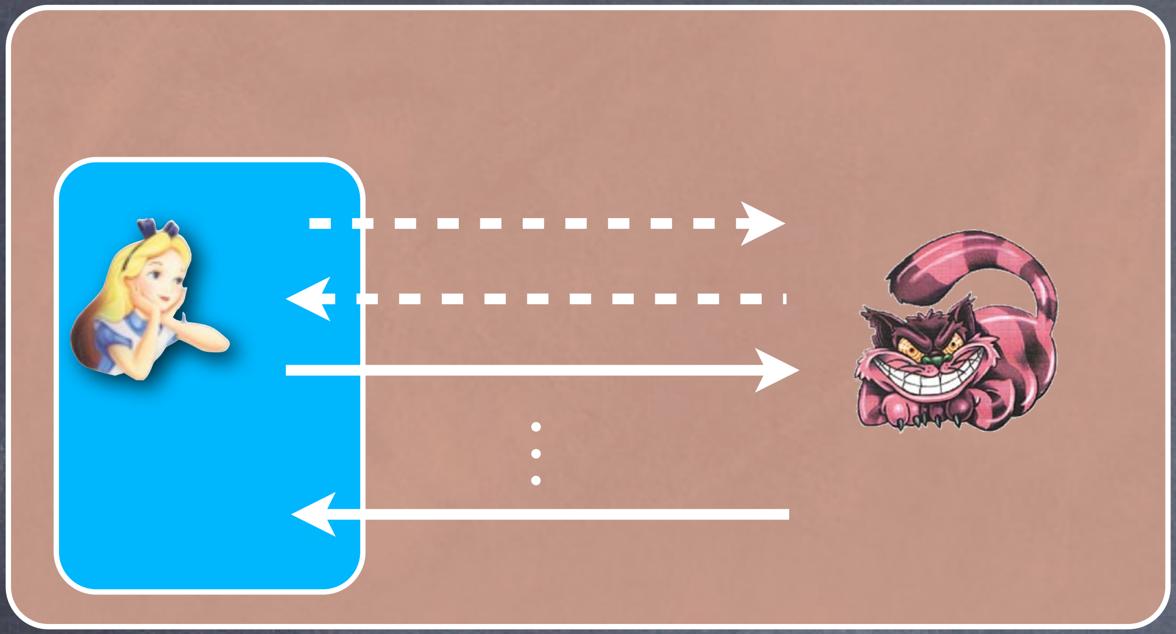
Formal Security Definition

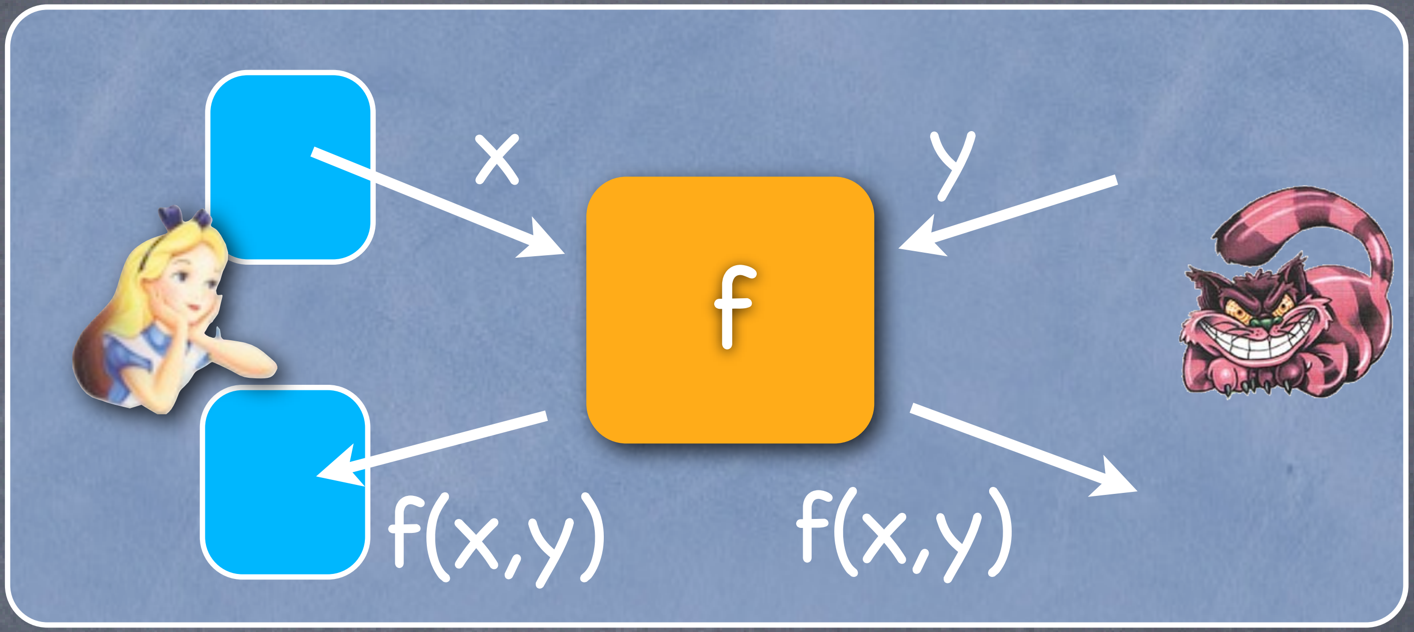




security holds if REAL looks like IDEAL to the outside world

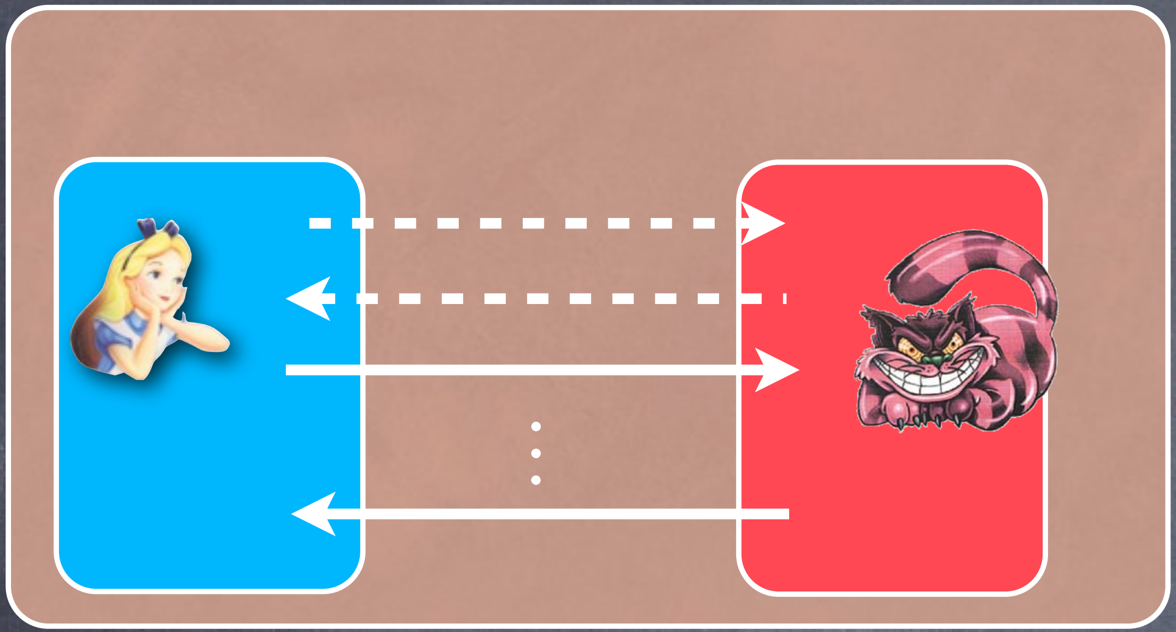
Formal Security Definition

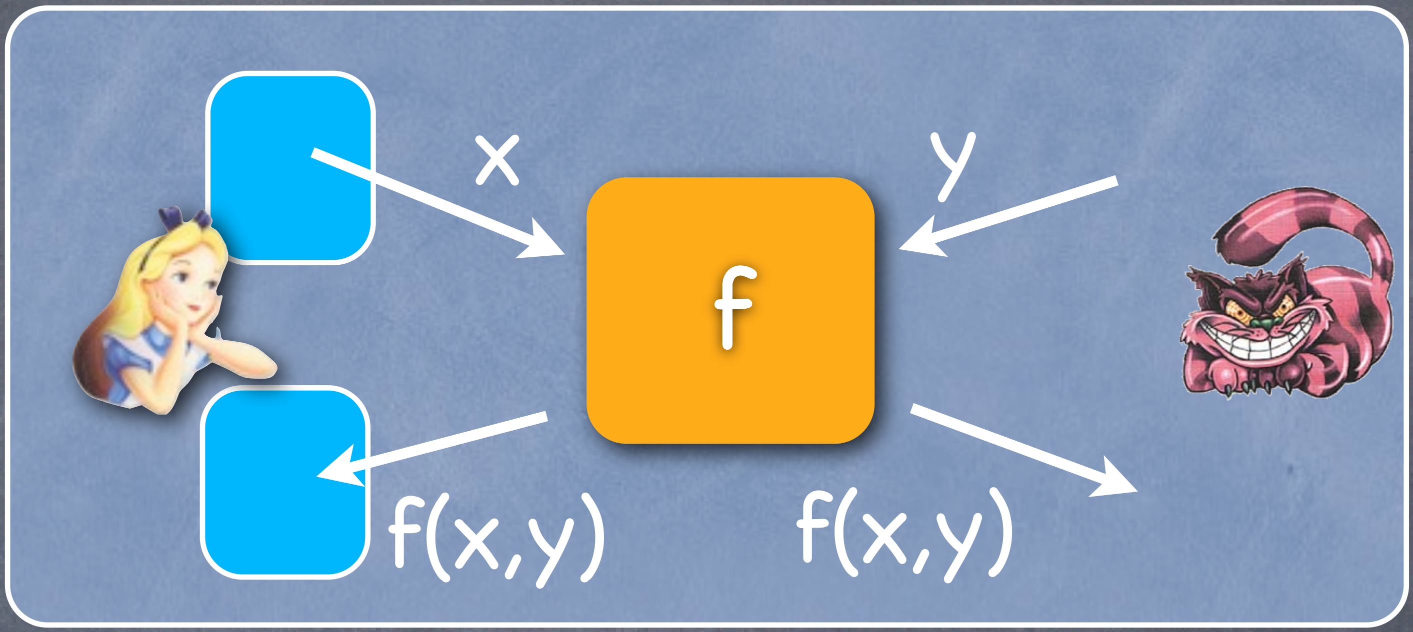




security holds if REAL looks like IDEAL to the outside world

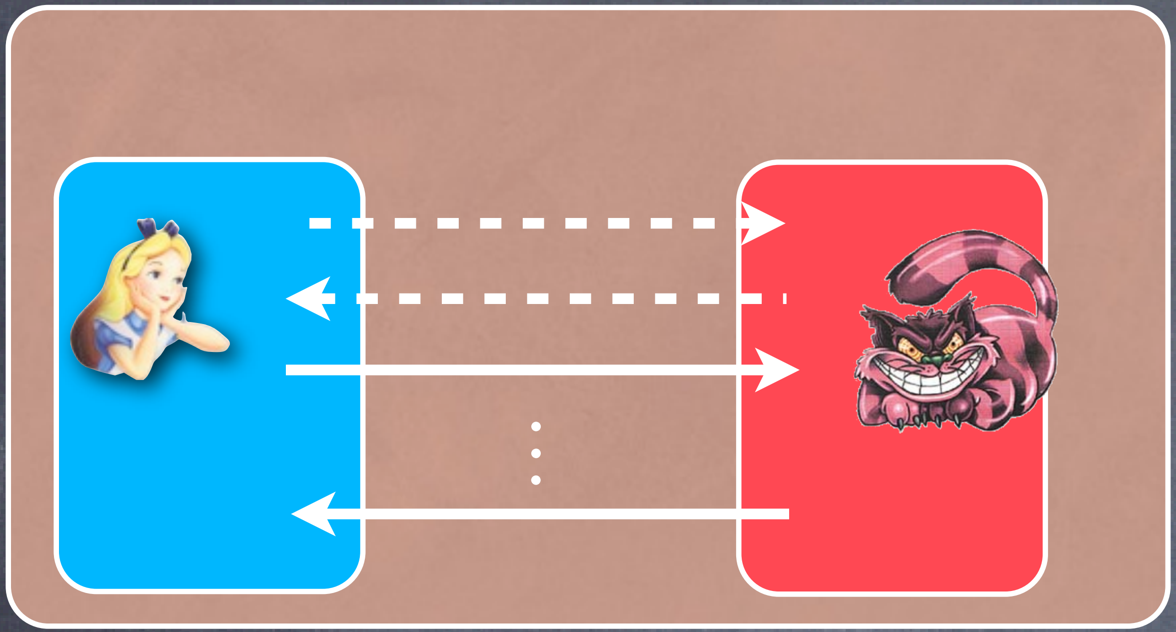
Formal Security Definition

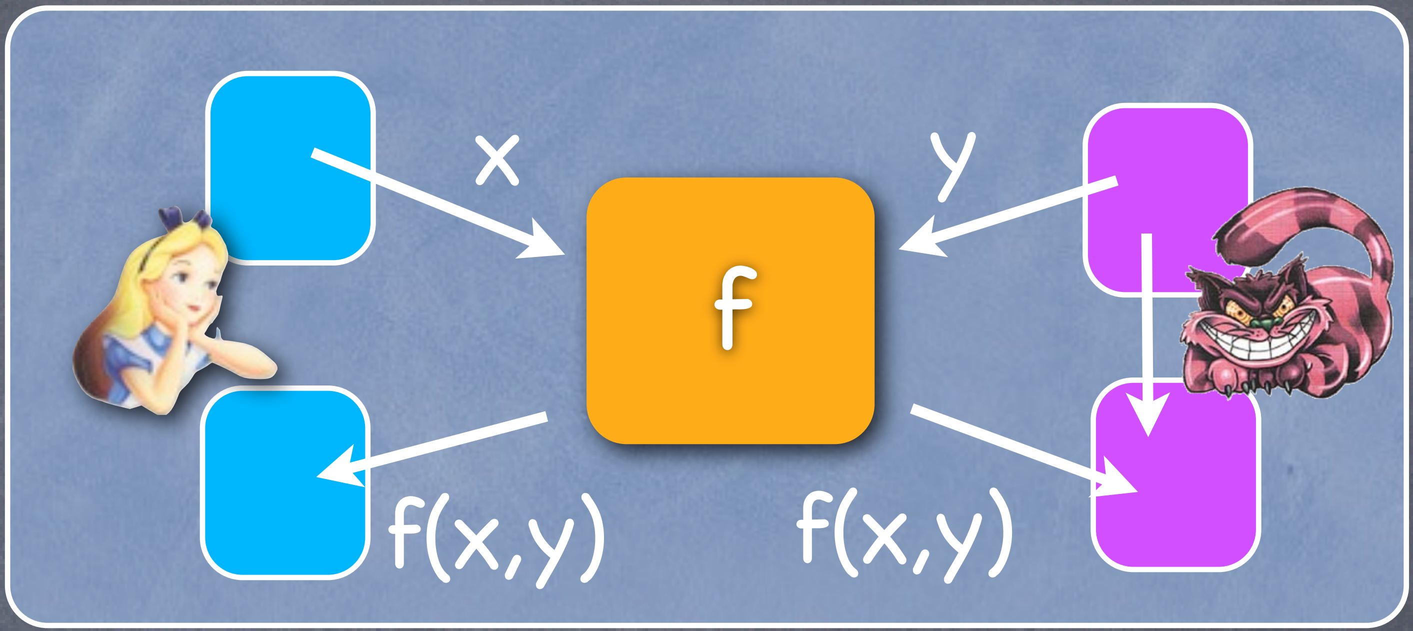




security holds if REAL looks like IDEAL to the outside world

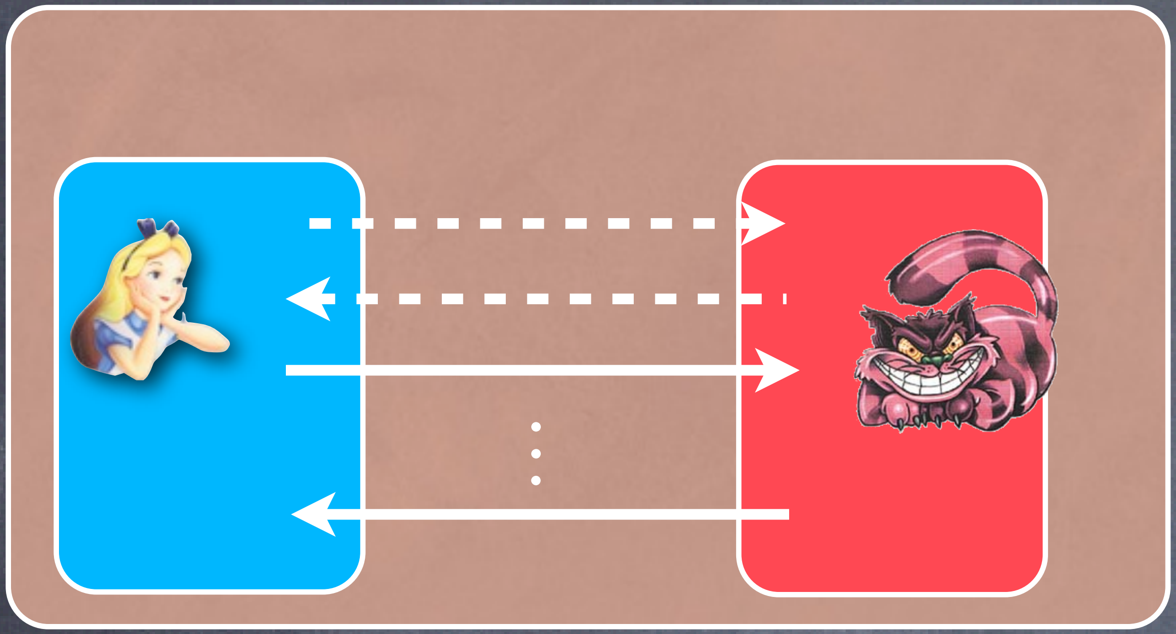
Formal Security Definition

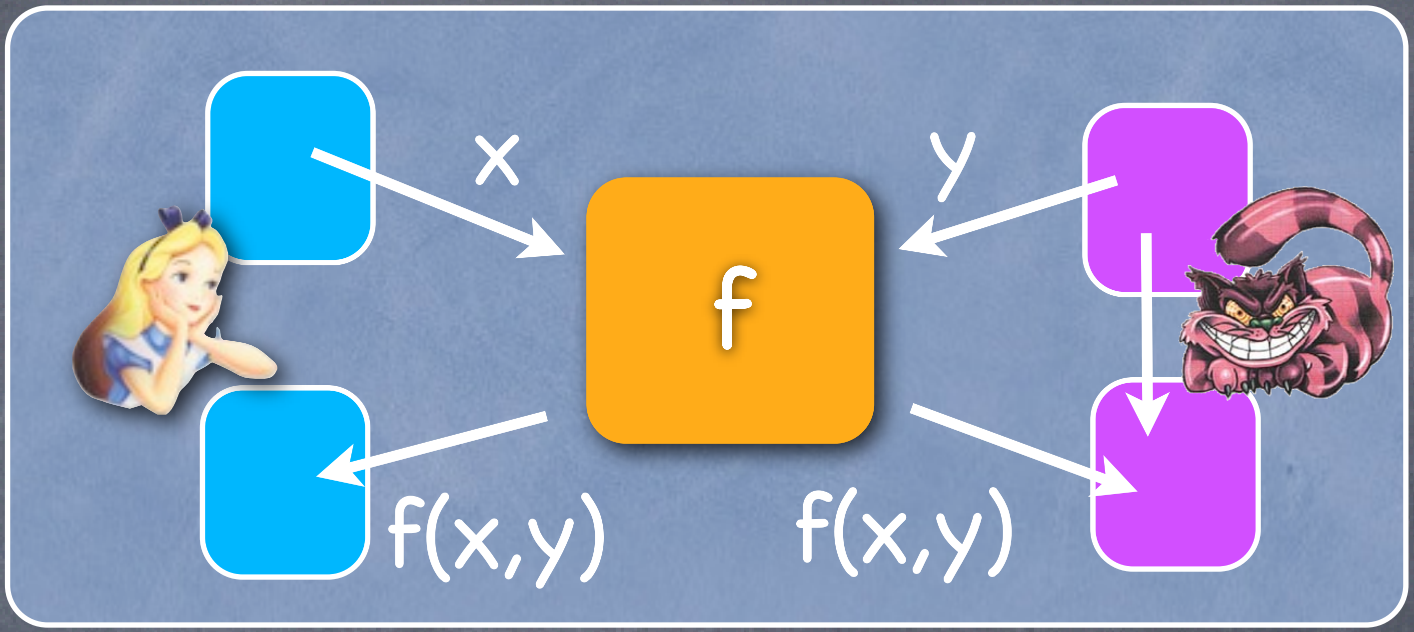




security holds if REAL looks like IDEAL to the outside world

Formal Security Definition

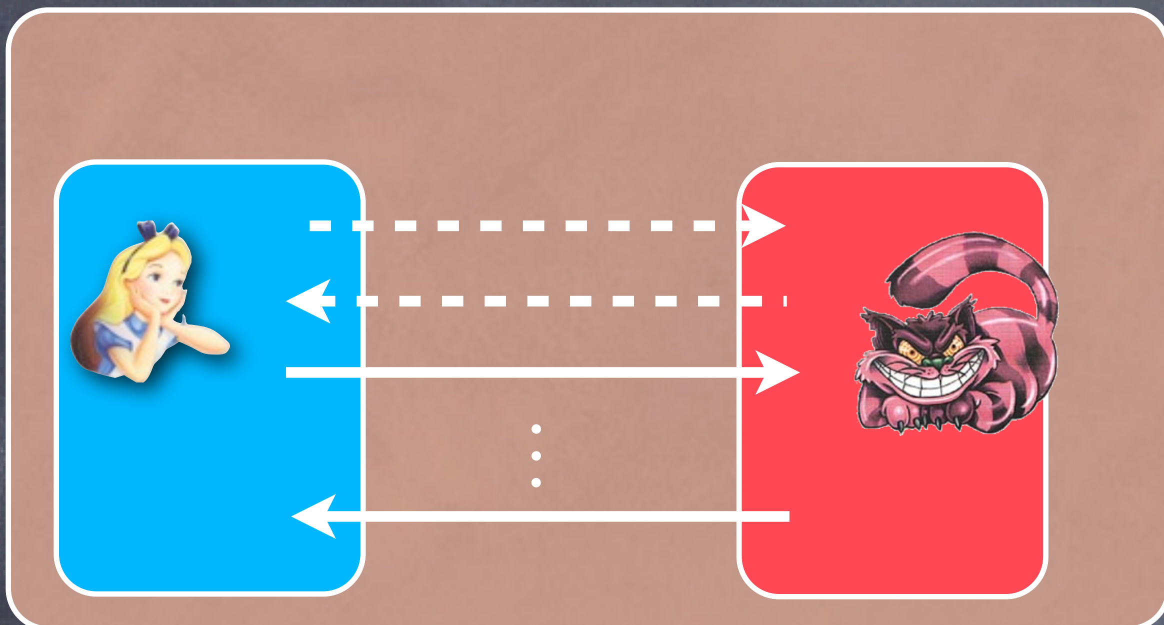


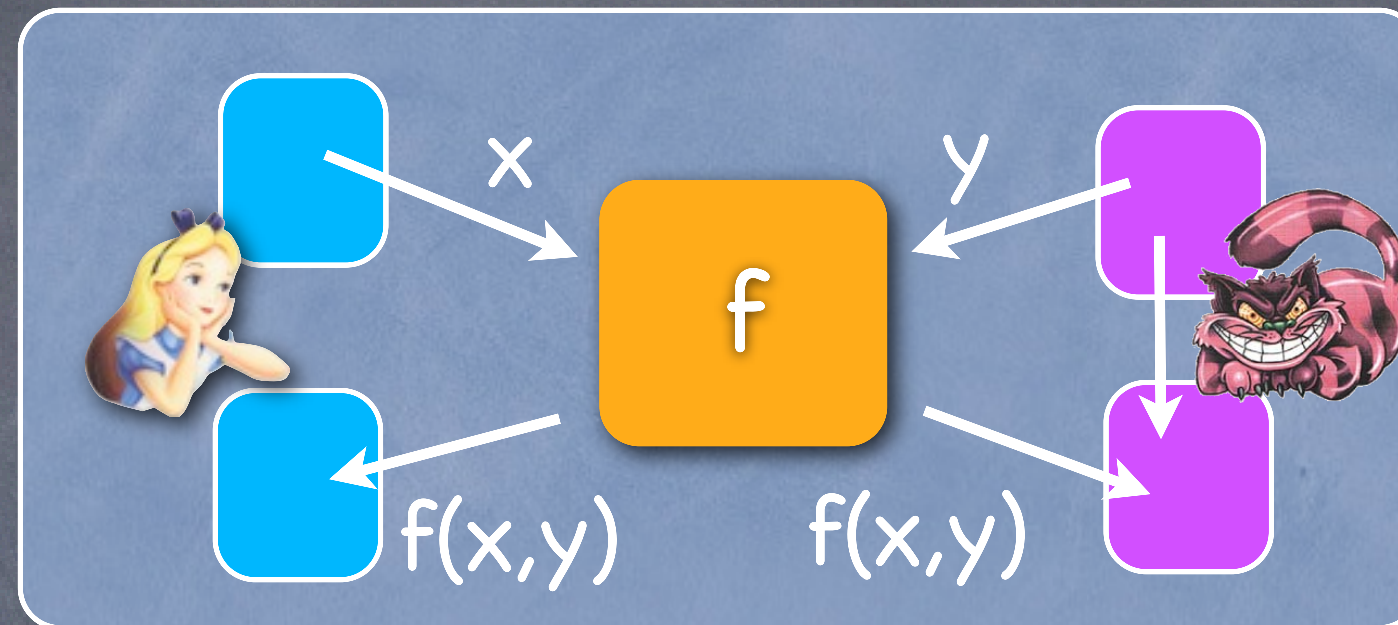


security holds if REAL looks like IDEAL to the outside world

- protocol is secure against dishonest Bob if

Formal Security Definition

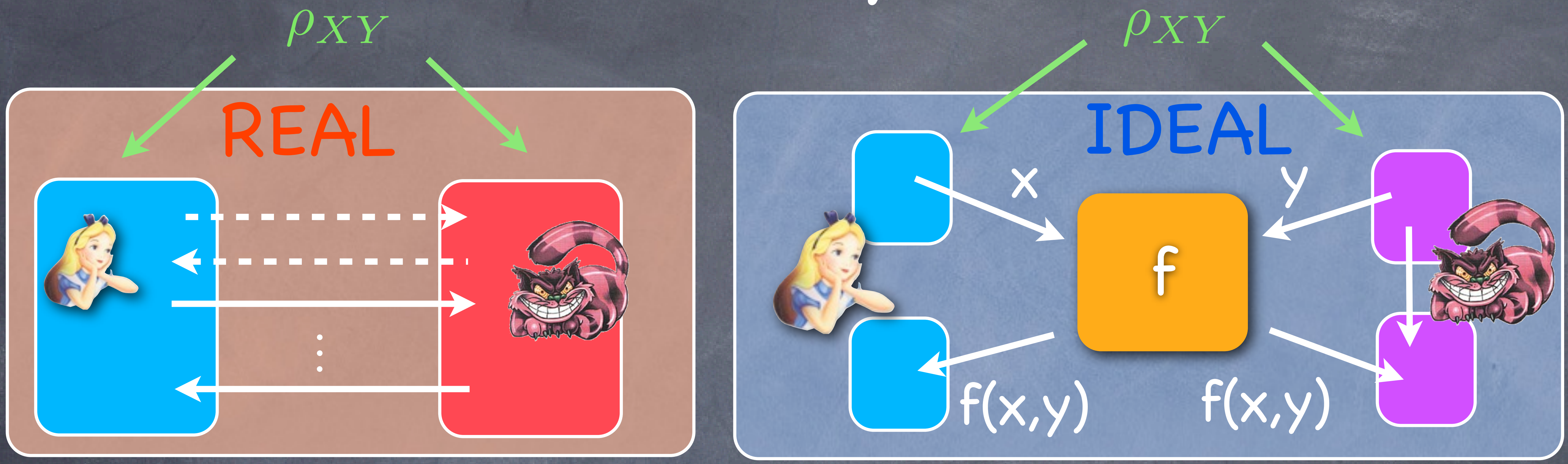




security holds if REAL looks like IDEAL to the outside world

- protocol is secure against dishonest Bob if
  - for every input distribution P(x,y), i.e. $\rho_{XY} = \sum_{x,y} P(x,y) |x\rangle\langle x|_A |y\rangle\langle y|_B$

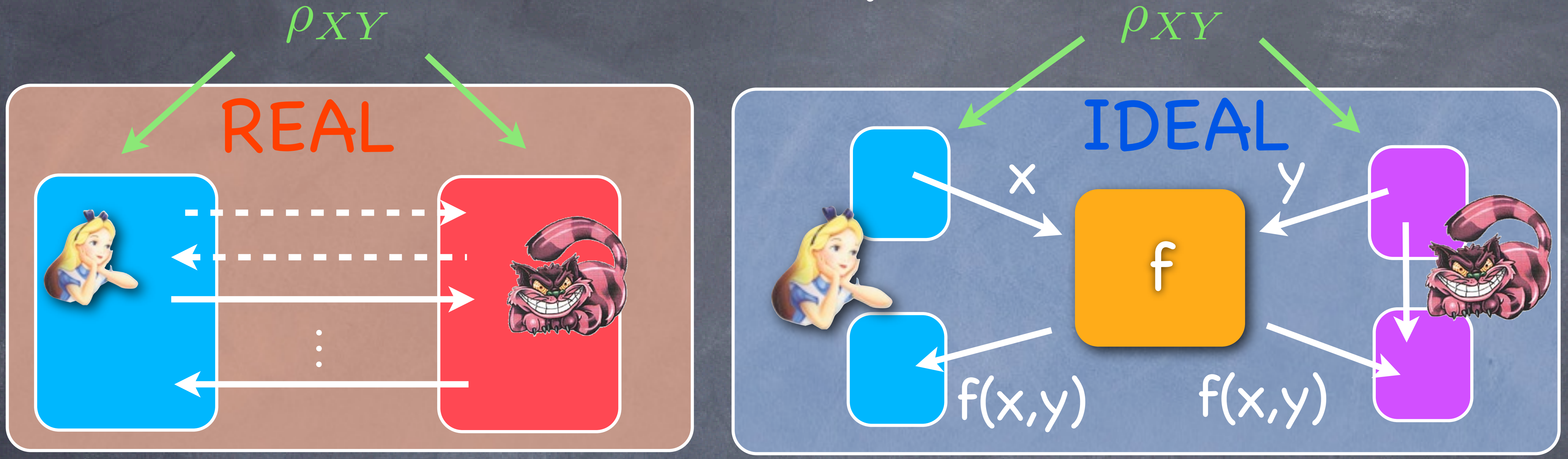
Formal Security Definition



security holds if REAL looks like IDEAL to the outside world

- protocol is secure against dishonest Bob if
  - for every input distribution P(x,y), i.e. $\rho_{XY} = \sum_{x,y} P(x,y) |x\rangle\langle x|_A |y\rangle\langle y|_B$

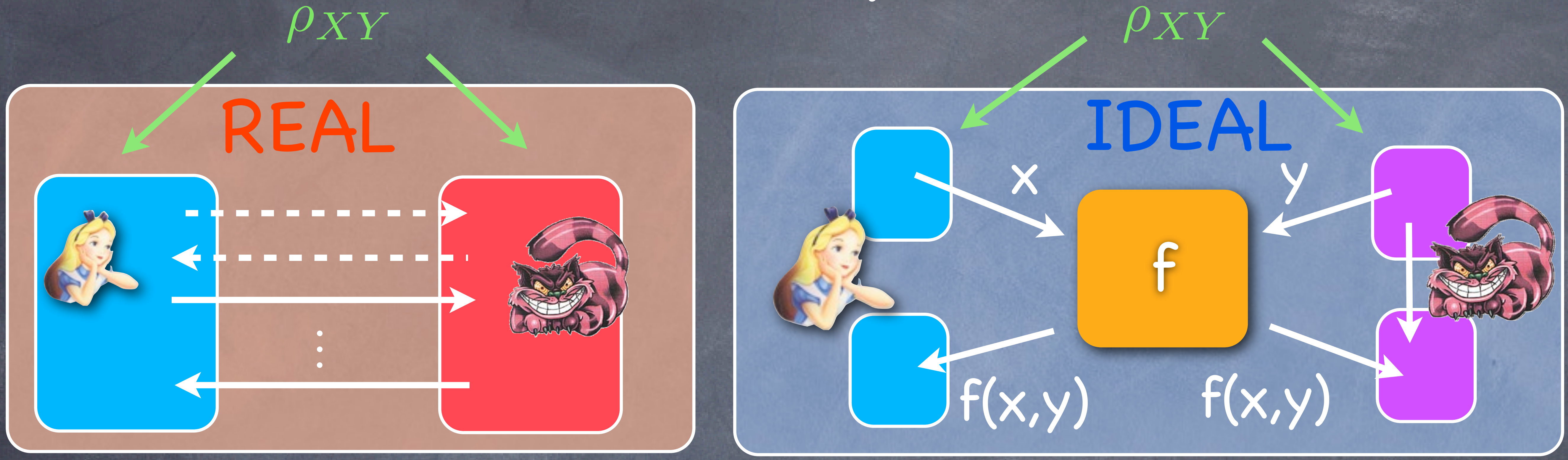
Formal Security Definition



security holds if REAL looks like IDEAL to the outside world

- protocol is secure against dishonest Bob if
  - for every input distribution P(x,y), i.e. $\rho_{XY} = \sum_{x,y} P(x,y) |x\rangle\langle x|_A |y\rangle\langle y|_B$
  - for every dishonest Bob B in the real world,

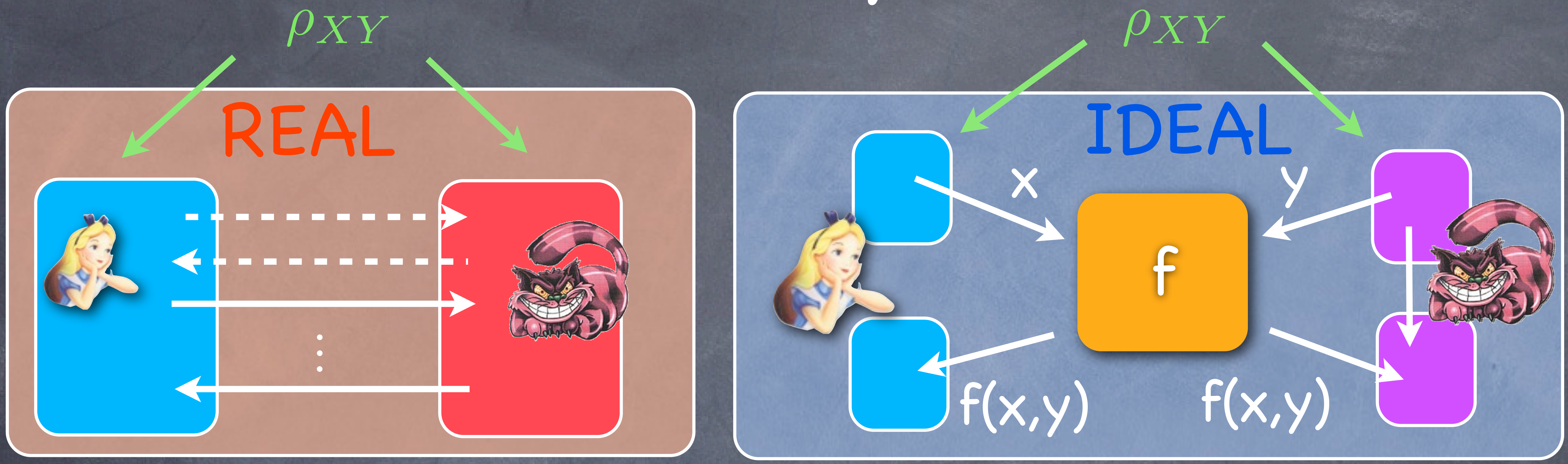
Formal Security Definition



security holds if REAL looks like IDEAL to the outside world

- protocol is secure against dishonest Bob if
  - for every input distribution P(x,y), i.e. $\rho_{XY} = \sum_{x,y} P(x,y)|x\rangle\langle x|_A|y\rangle\langle y|_B$
  - for every dishonest Bob B in the real world,
  - there exists a dishonest Bob B in the ideal world

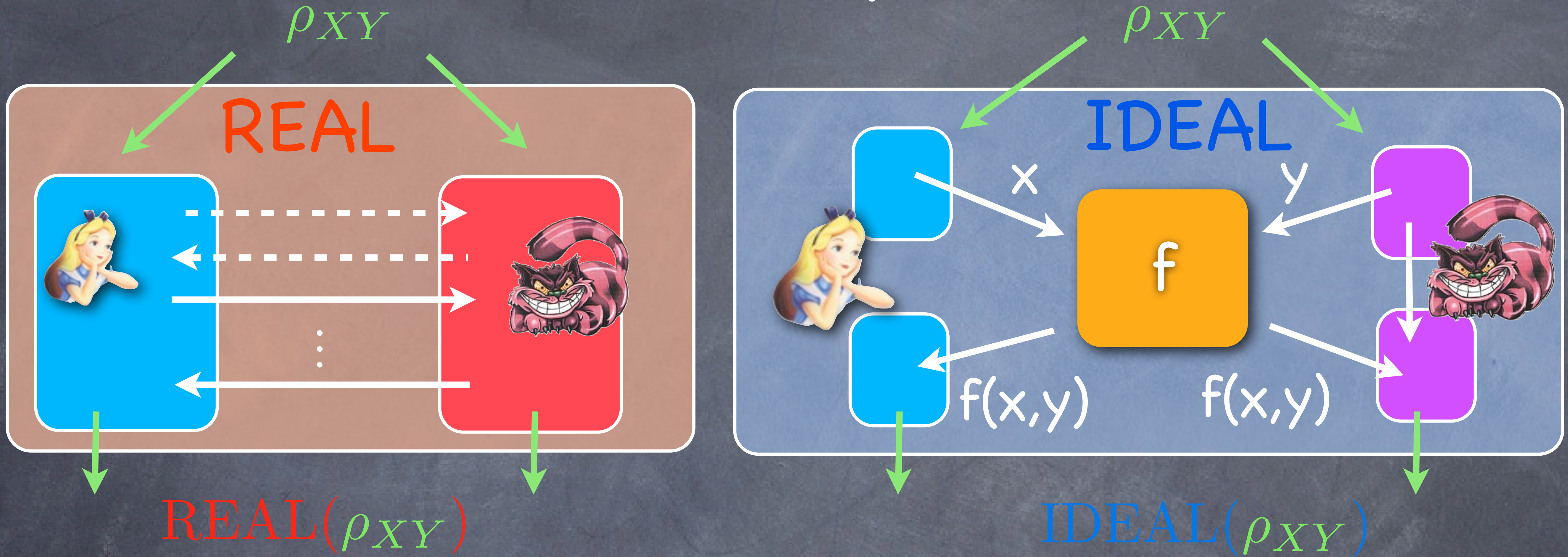
Formal Security Definition



security holds if REAL looks like IDEAL to the outside world

- protocol is secure against dishonest Bob if
  - for every input distribution P(x,y), i.e. $\rho_{XY} = \sum_{x,y} P(x,y)|x\rangle\langle x|_A|y\rangle\langle y|_B$
  - for every dishonest Bob B in the real world,
  - there exists a dishonest Bob B in the ideal world
  - such that

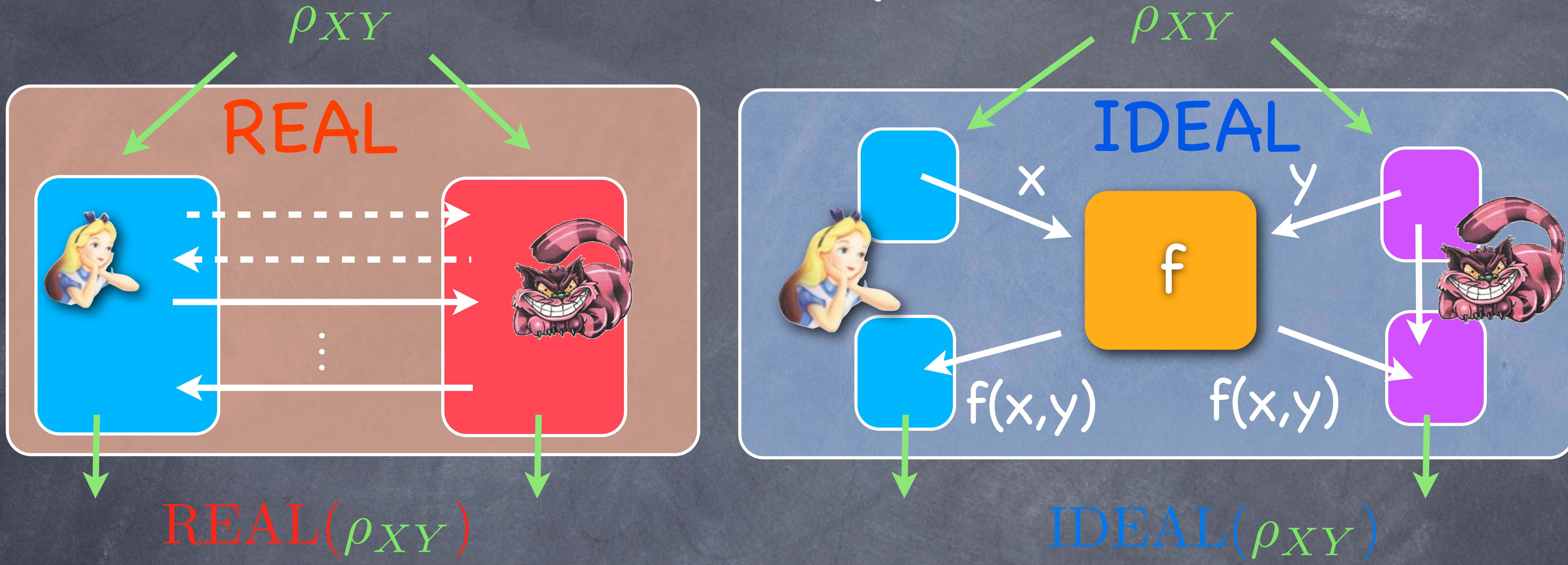
Formal Security Definition



security holds if REAL looks like IDEAL to the outside world

- protocol is secure against dishonest Bob if
  - for every input distribution P(x,y), i.e. $\rho_{XY} = \sum_{x,y} P(x,y) |x\rangle\langle x|_A |y\rangle\langle y|_B$
  - for every dishonest Bob B in the real world,
  - there exists a dishonest Bob B in the ideal world
  - such that $\mathrm{REAL}(\rho_{XY}) = \mathrm{IDEAL}(\rho_{XY})$

Formal Security Definition



security holds if REAL looks like IDEAL to the outside world

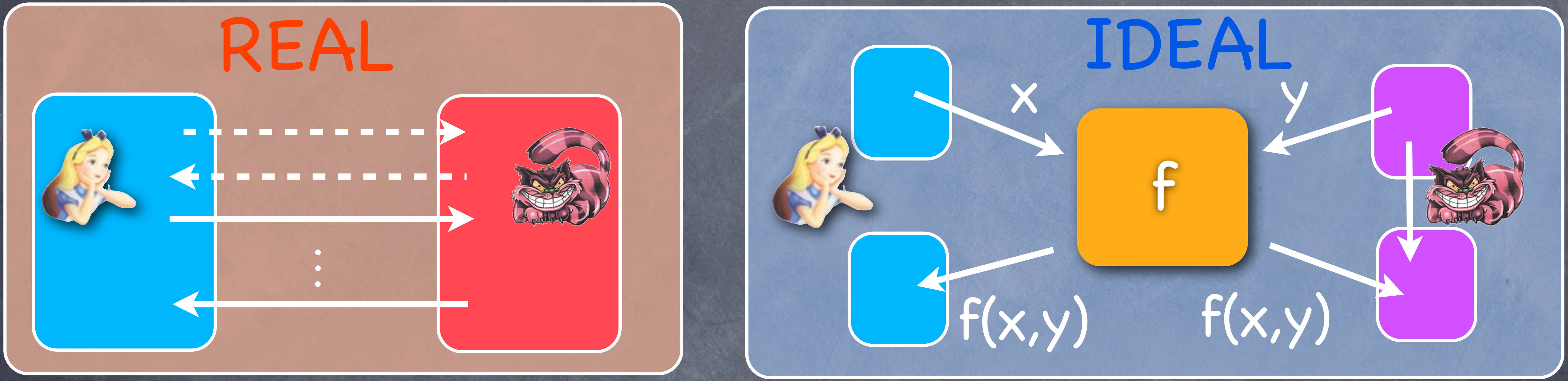
- protocol is secure against dishonest Bob if
  - for every input distribution P(x,y), i.e. $\rho_{XY} = \sum_{x,y} P(x,y) |x\rangle\langle x|_A |y\rangle\langle y|_B$
  - for every dishonest Bob B in the real world,
  - there exists a dishonest Bob B in the ideal world
  - such that $\mathrm{REAL}(\rho_{XY}) = \mathrm{IDEAL}(\rho_{XY})$

also relative to purification

Proof of Insecurity

Security against Bob => Insecurity against Alice

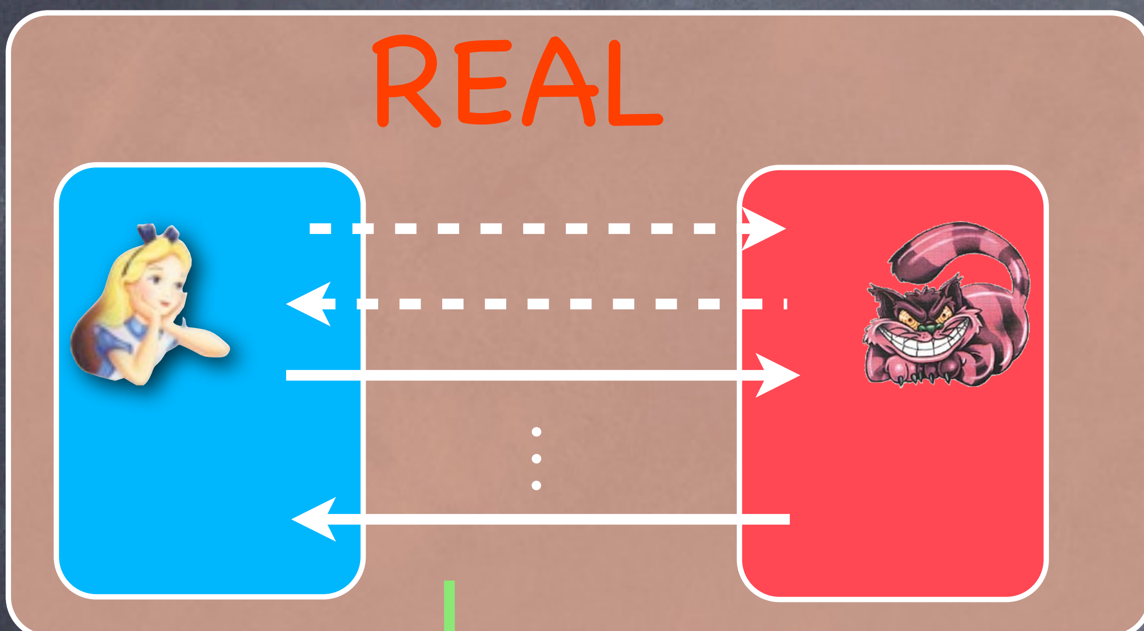
security holds if REAL looks like IDEAL to the outside world

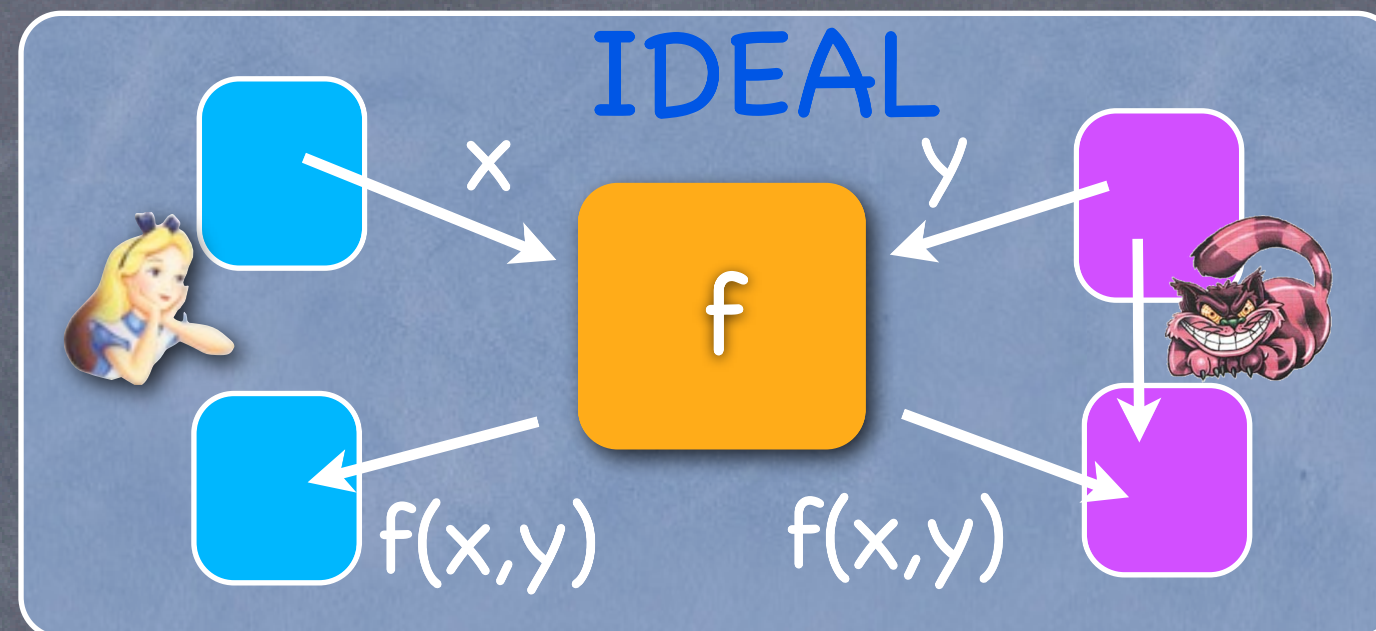


Proof of Insecurity

Security against Bob => Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world





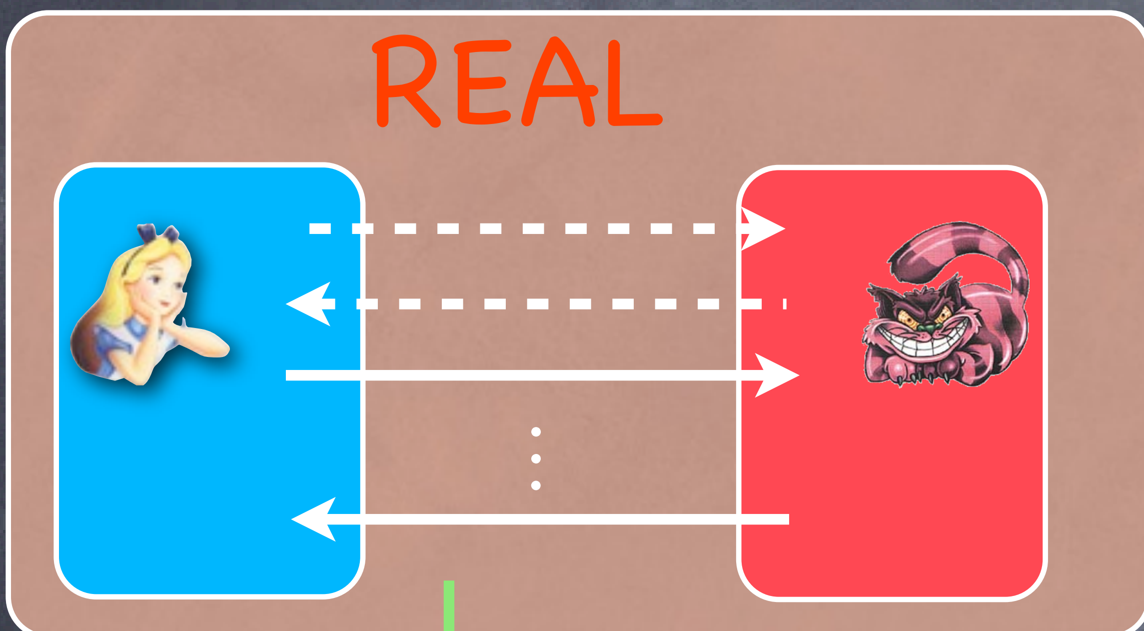
$|\psi\rangle_{A_p A B B_p}$

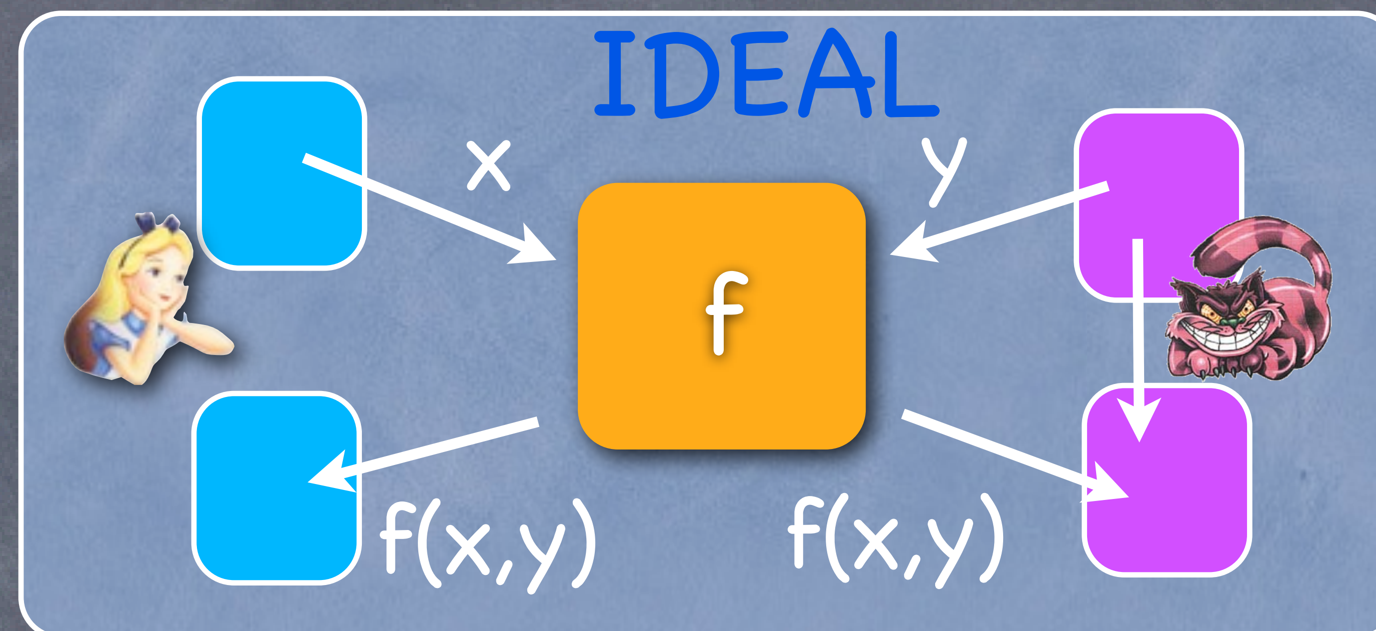
state after the real protocol if both parties play "dishonestly" by purifying their actions

Proof of Insecurity

Security against Bob => Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world



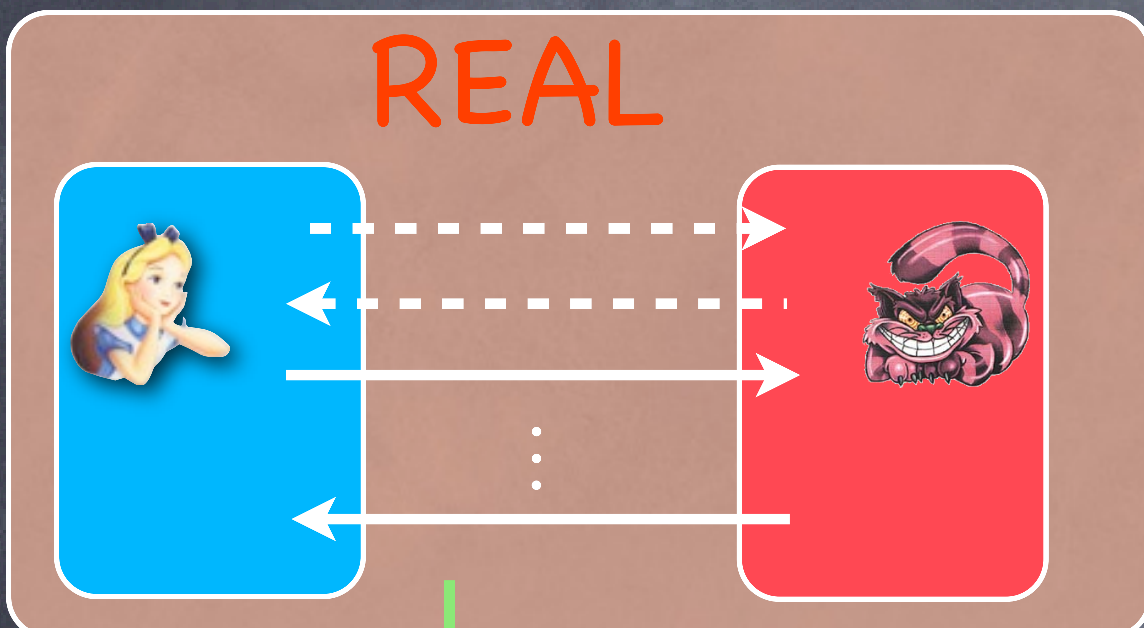


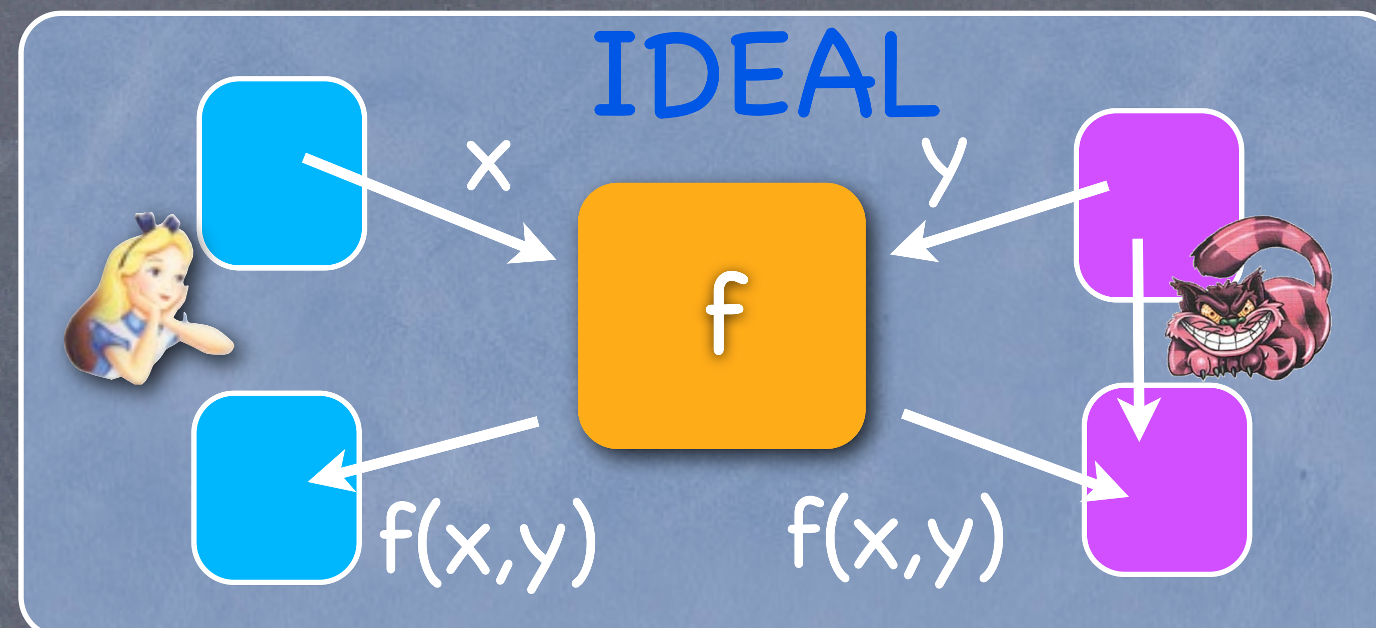
 $|\psi\rangle_{A_p A B B_p}$  state after the real protocol if both parties play “dishonestly” by purifying their actions

Proof of Insecurity

Security against Bob => Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world





$|\psi\rangle_{A_pABB_p}$

state after the real protocol if both parties play "dishonestly" by purifying their actions

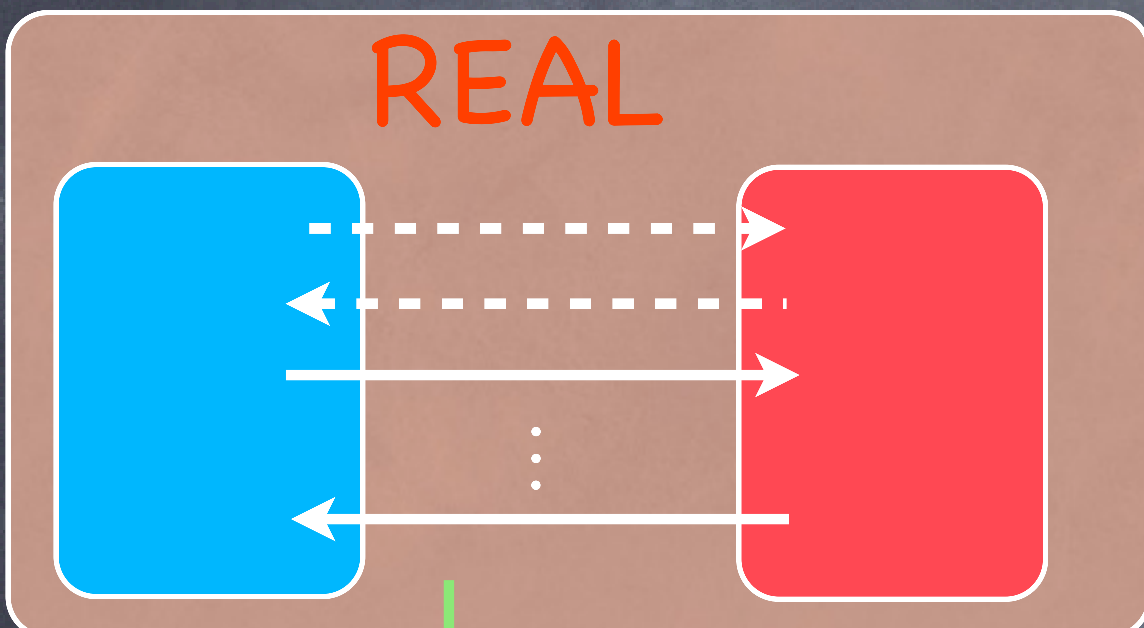
tr_{A_p}

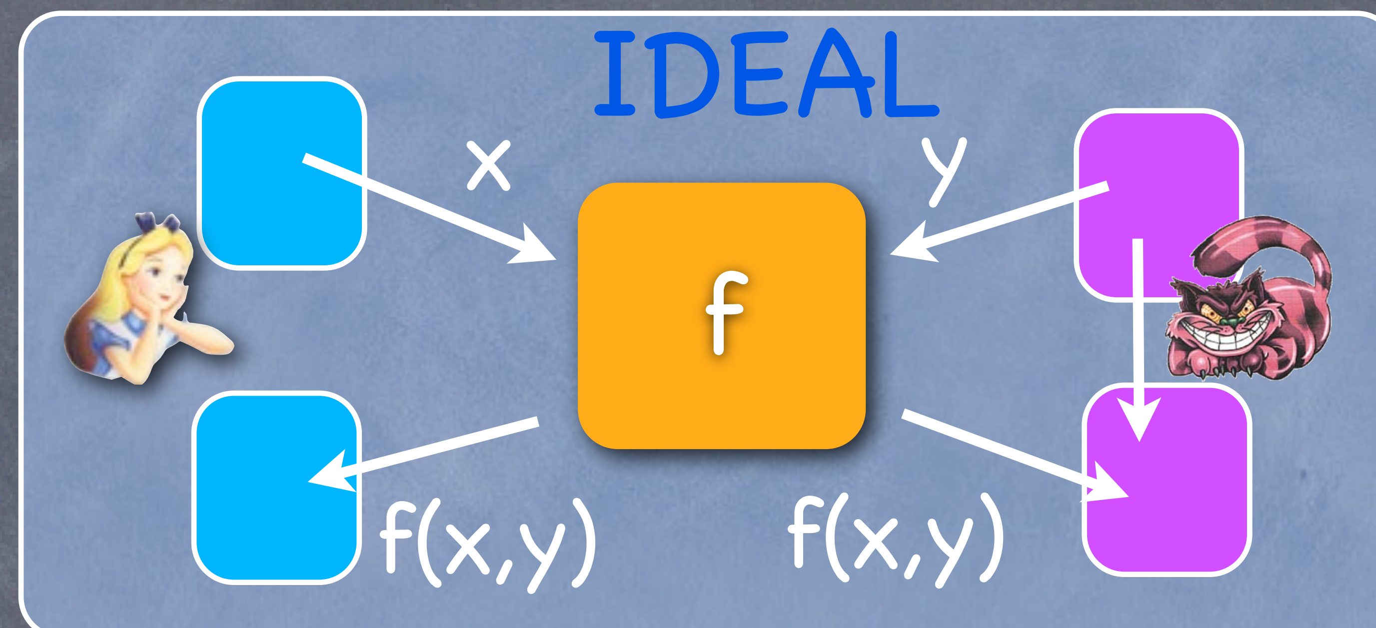
$$\rho_{ABB_p} = \sigma_{ABB_p} = \mathrm{tr}_Y(\sigma_{ABB_pY})$$

Proof of Insecurity

Security against Bob => Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world





$|\psi\rangle_{A_p A B B_p}$

state after the real protocol if both parties play "dishonestly" by purifying their actions

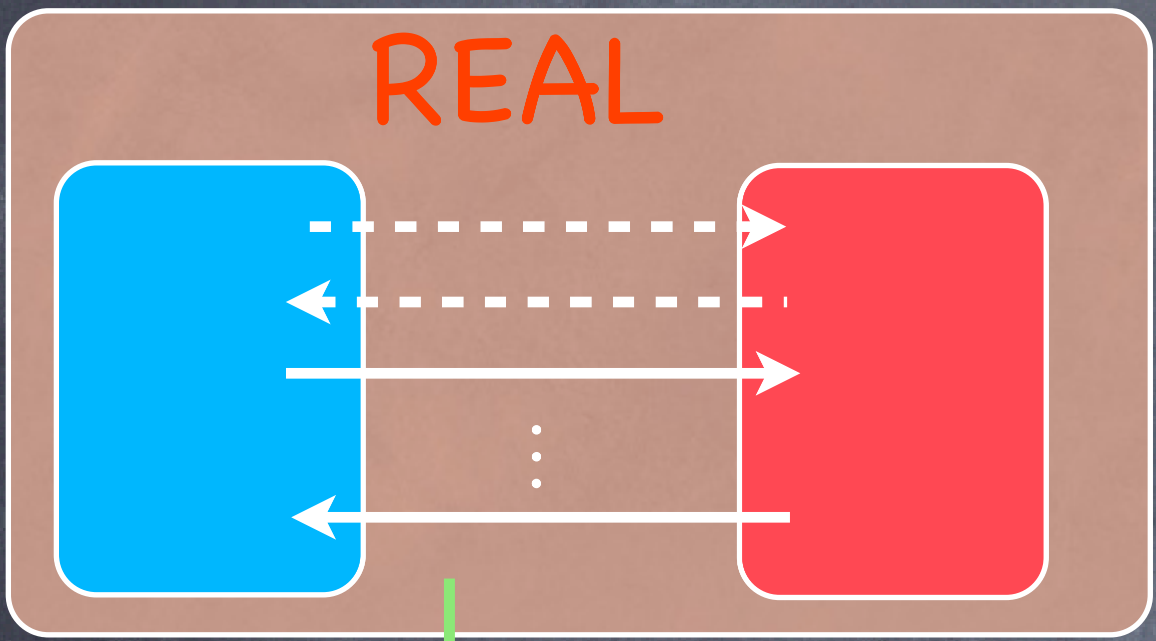
$\xrightarrow{\mathrm{tr}_{A_p}}$

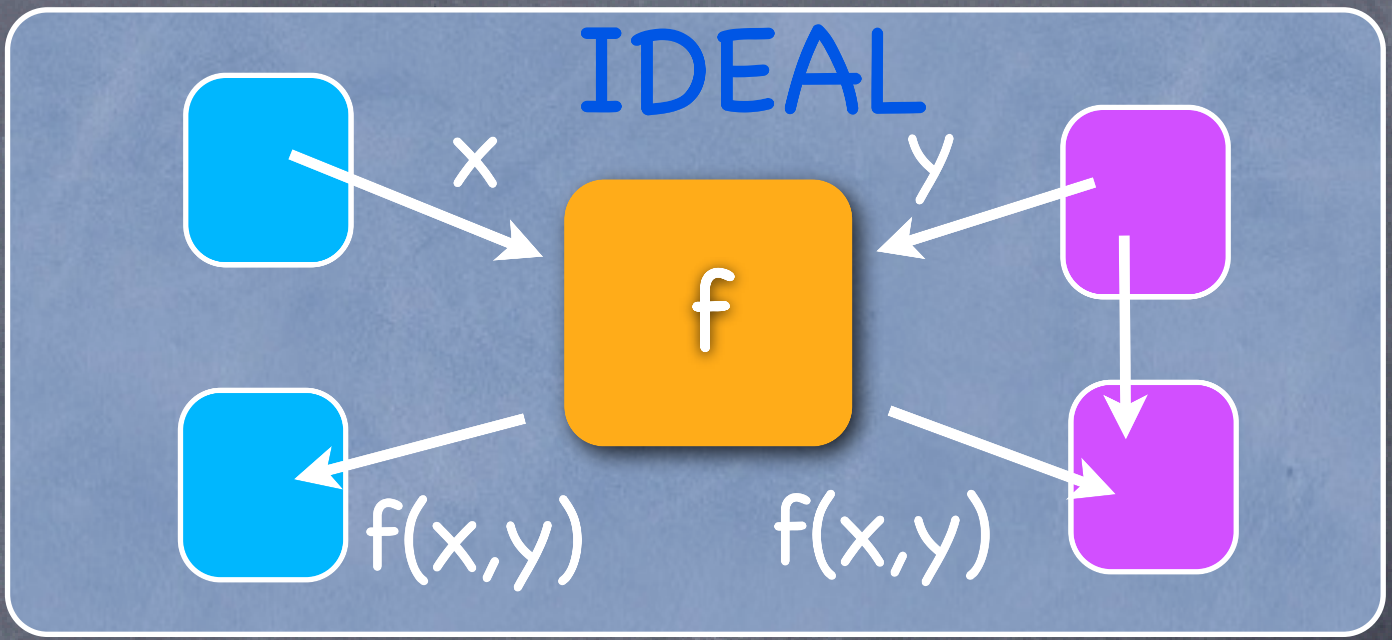
$$\rho_{ABB_p} = \sigma_{ABB_p} = \mathrm{tr}_Y(\sigma_{ABB_pY})$$

Proof of Insecurity

Security against Bob => Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world





$|\psi\rangle_{A_p A B B_p}$

state after the real protocol if both parties play "dishonestly" by purifying their actions

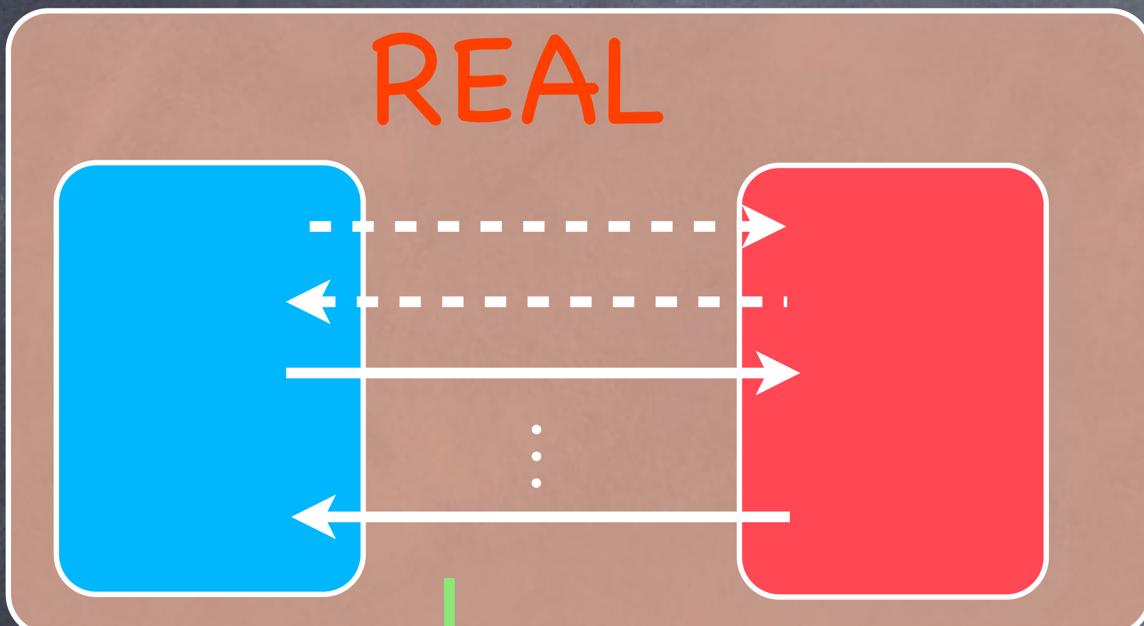
tr_{A_p}

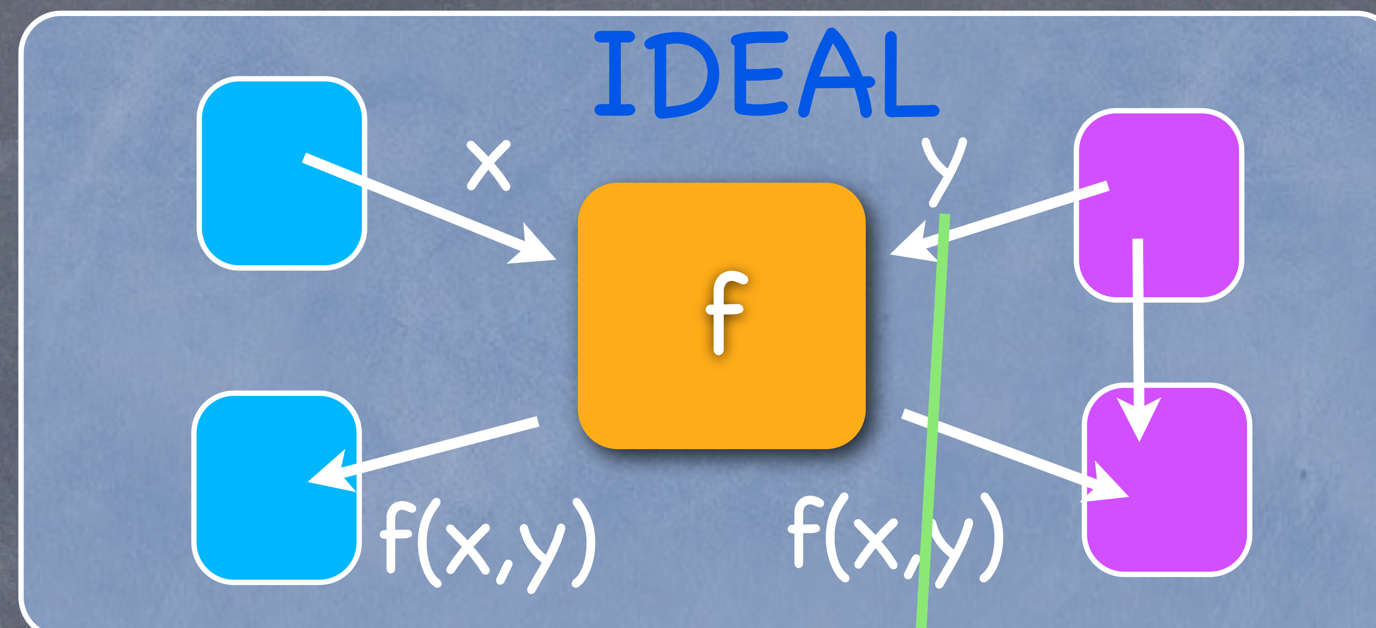
$$\rho_{ABB_p} = \sigma_{ABB_p} = \mathrm{tr}_Y(\sigma_{ABB_pY})$$

Proof of Insecurity

Security against Bob => Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world



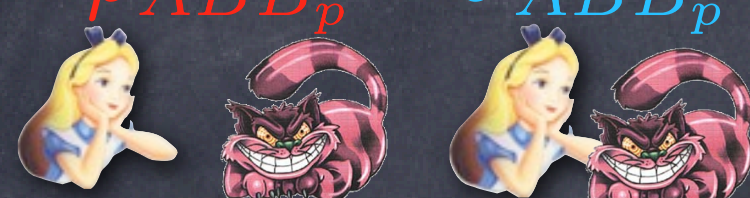


$|\psi\rangle_{A_pABB_p}$

state after the real protocol if both parties play “dishonestly” by purifying their actions

tr_{A_p}

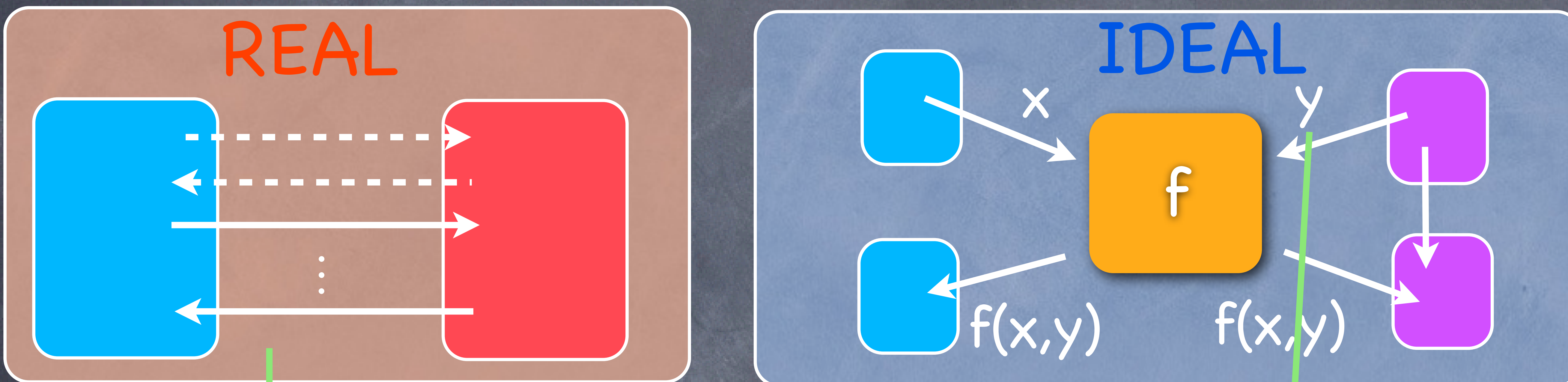
$$\rho_{ABB_p} = \sigma_{ABB_p} = \mathrm{tr}_Y(\sigma_{ABB_pY})$$



Proof of Insecurity

Security against Bob => Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world



 $|\psi\rangle_{A_pABB_p}$  state after the real protocol if both parties play "dishonestly" by purifying their actions

tr_{A_p}

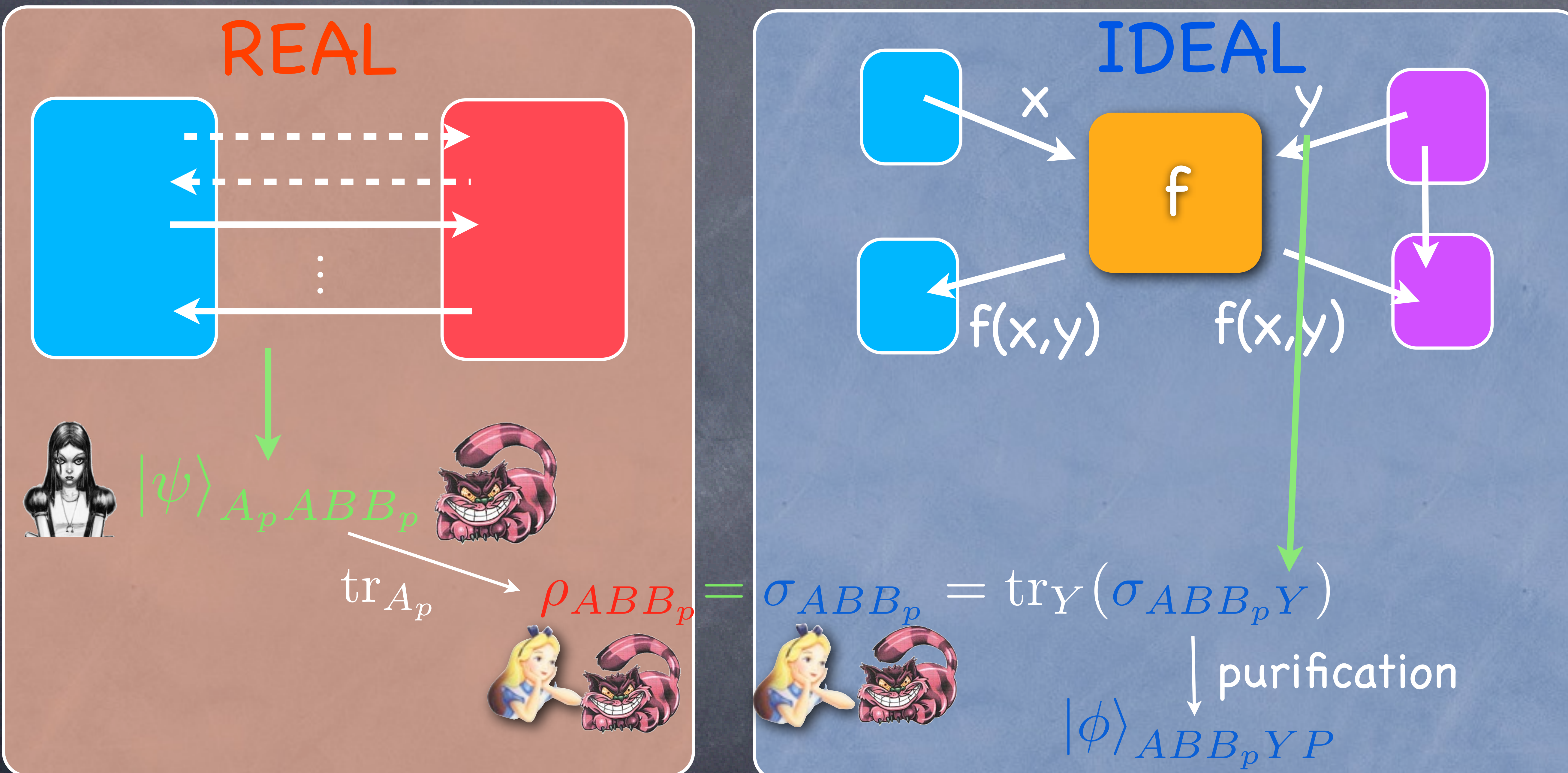
$$\rho_{ABB_p} = \sigma_{ABB_p} = \mathrm{tr}_Y(\sigma_{ABB_pY})$$

purification

$$|\phi\rangle_{ABB_pYP}$$

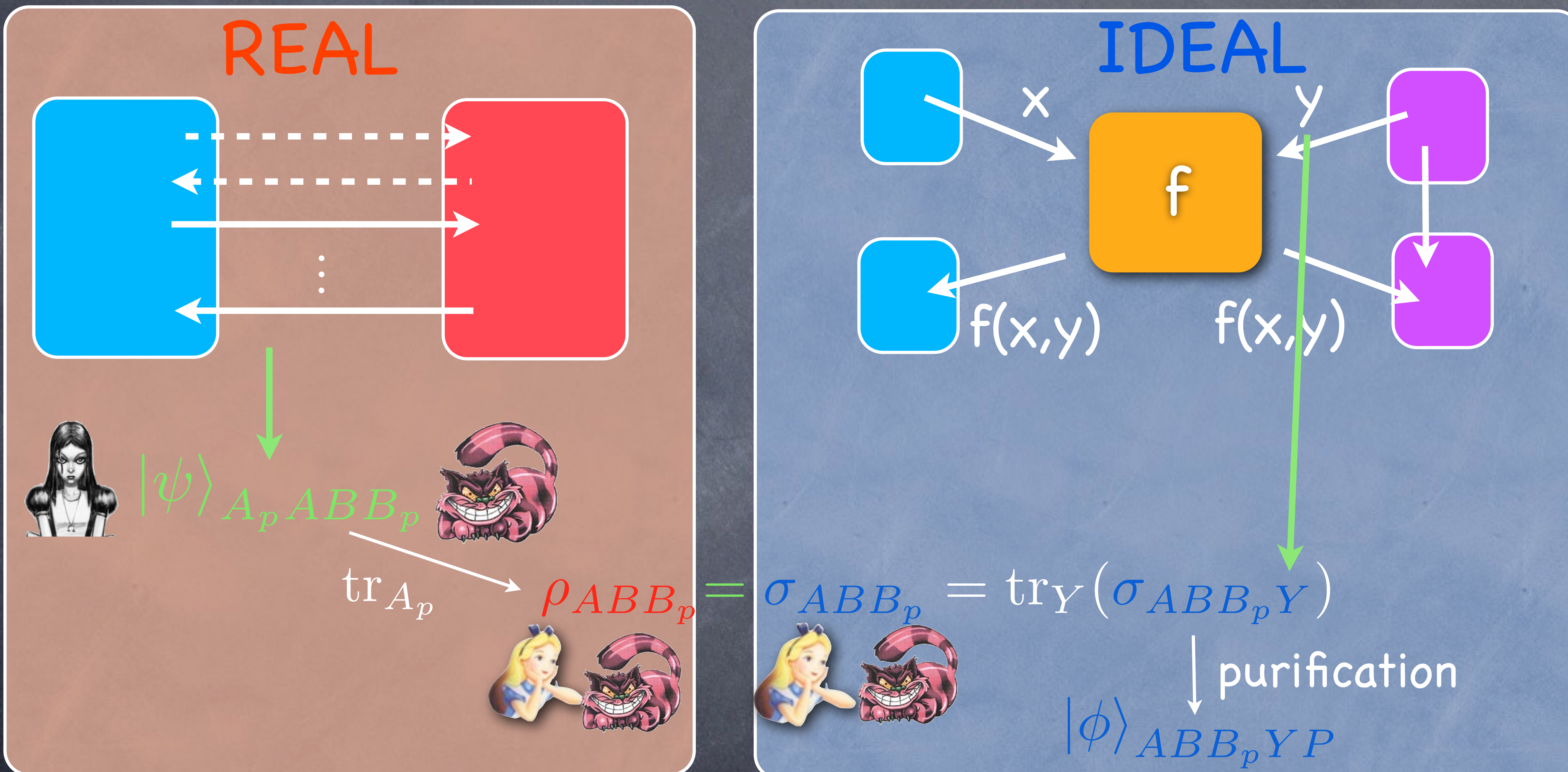
Proof of Insecurity

security holds if REAL looks like IDEAL to the outside world



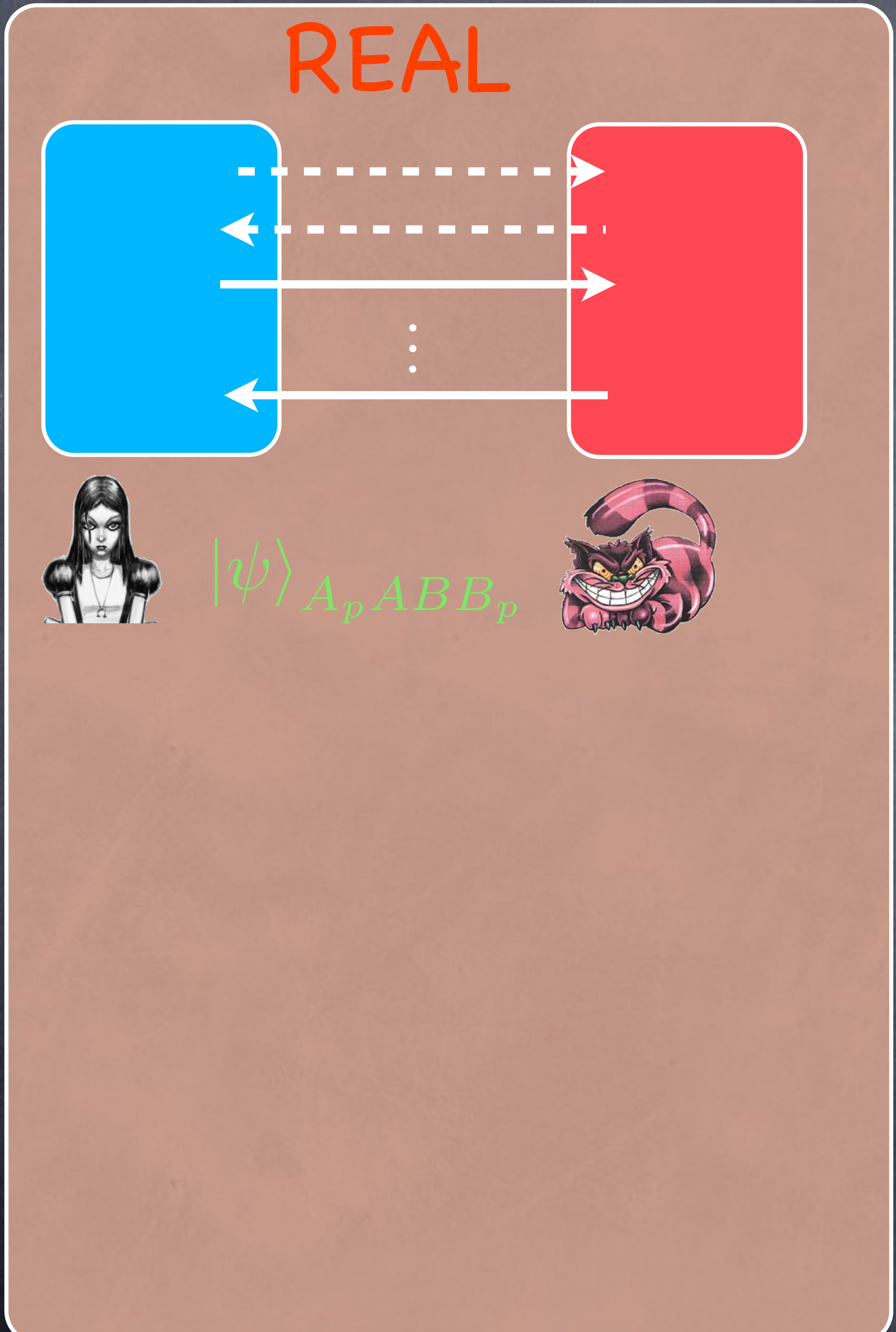
Proof of Insecurity

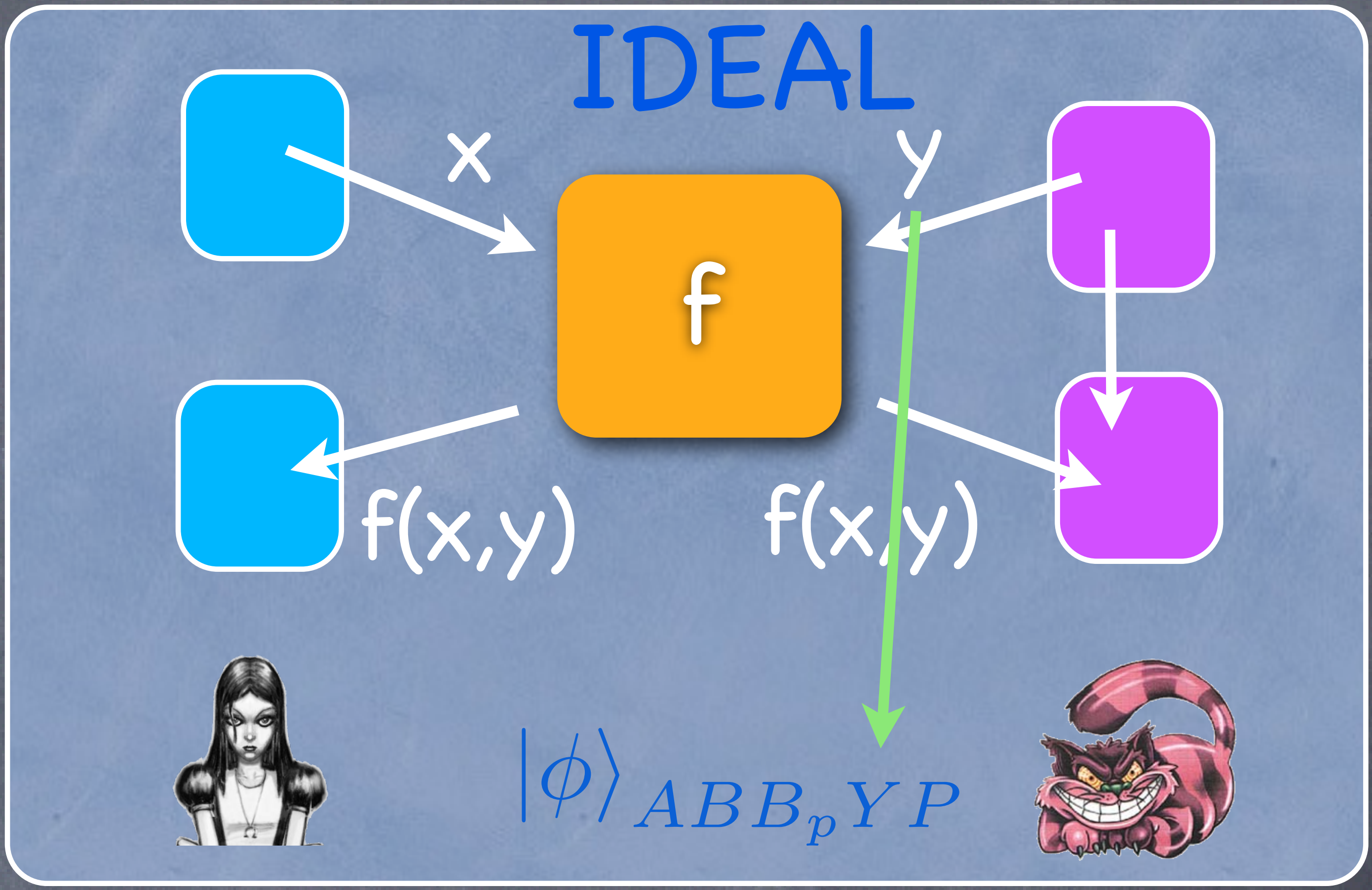
security holds if REAL looks like IDEAL to the outside world



- by Uhlmann's theorem: there exists a cheating unitary U such that $U_{A_p \to YP} \, |\psi\rangle_{A_pABB_p} = |\phi\rangle_{ABB_pYP}$

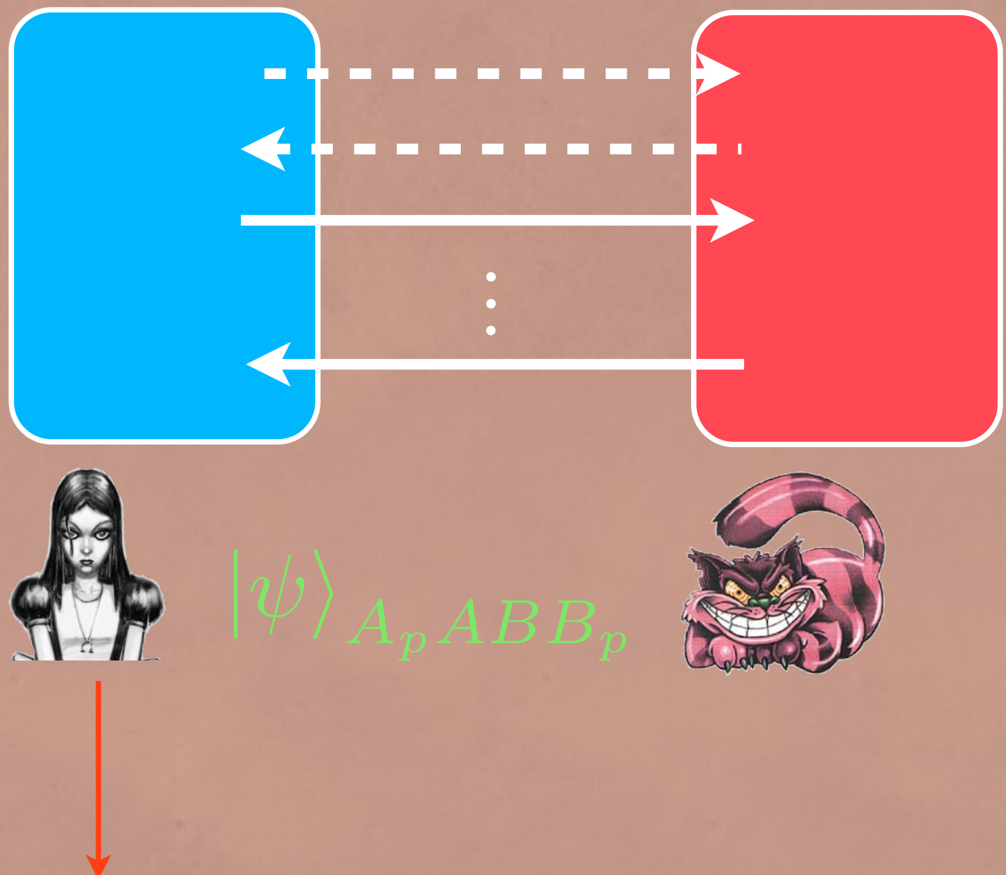
Proof of Insecurity





Proof of Insecurity

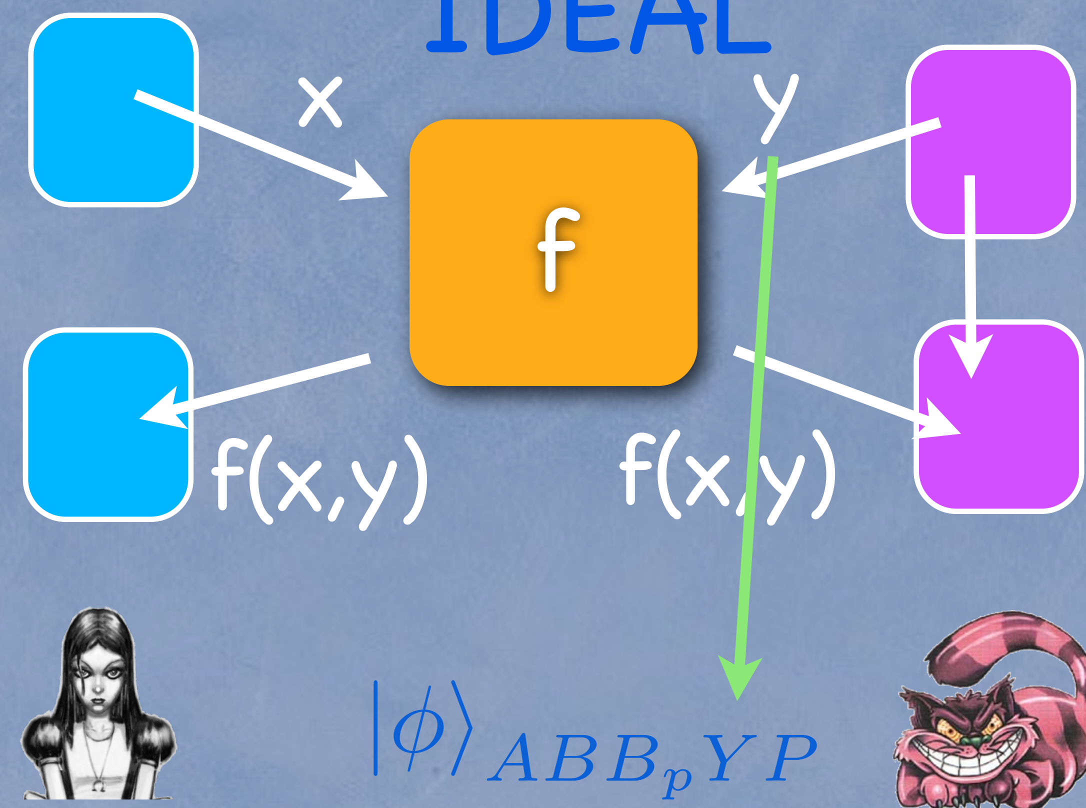
REAL



$$|\psi\rangle_{A_pABB_p}$$

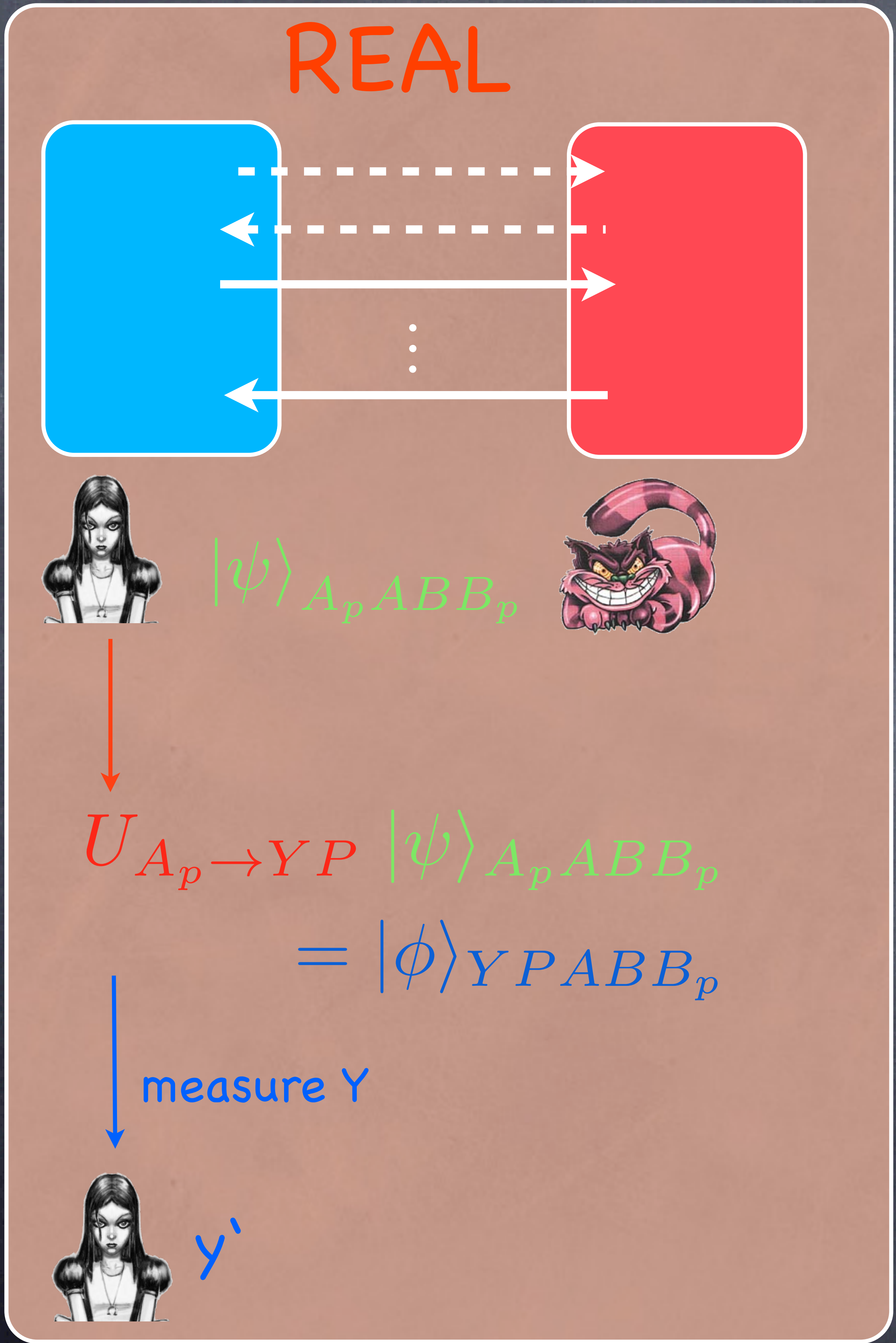
$$U_{A_p \to YP}\, |\psi\rangle_{A_pABB_p}$$
$$= |\phi\rangle_{YPABB_p}$$

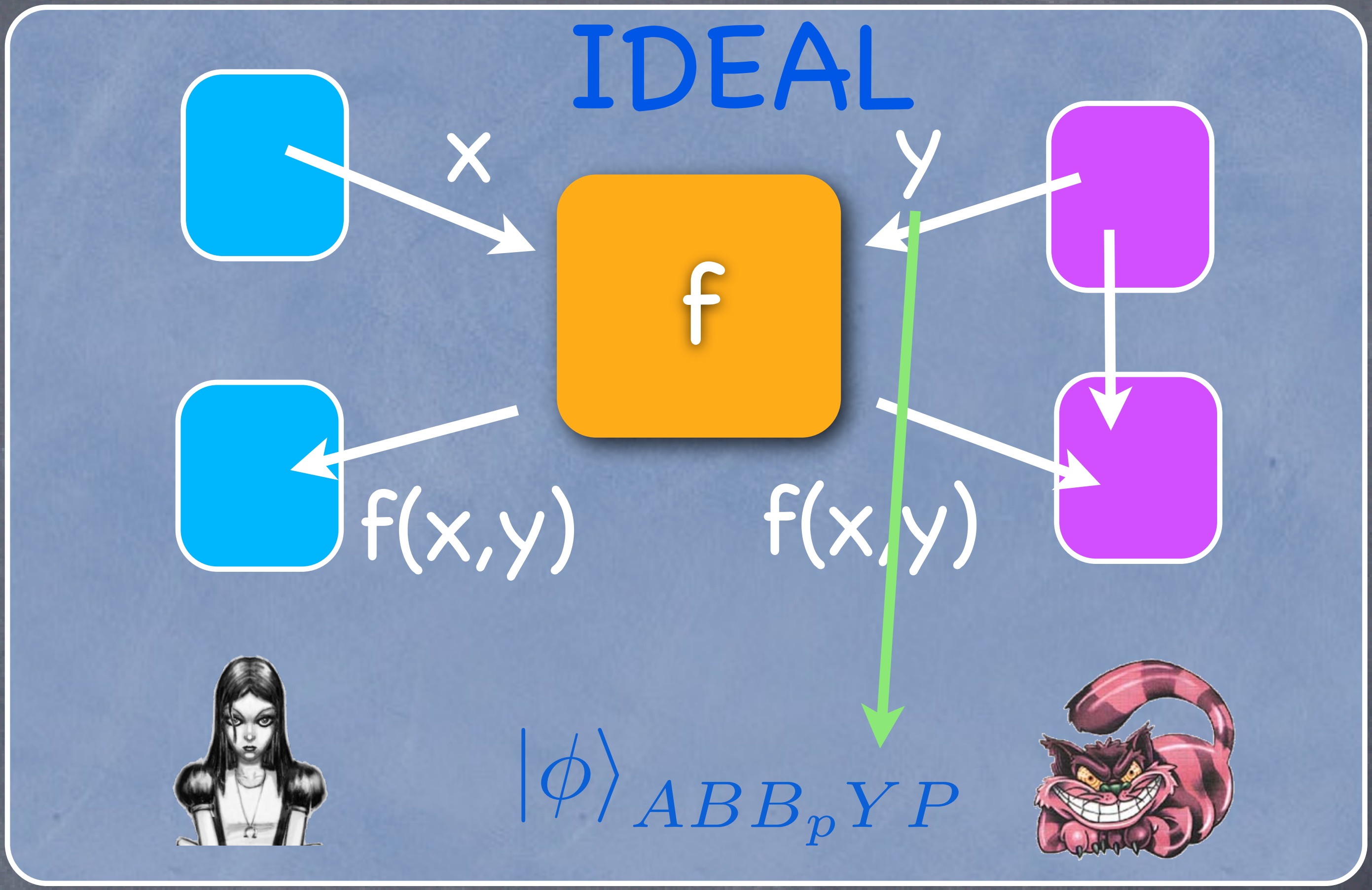
IDEAL



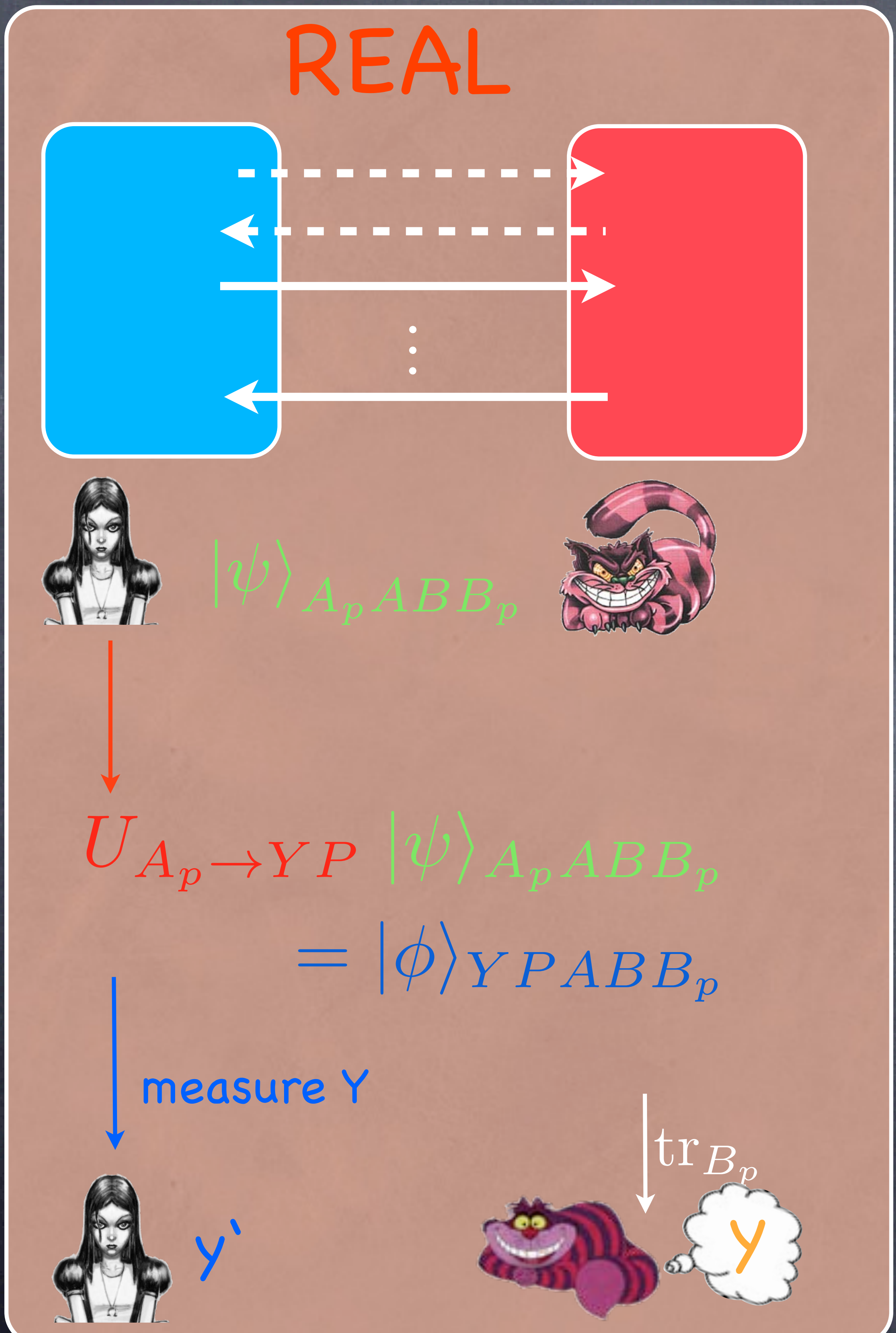
$$|\phi\rangle_{ABB_pYP}$$

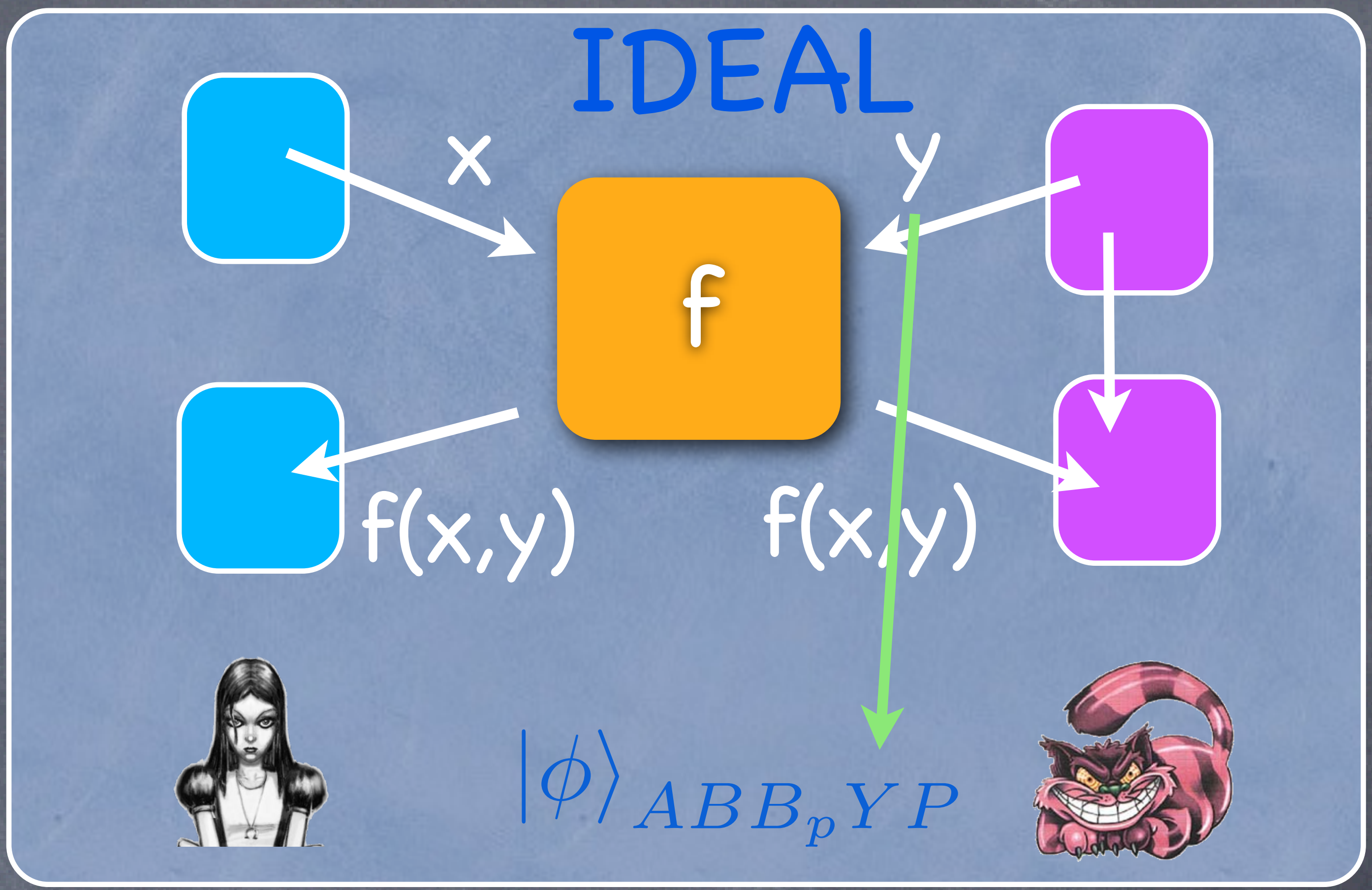
Proof of Insecurity



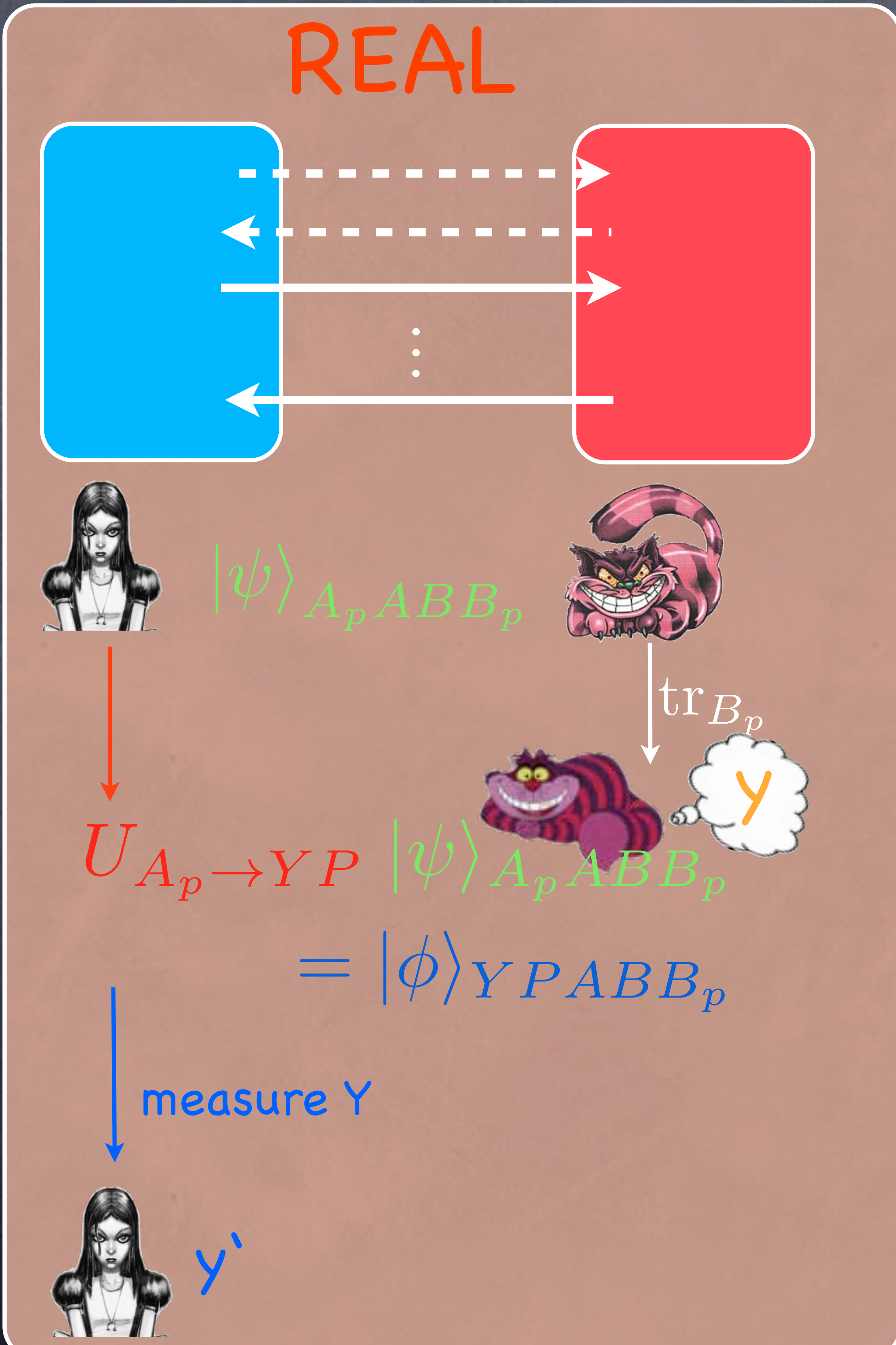


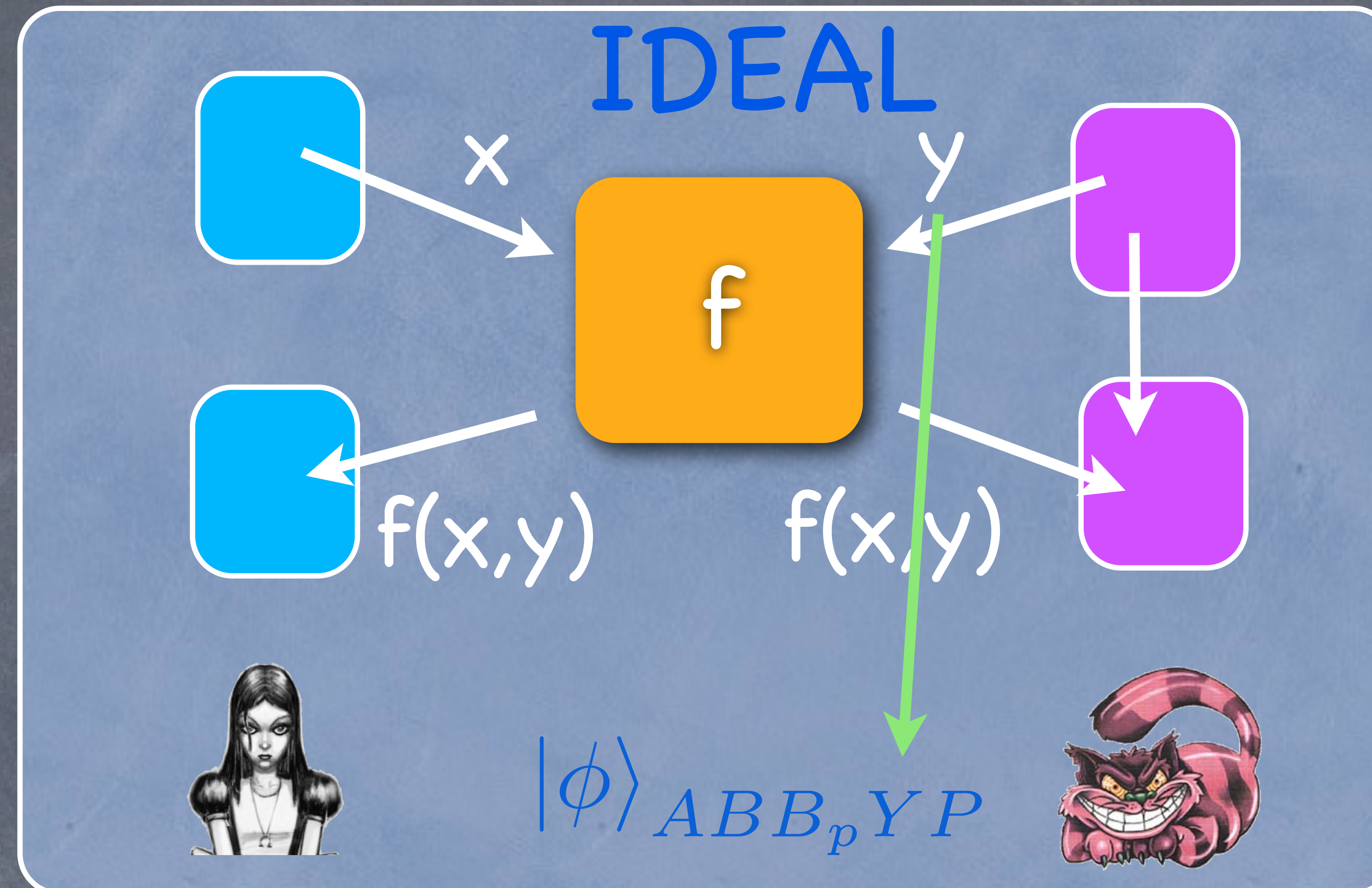
Proof of Insecurity



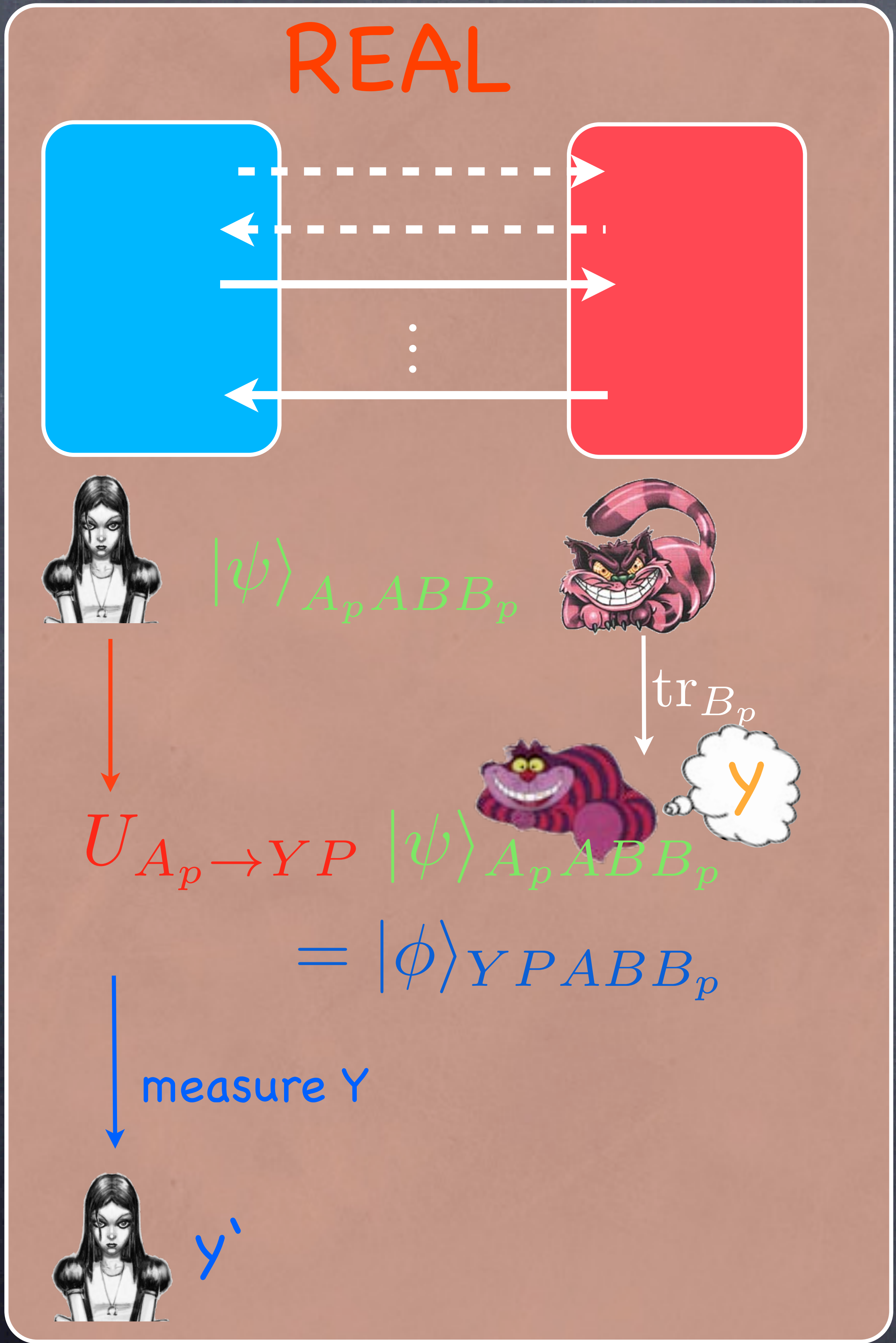


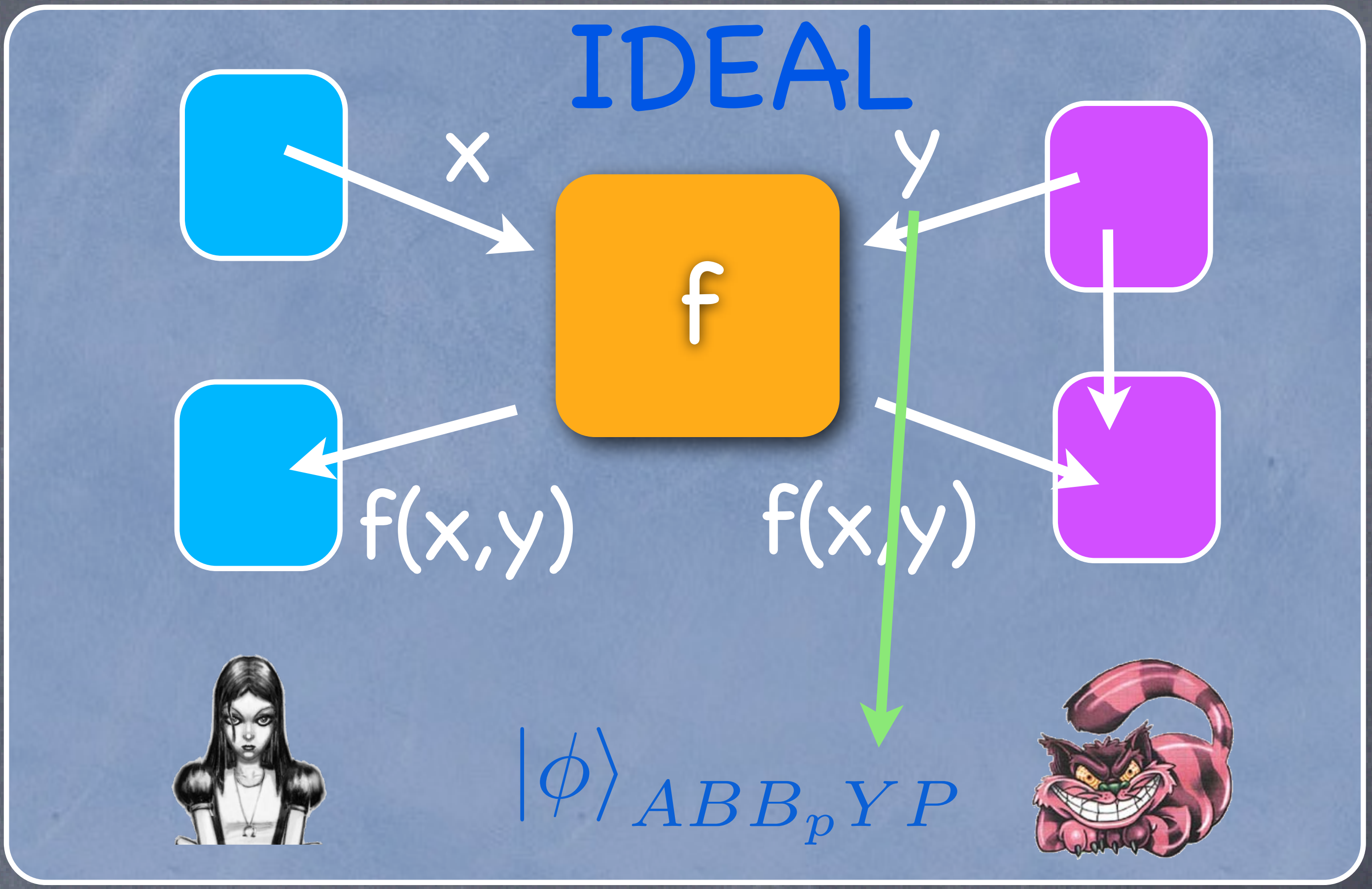
Proof of Insecurity





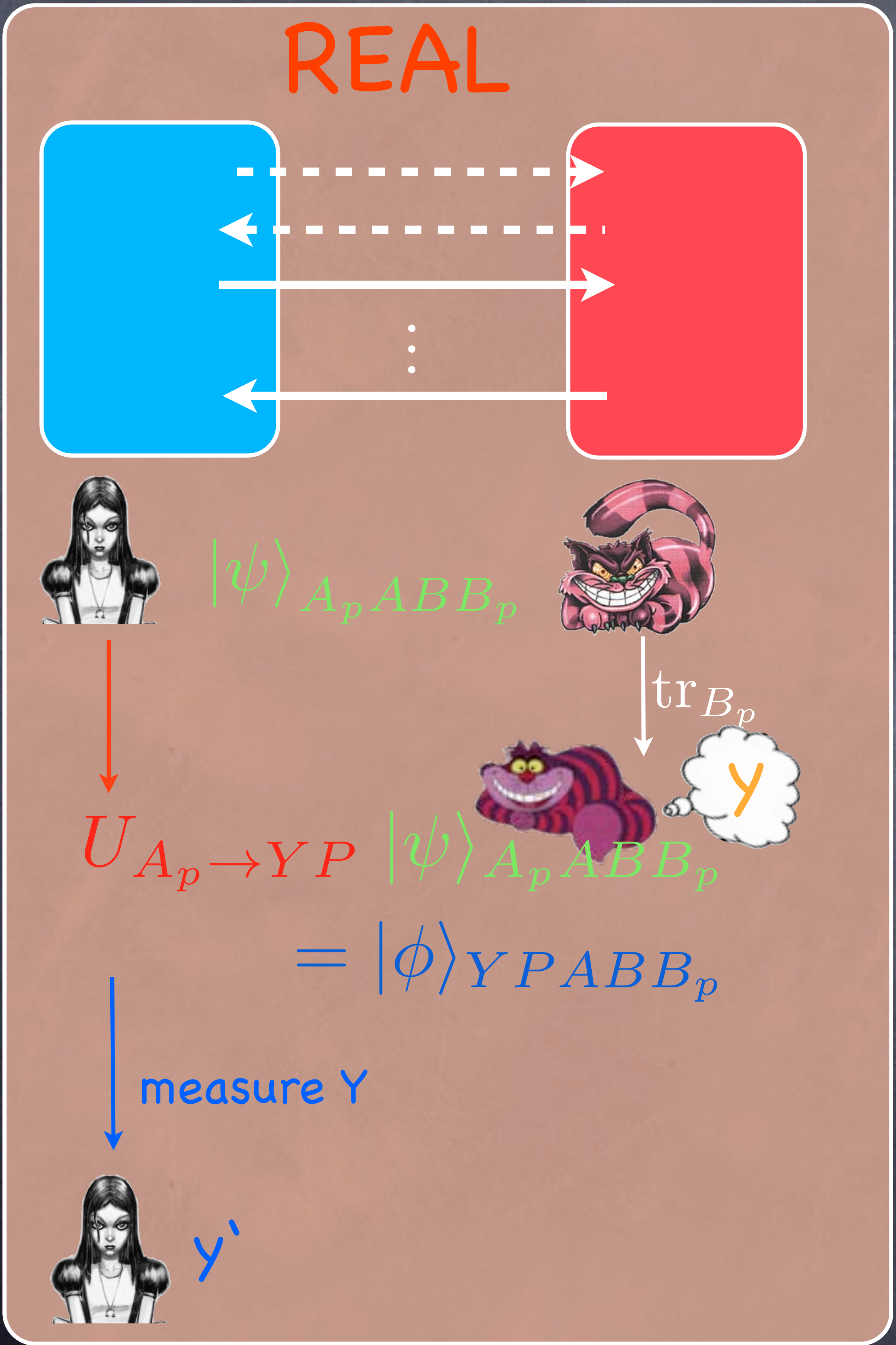
Proof of Insecurity

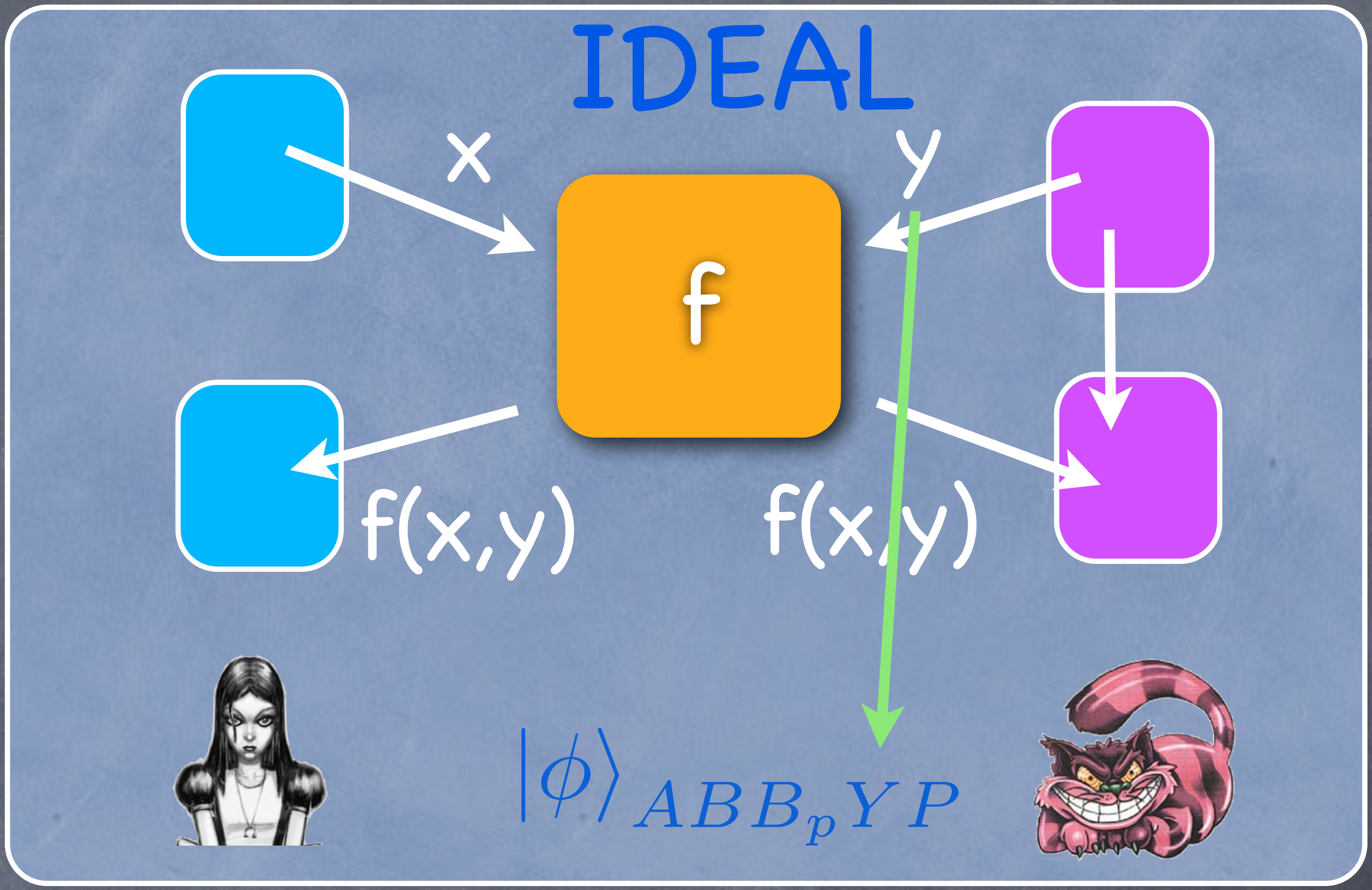




1. Alice plays „dishonestly" by purifying, Bob plays honestly

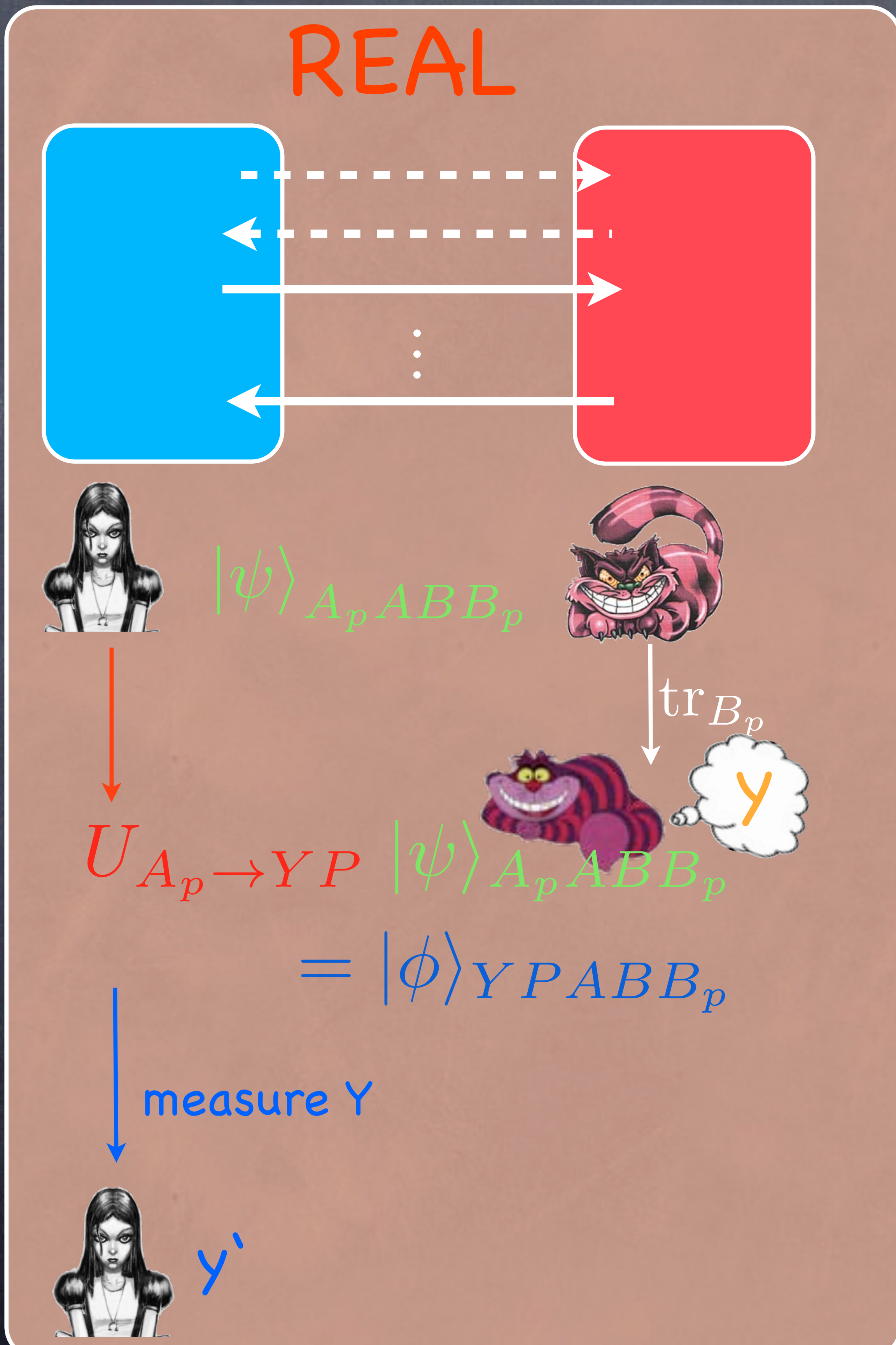
Proof of Insecurity

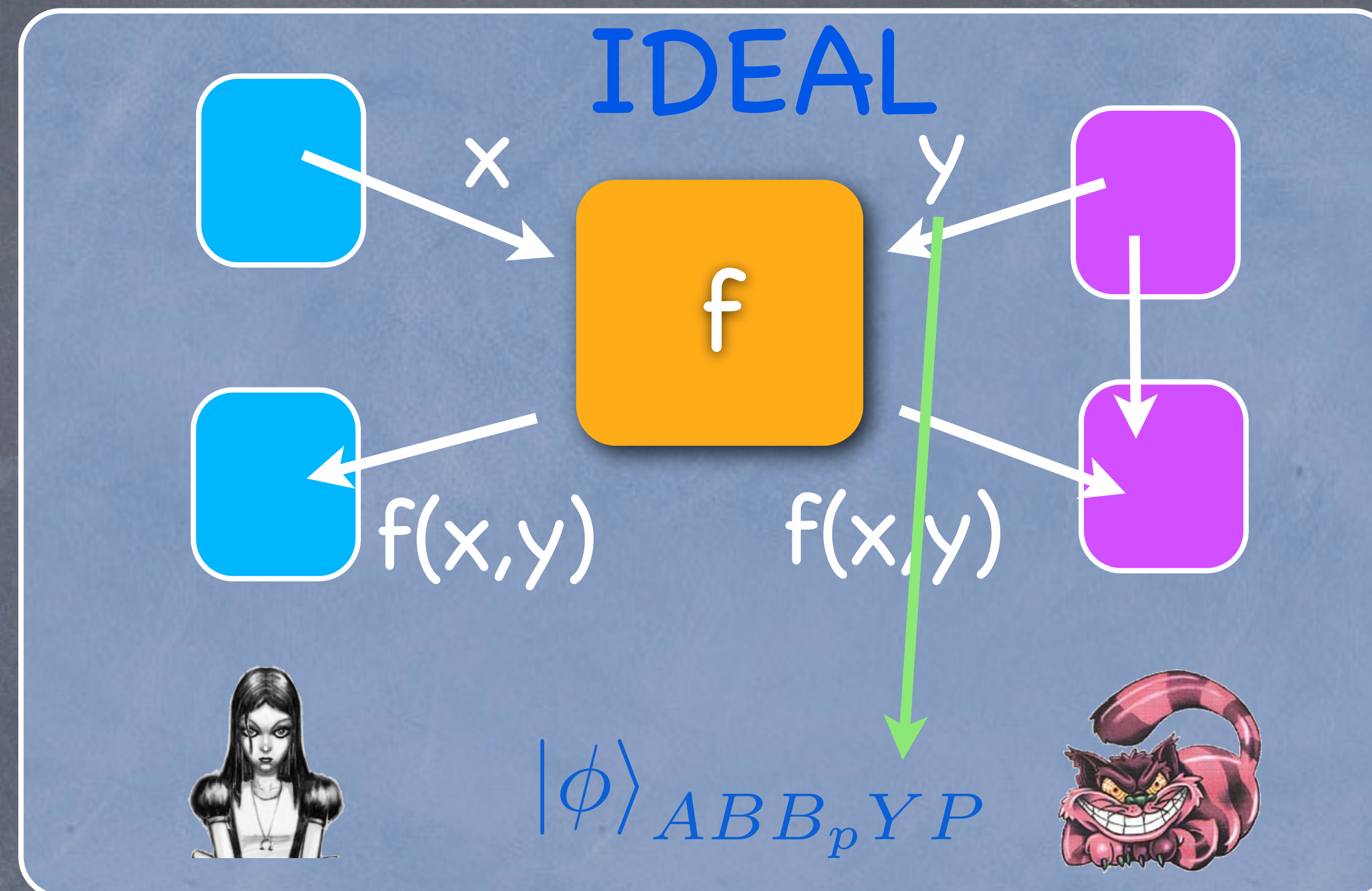




1. Alice plays „dishonestly" by purifying, Bob plays honestly
2. Alice applies cheating unitary U

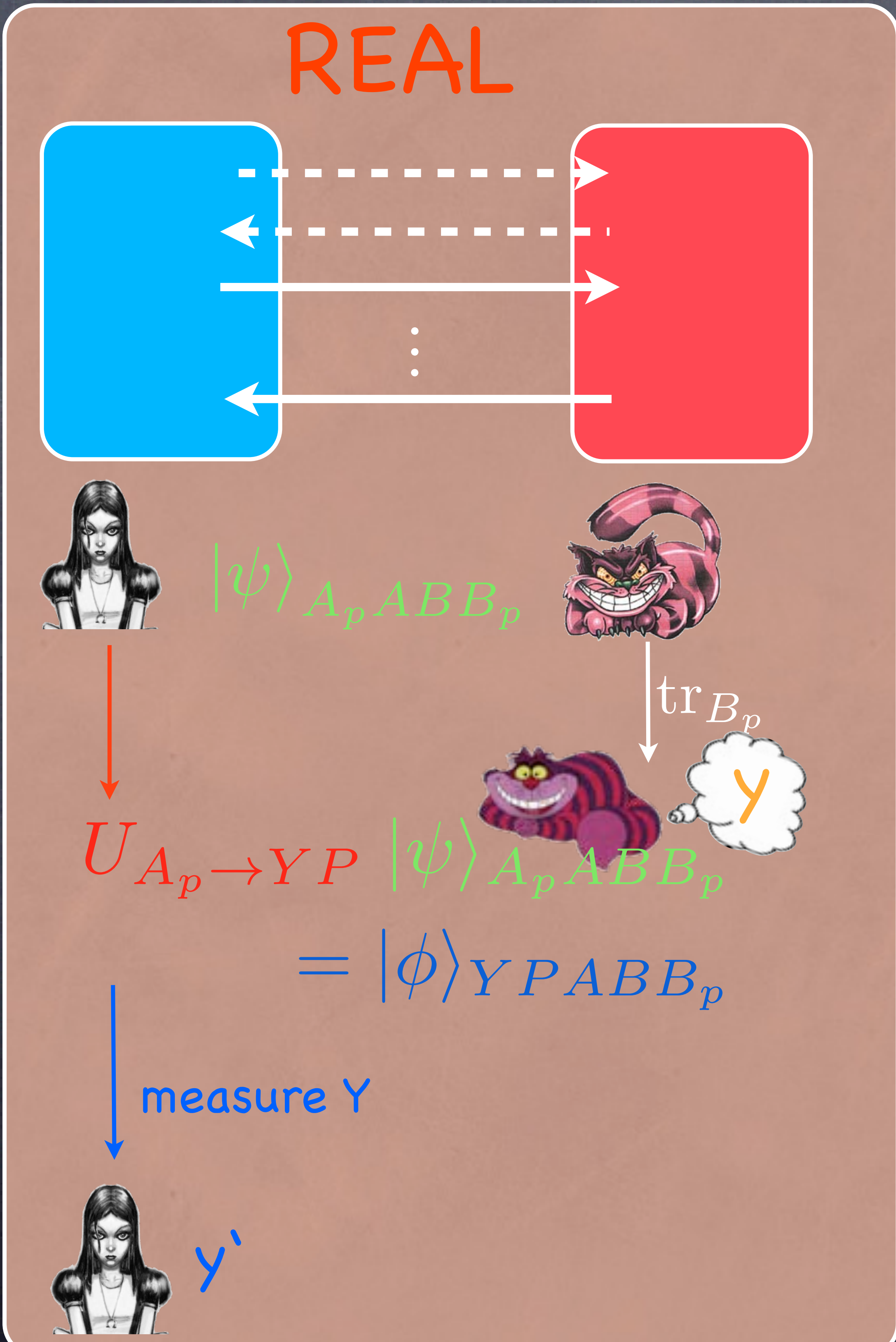
Proof of Insecurity

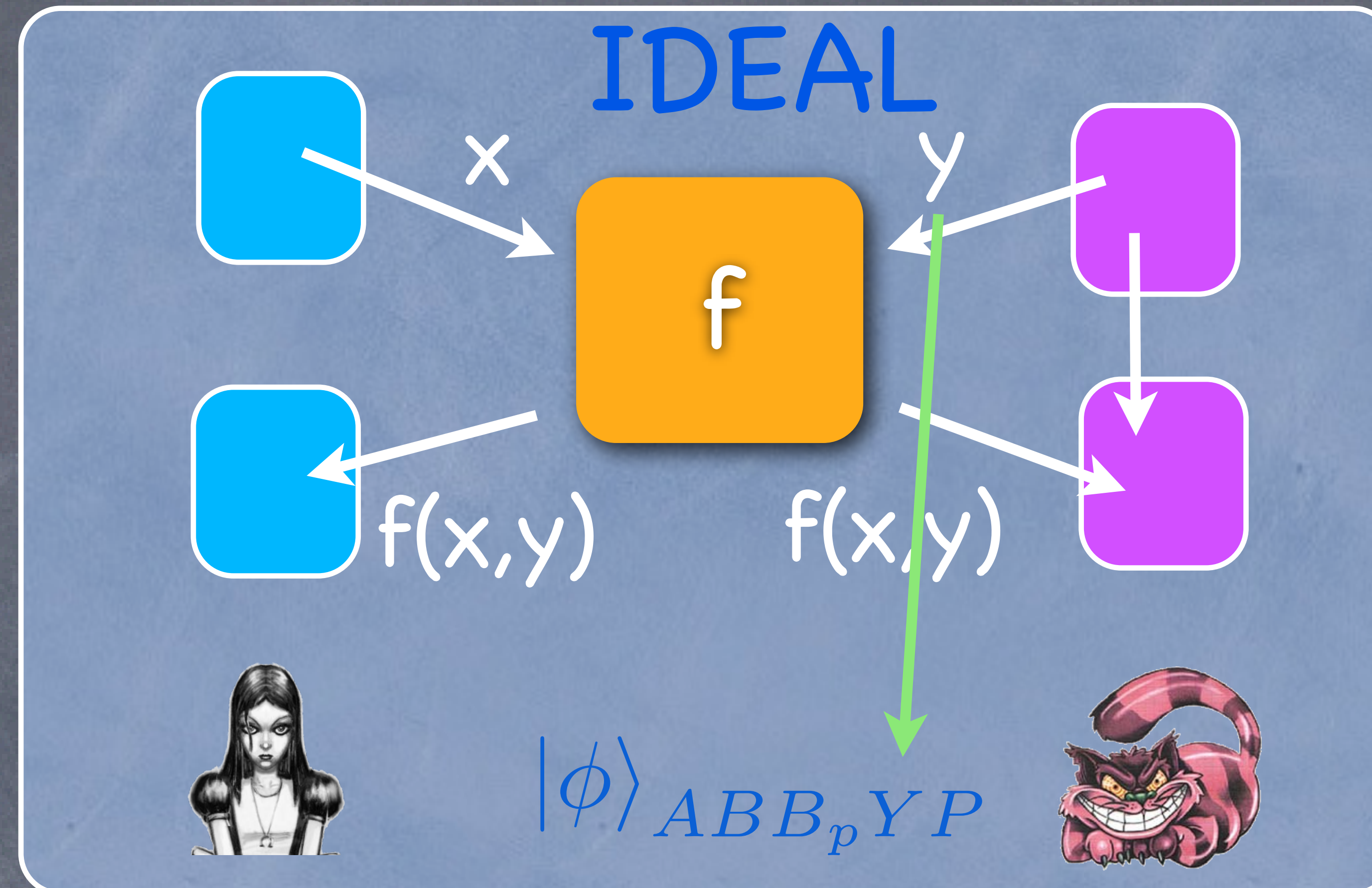




1. Alice plays „dishonestly" by purifying, Bob plays honestly
2. Alice applies cheating unitary U
3. measures register Y to obtain y'.

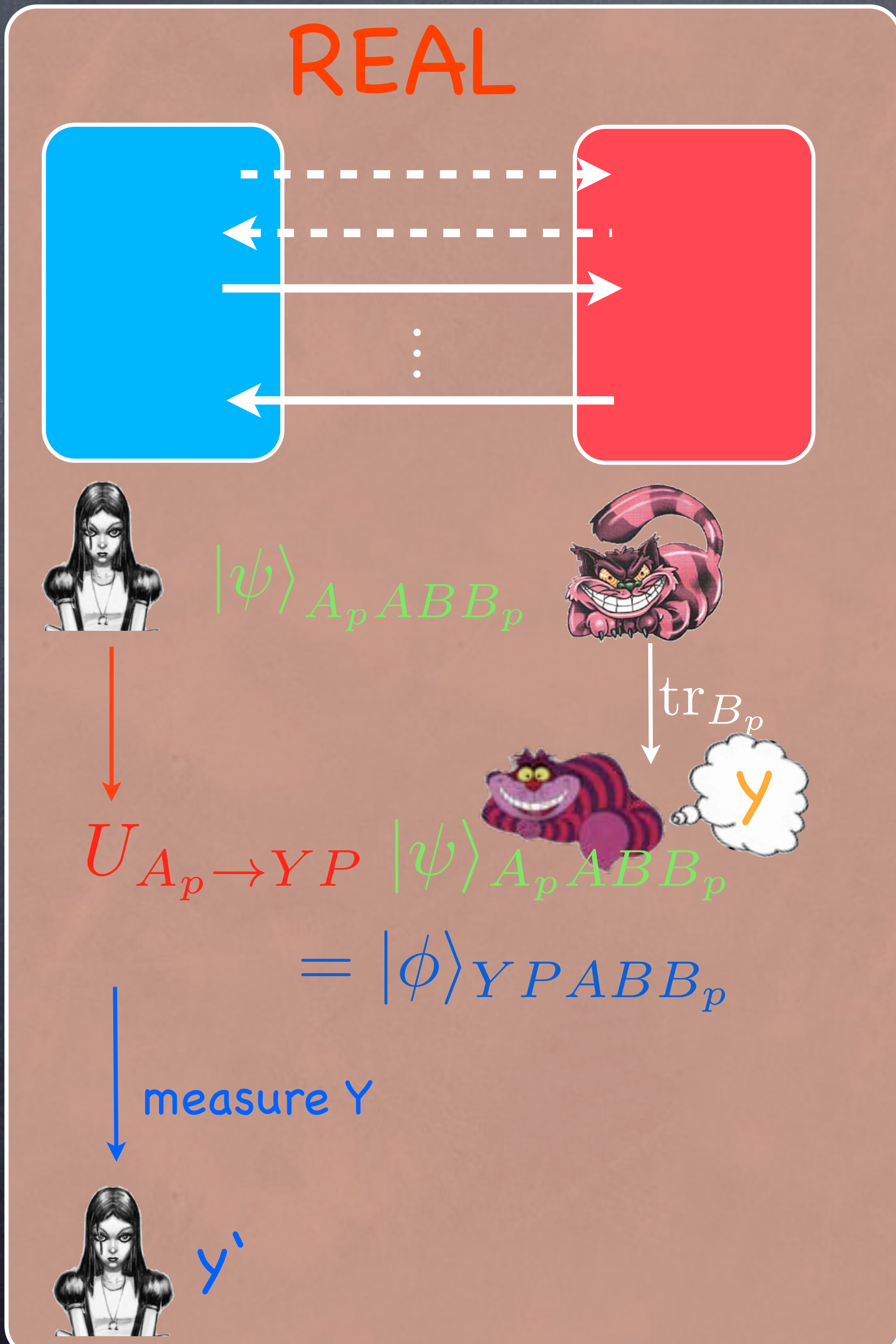
Proof of Insecurity

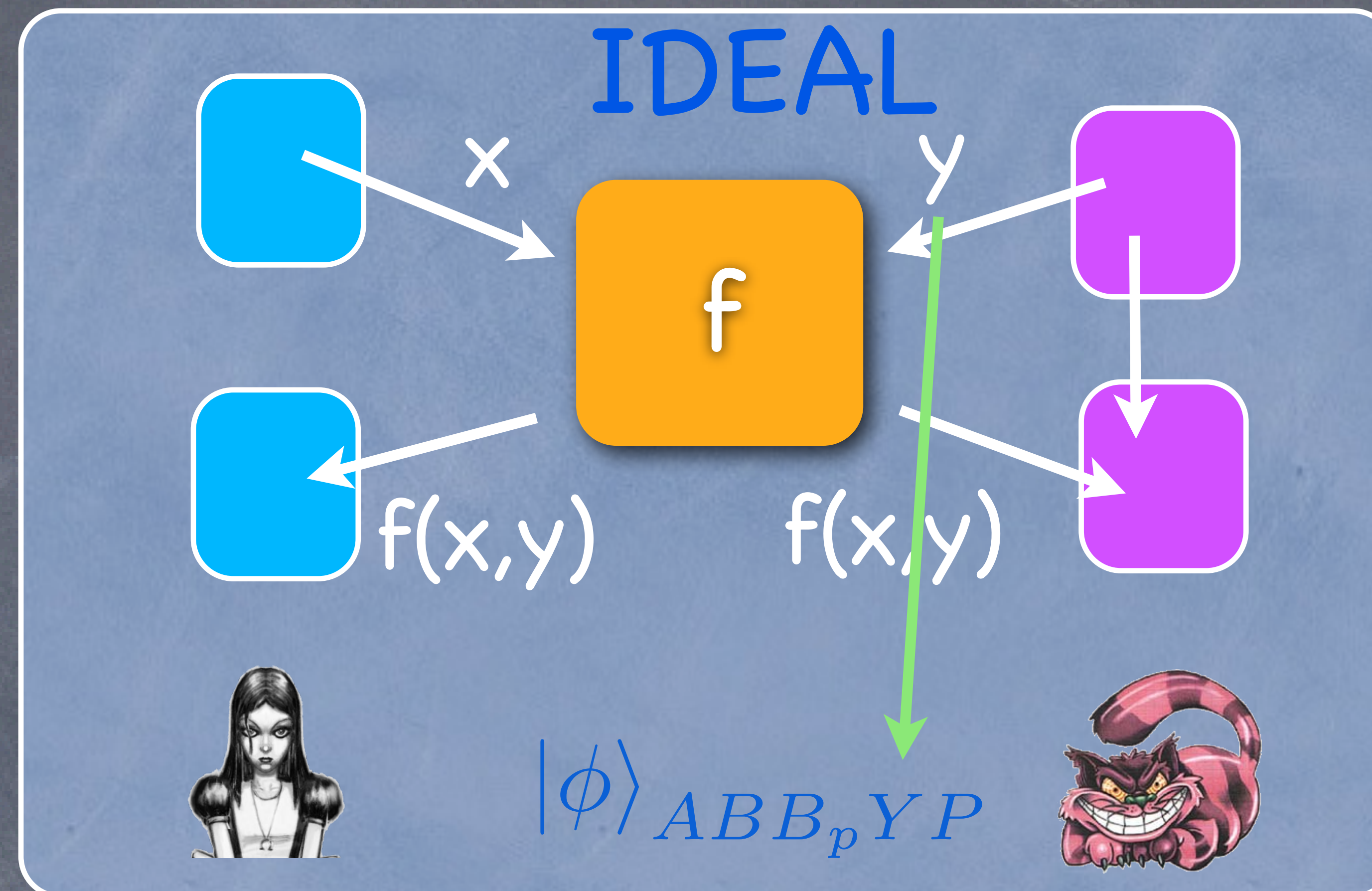




1. Alice plays „dishonestly“ by purifying, Bob plays honestly
2. Alice applies cheating unitary U
3. measures register Y to obtain y`.
4. since she only used purified strategy, correctness implies:
   for all x: f(x,y`) = f(x,y).

Proof of Insecurity



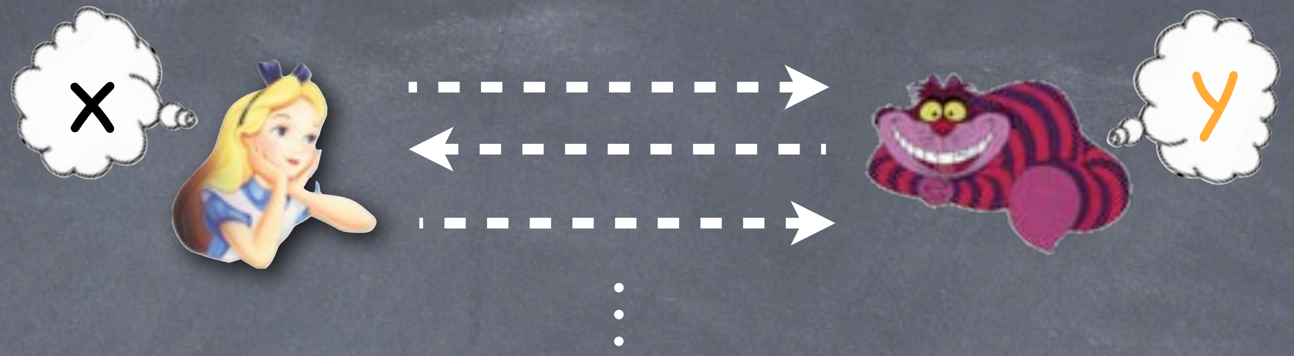


1. Alice plays „dishonestly" by purifying, Bob plays honestly
2. Alice applies cheating unitary U
3. measures register Y to obtain y`.
4. since she only used purified strategy, correctness implies: for all x: f(x,y`) = f(x,y).

$\square$

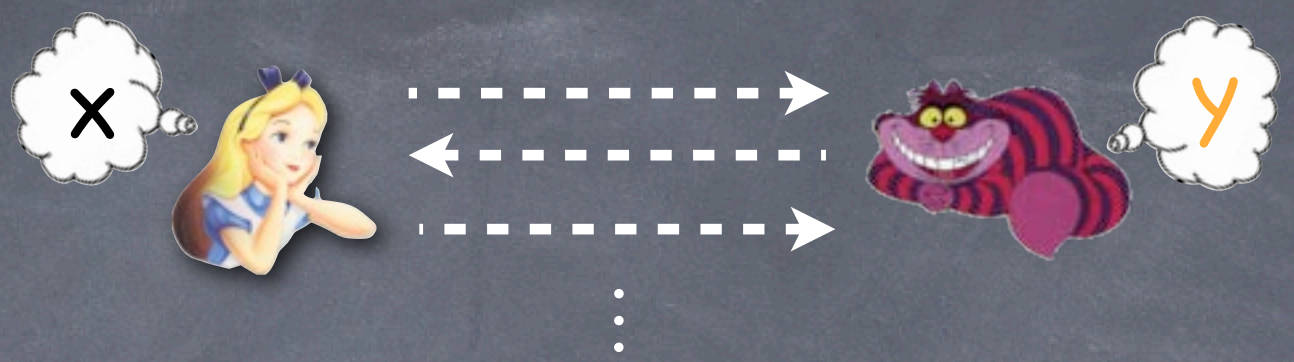
Error Case

Error Case



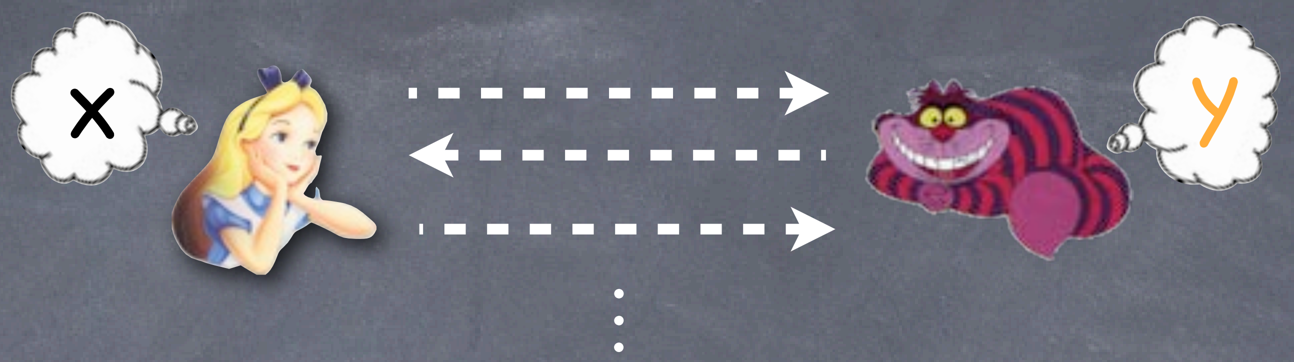
- our results also hold for ε-correctness and ε-security

Error Case



- our results also hold for ε-correctness and ε-security
- Alice gets a value y' with distribution $Q(y'|y)$ such that for all x: $\Pr_{y'}[\ f(x,y)=f(x,y')\ ] \geq 1-O(\varepsilon)$

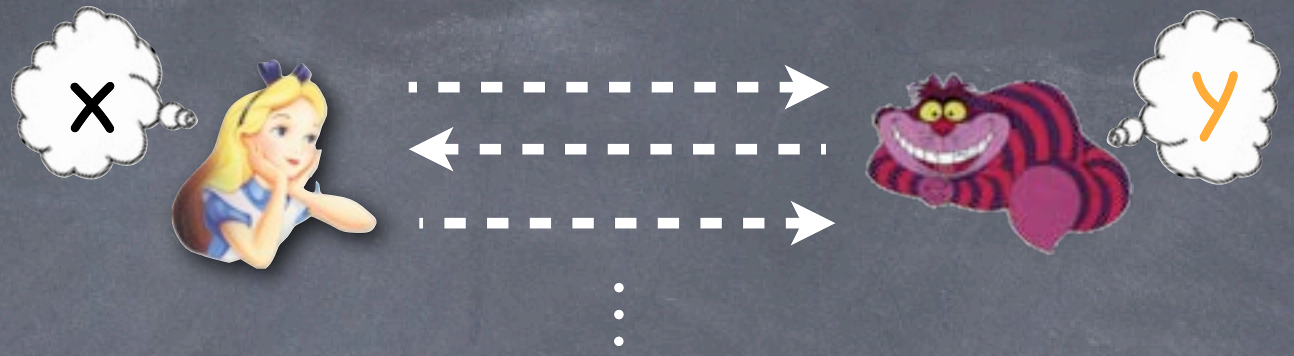
Error Case



- our results also hold for ε-correctness and ε-security
- Alice gets a value y' with distribution $Q(y'|y)$ such that for all x: $\Pr_{y'}[\ f(x,y)=f(x,y')\ ] \geq 1-O(\varepsilon)$

optimal: disjointnes

Error Case



- our results also hold for ε-correctness and ε-security
- Alice gets a value y' with distribution $Q(y'|y)$ such that for all x: $\Pr_{y'}[\ f(x,y)=f(x,y')\ ] \geq 1-O(\varepsilon)$

optimal: disjointnes

- in contrast to Lo's proof where the overall error increases linearly with the number of inputs.

Error Case

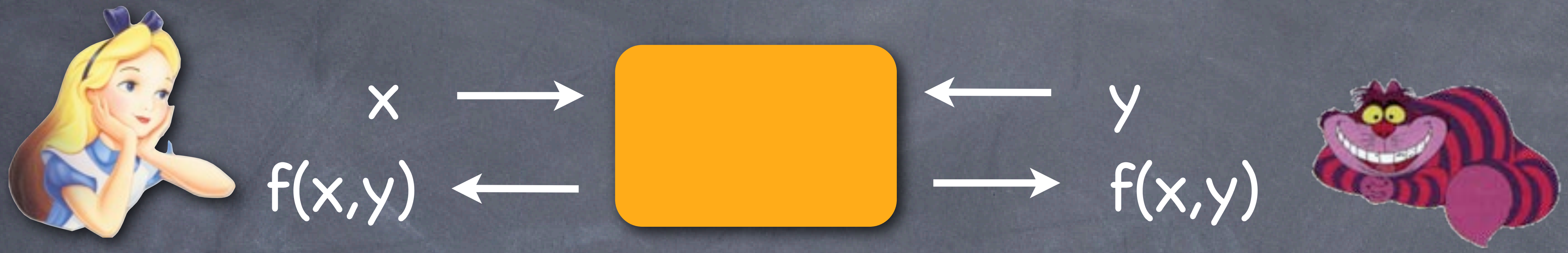
- our results also hold for ε-correctness and ε-security
- Alice gets a value y' with distribution $Q(y'|y)$ such that for all x: $\Pr_{y'}[\ f(x,y)=f(x,y')\ ] \geq 1-O(\varepsilon)$

optimal: disjointnes

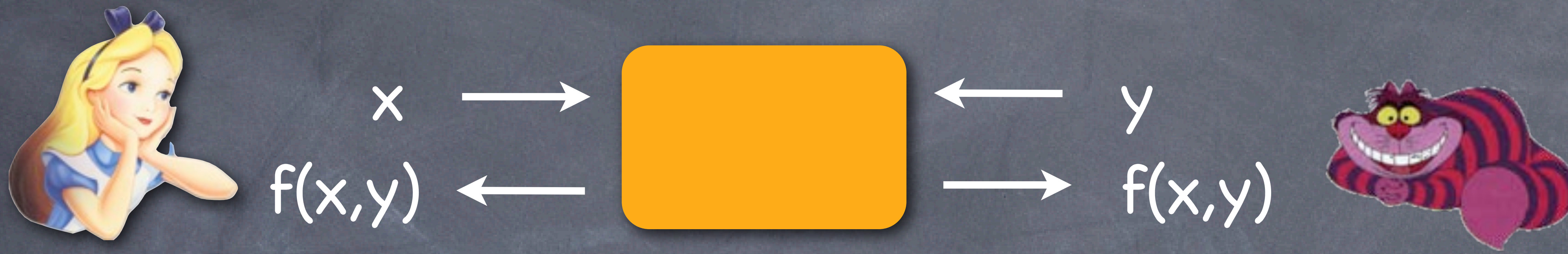
- in contrast to Lo's proof where the overall error increases linearly with the number of inputs.
- crucial use of von Neumann's minimax theorem

motivated from strong no bit commitment result
[D'Ariano Kretschmann Schlingemann Werner, 2007]

Conclusion & Open Problems

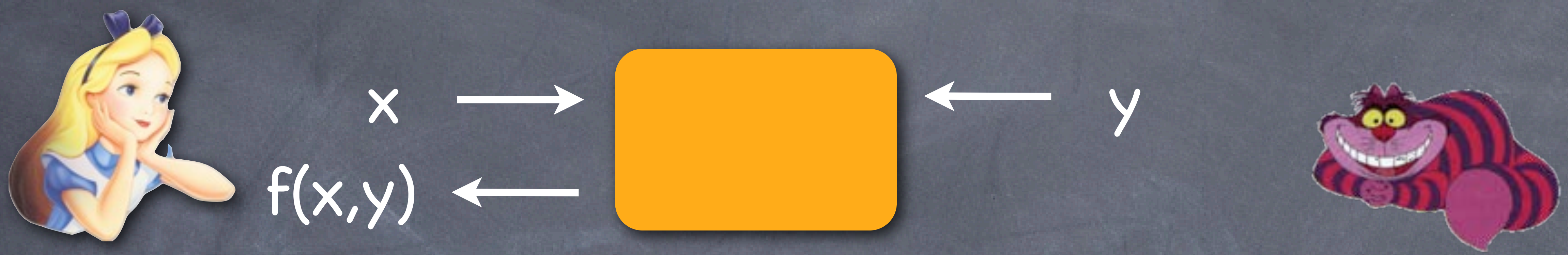


Conclusion & Open Problems



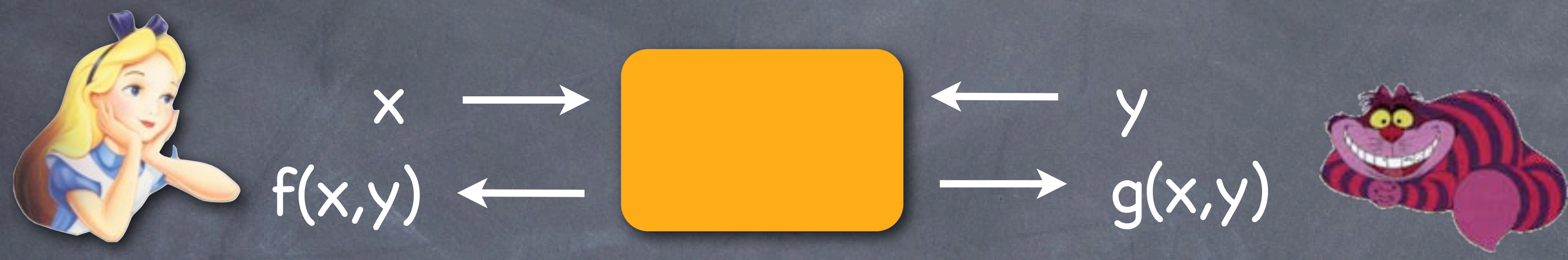
- secure two-party computation not possible

Conclusion & Open Problems



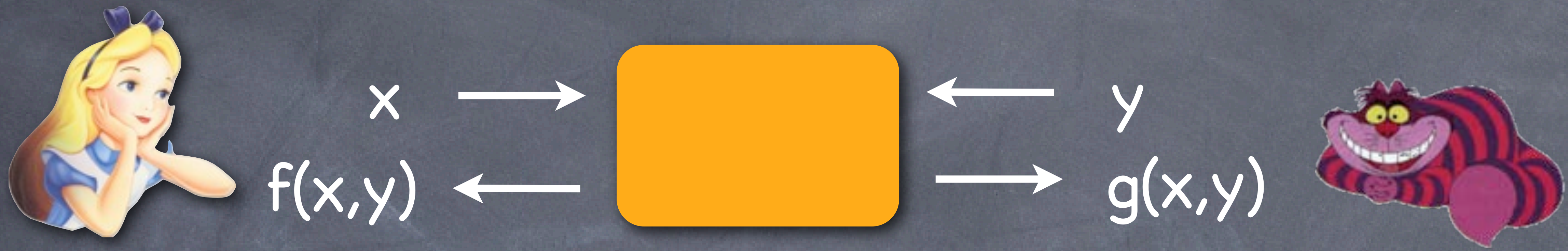
- secure two-party computation not possible

Conclusion & Open Problems



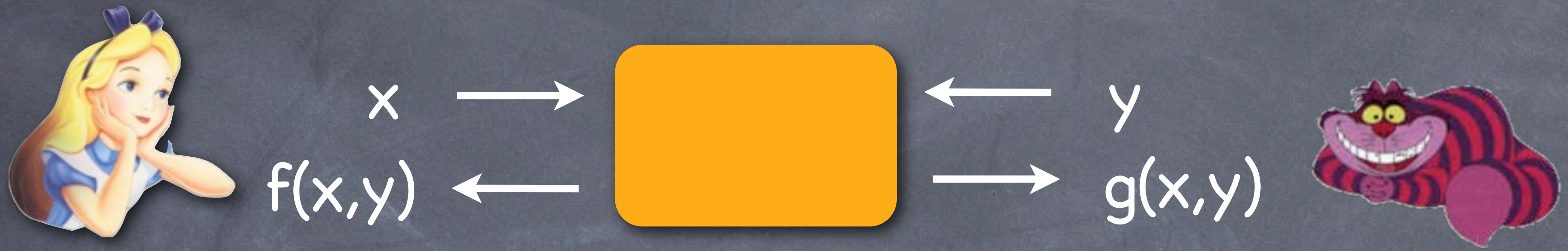
- secure two-party computation not possible

Conclusion & Open Problems



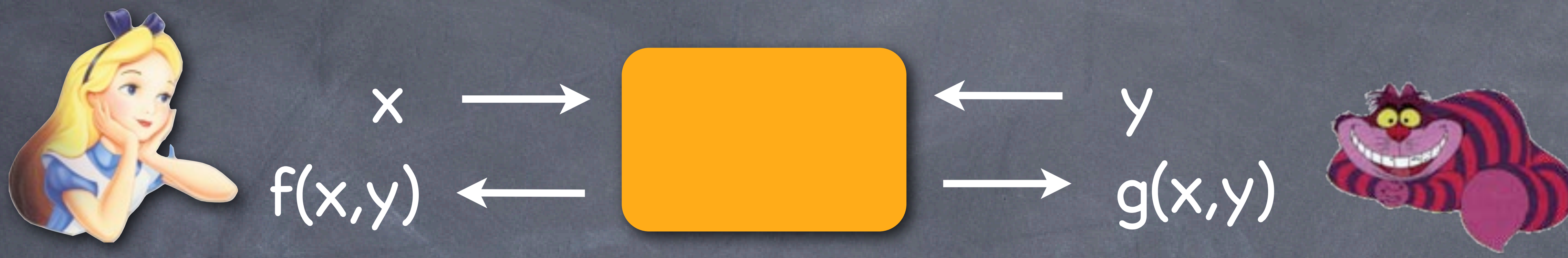
- secure two-party computation not possible
- weaker security definition?

Conclusion & Open Problems



- secure two-party computation not possible
- weaker security definition?
- randomized functions?

Conclusion & Open Problems



- secure two-party computation not possible
- weaker security definition?
- randomized functions?

Thank you!