Complete Insecurity of Quantum Protocols for Classical Two-Party Computation

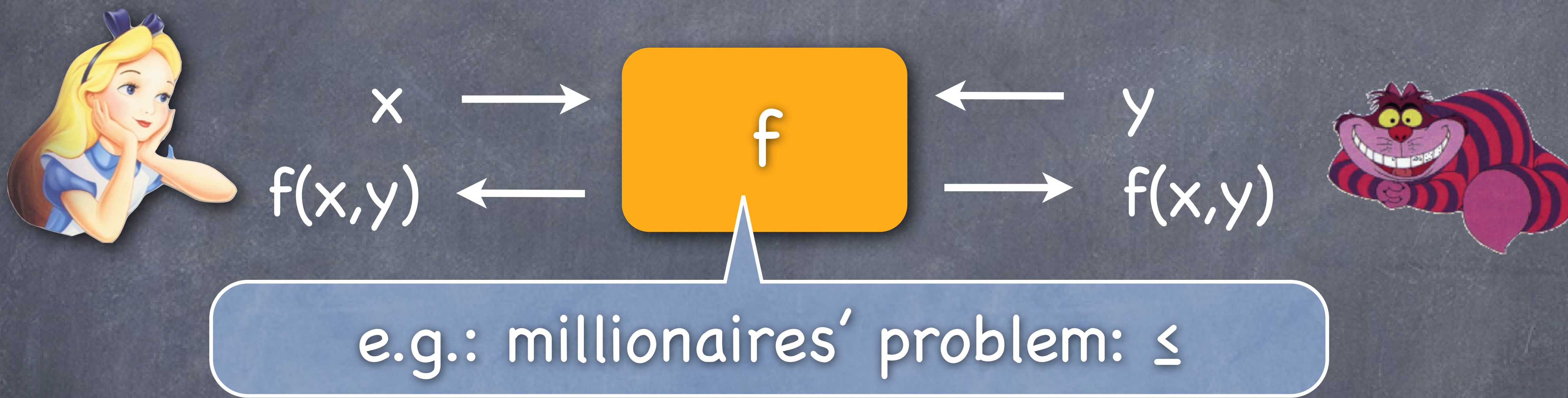
Harry Buhrman (CWI, University of Amsterdam)
Matthias Christandl (ETH Zurich)
Christian Schaffner (University of Amsterdam, CWI)

QCRYPT 2012, Thursday, 13th September
(arxiv, to appear in PRL)

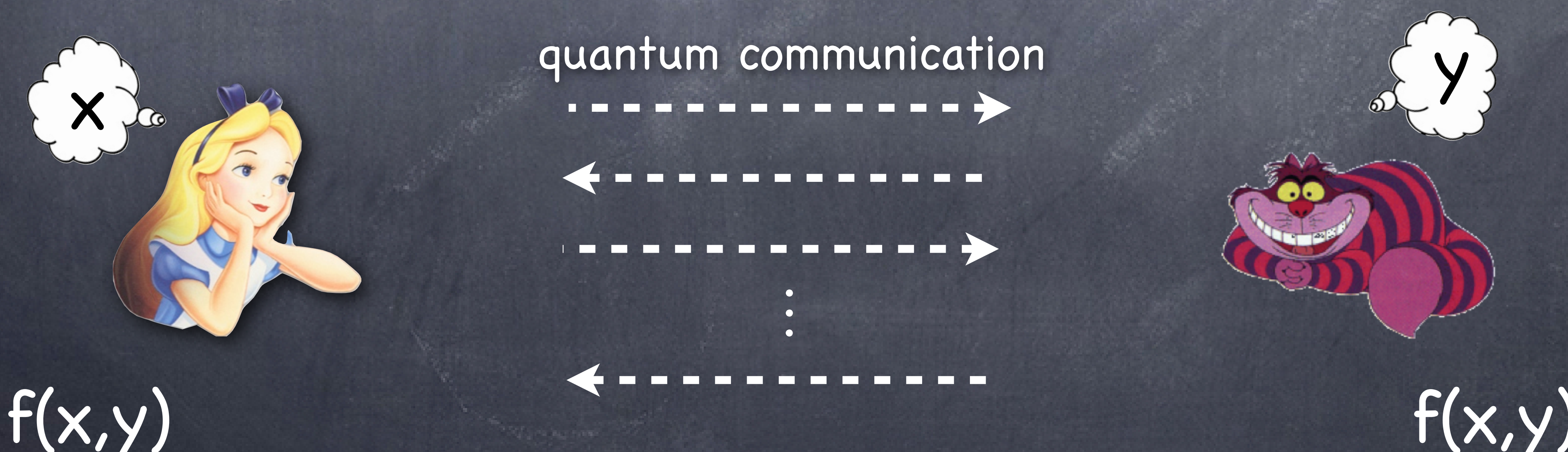
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

Motivation

- ideally: Alice & Bob have a box computing f on private inputs x and y

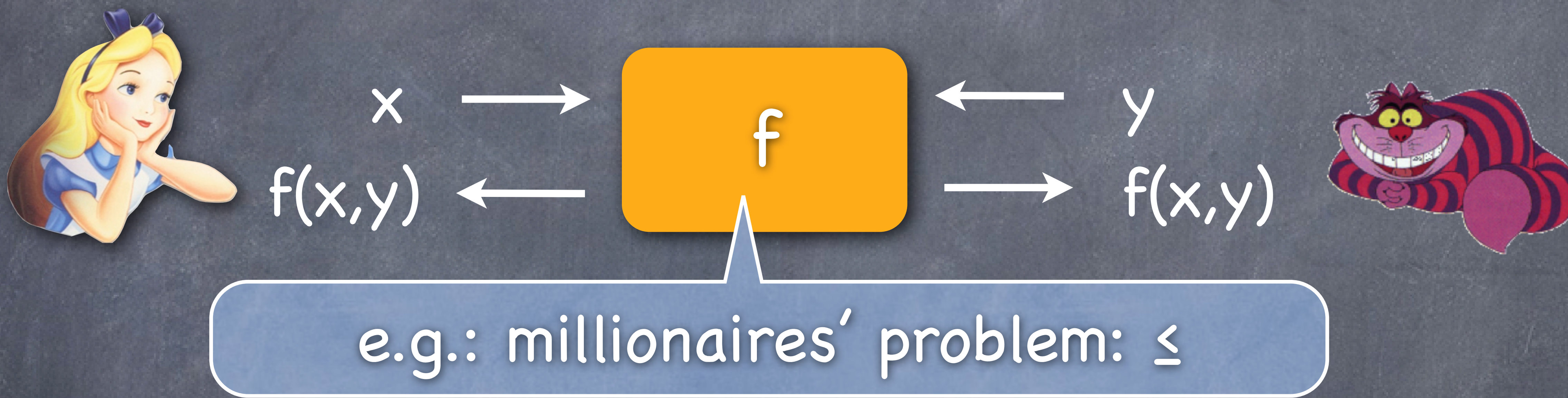


- reality: Alice and Bob perform a protocol

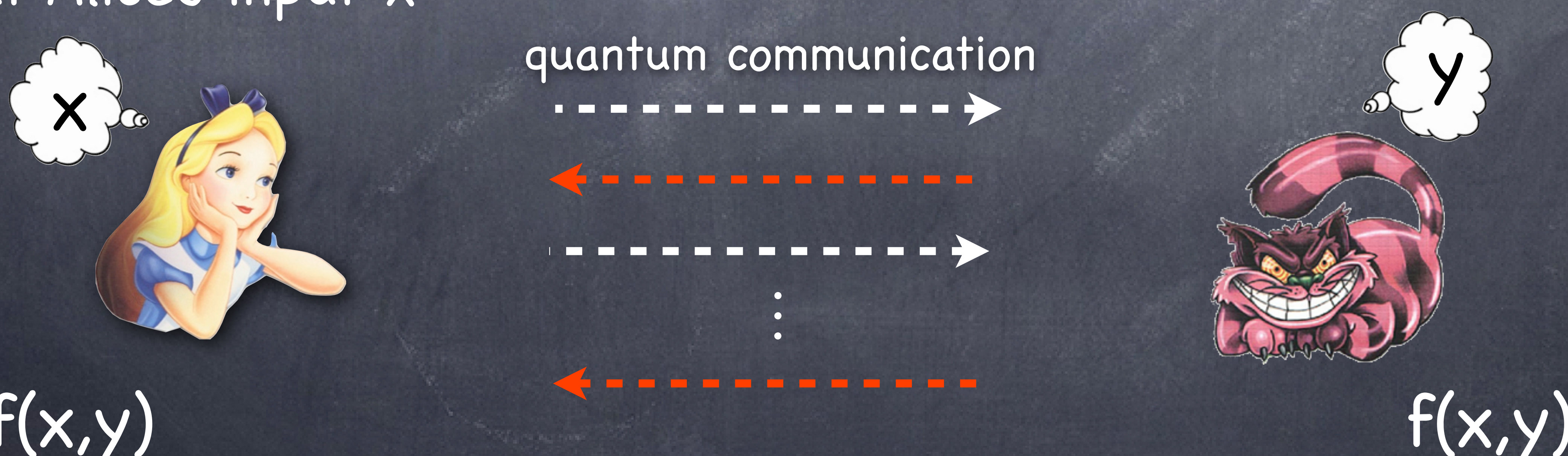


Motivation

- ideally: Alice & Bob have a box computing f on private inputs x and y



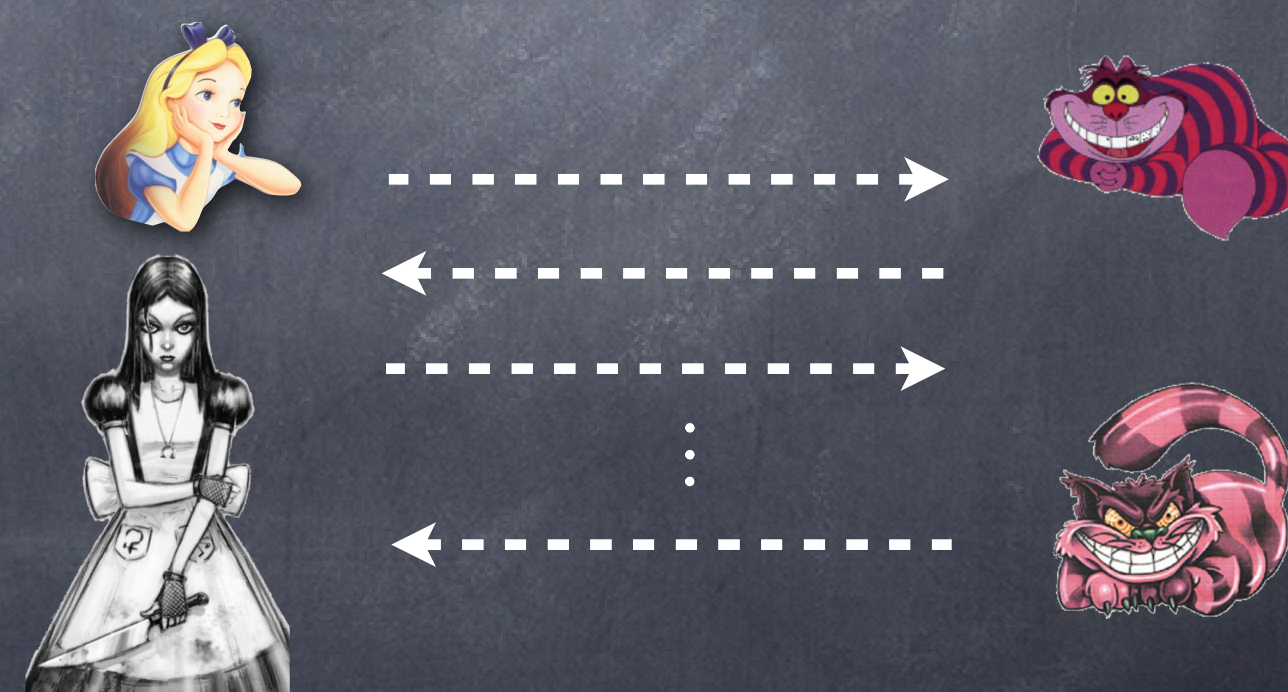
- reality: dishonest Bob might deviate from protocol to learn more about Alice's input x



Secure Function Evaluation

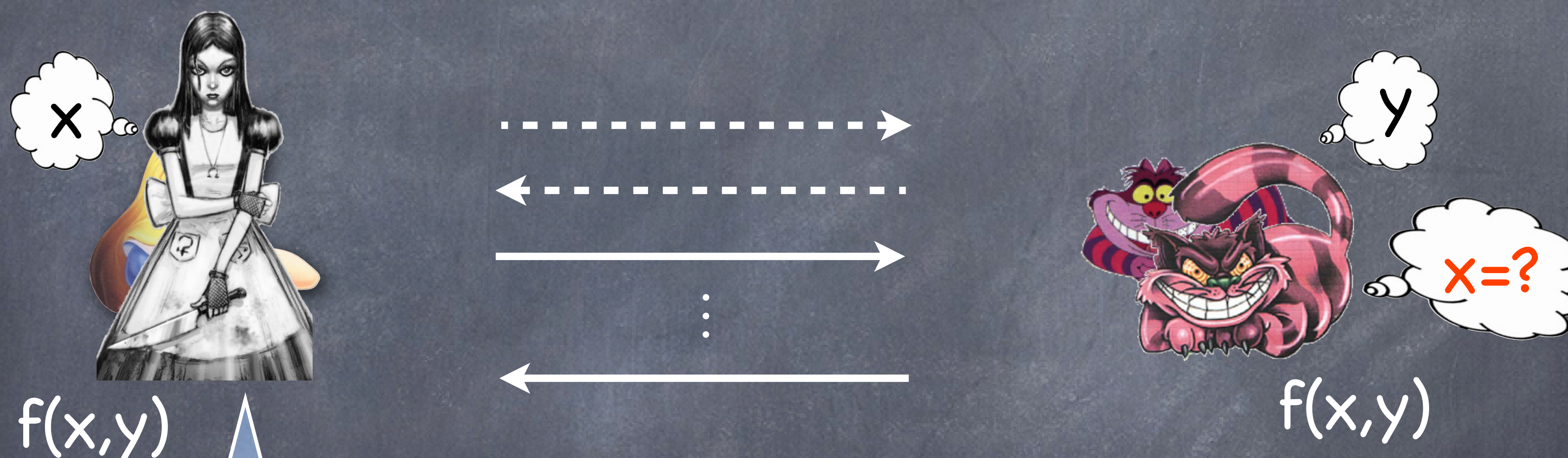
- ideally: Alice & Bob have a box computing f on private inputs x and y

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



Main Impossibility 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.



after protocol: dishonest Alice can compute $f(x,y)$ not just for one x, but 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 $1-O(\varepsilon)$.

History

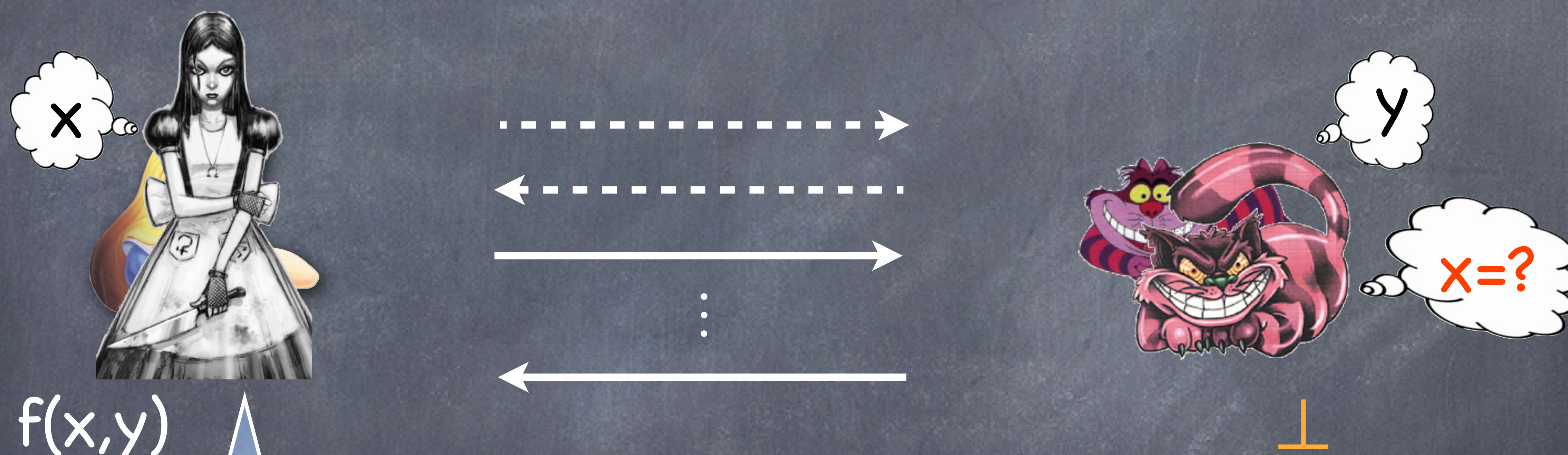
- ~1970: Conjugate Coding [Wiesner]
- 1984: Quantum Key Distribution [Bennett Brassard]
- ~1991: Bit Commitment and Oblivious Transfer?
- 1997: No Bit Commitment [Lo Chau, Mayers]
- 1997: No One-Sided Secure Computation [Lo]
- Really no Quantum Bit Commitment?
- 2007: No BC [D'Ariano Kretschmann Schlingemann Werner]
- 2007: Some Functions are Impossible [Colbeck]
- 2009: Secure Computation has to Leak Information [Salvail Sotakova Schaffner]
- this work: Complete Insecurity of Two-Sided Deterministic Computations

Talk Outline

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

[Lo97] Impossibility 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.

- holds only for one-sided computations
- error increases with number of inputs

[Lo97] Impossibility Result

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
- for dishonest Bob inputting y in superposition, define:

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

- security against dishonest Bob:

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

[Lo97] Impossibility Result

$\vdots$

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

- security against dishonest Bob:

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

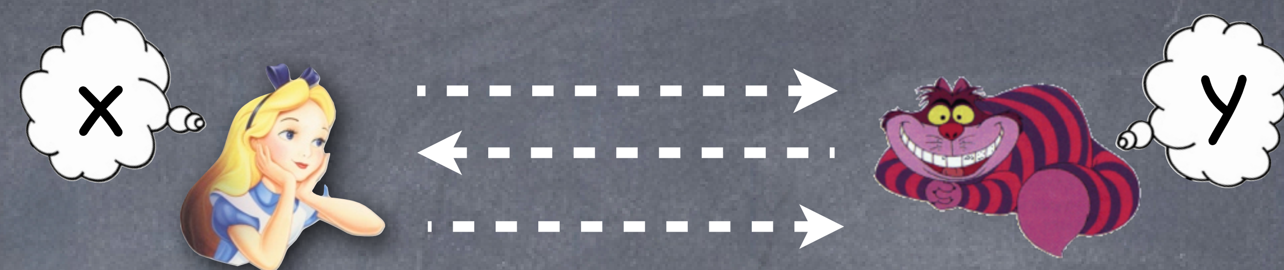
- implies existence of cheating unitary for Alice: (not dep on y)

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

- dishonest Alice starts with input x_0, can read out f(x_0,y), switches to x_1, reads out f(x_1,y) etc.

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

Two-Sided Comp?



f(x,y) ⋮ f(x,y)

- ~~only~~ Bob& Alice get~~s~~ output
- wlog measurements are moved to the end, final state is pure
- for dishonest Bob inputting y in superposition, define:

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

- security against dishonest Bob:

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

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

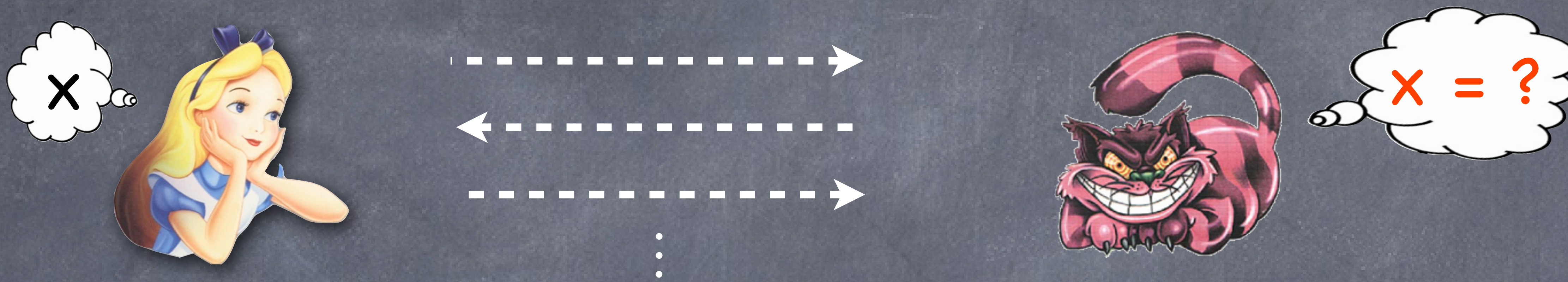
$$(U_A \otimes \mathbb{I}_B)\,|\psi^{x_0}\rangle_{AB} =$$

trouble starts here...

- dishonest Alice starts with input x_0, can read out $f(x_0,y)$, switches to x_1, reads out $f(x_1,y)$ etc.

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

Security Against Players With Output



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

- security against dishonest Bob without output:

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

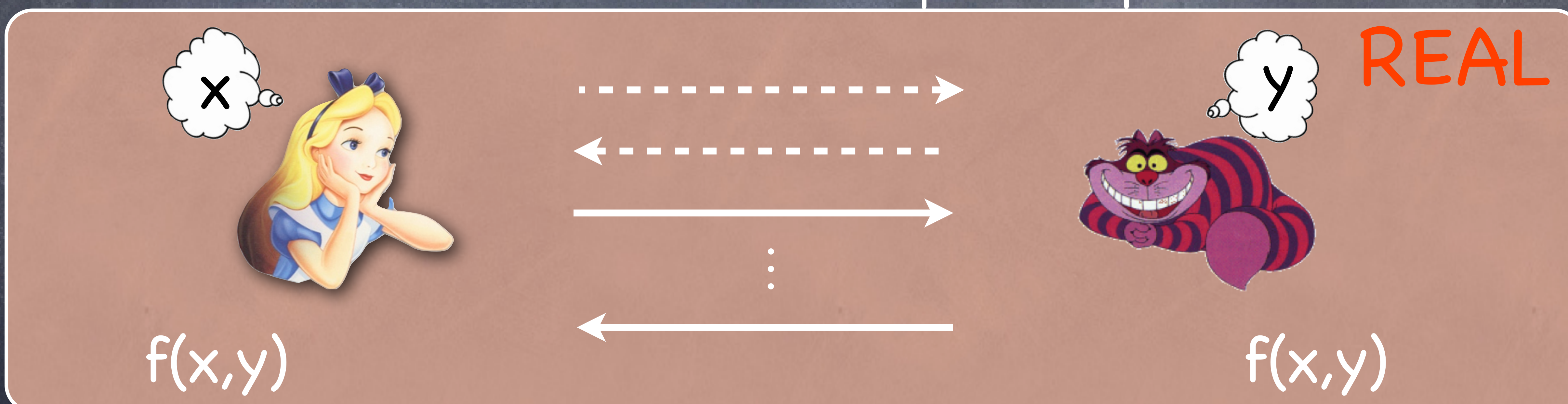
- but given f(x,y) ??? (e.g. in the millionaire's problem)
- precise formalisation of intuitive notion of "not learning more than f(x,y)" is non-trivial

use the real/ideal paradigm

Security Definition

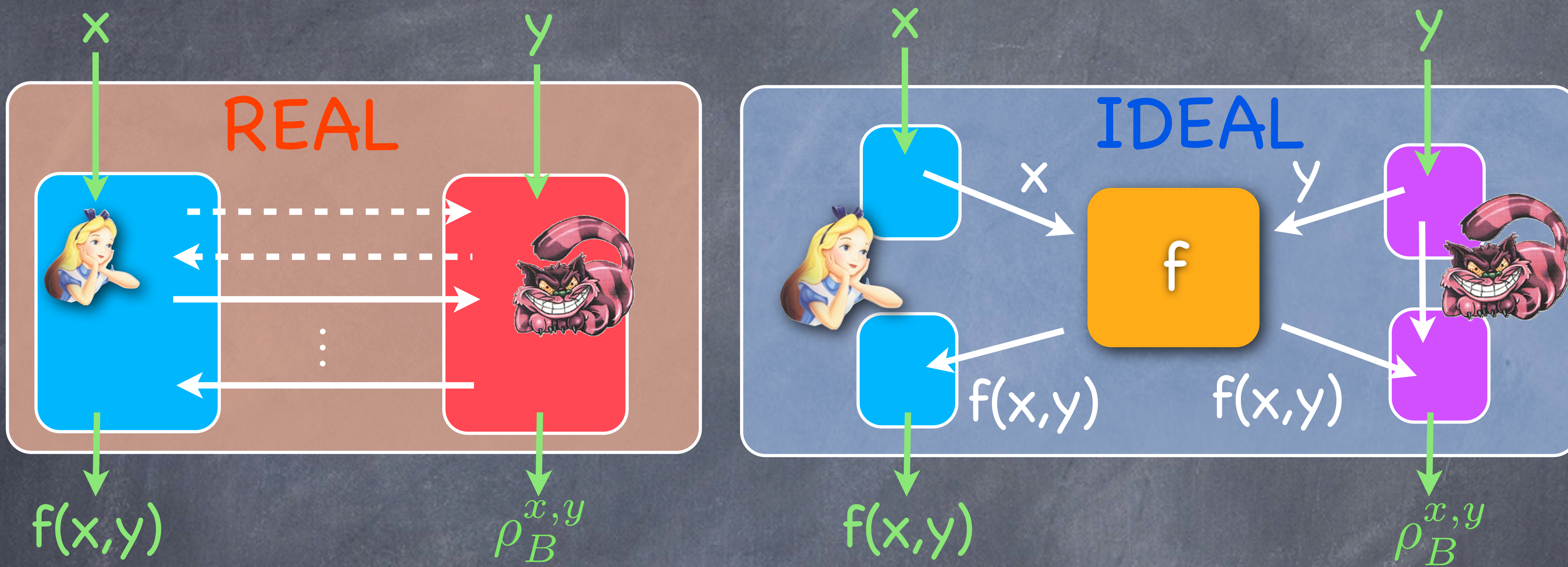
- we want: Alice & Bob interact with the ideal functionality

- we have: Alice & Bob interact in a quantum protocol



security holds if REAL looks like IDEAL to the outside world

More Formal Security Definition

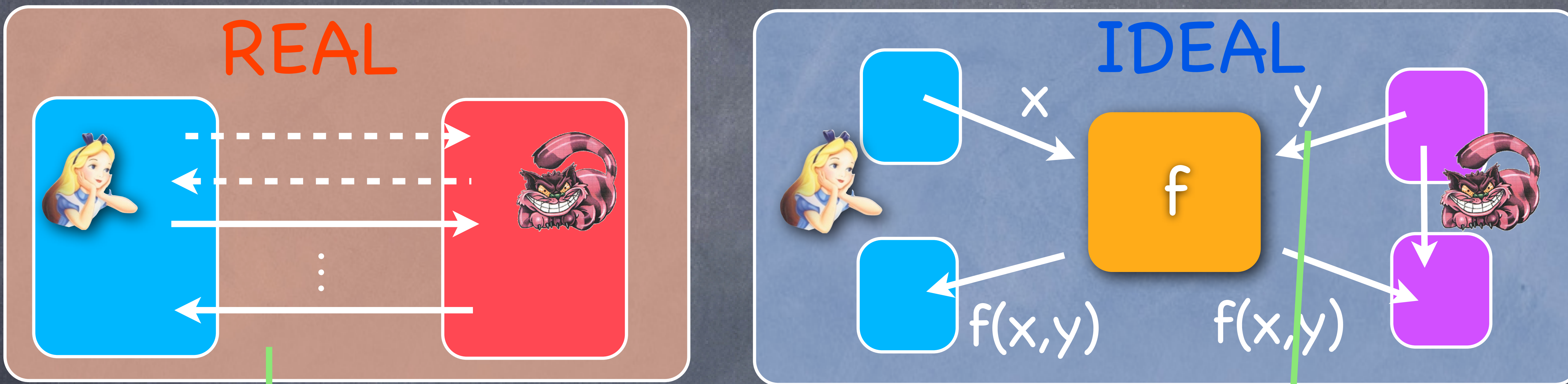


security holds if REAL looks like IDEAL to the outside world

- protocol is secure against dishonest Bob if
  - for every input distribution P(x,y) and $\rho_{XY} = \sum_{x,y} \sqrt{P(x,y)} |x\rangle_A |y\rangle_B$
  - for every dishonest Bob B in the real world,
  - there exists a dishonest Bob B in the ideal world
  - such that $\mathrm{REAL}(\rho_{XY}) = \mathrm{IDEAL}(\rho_{XY})$

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 "honestly" but purify their actions

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

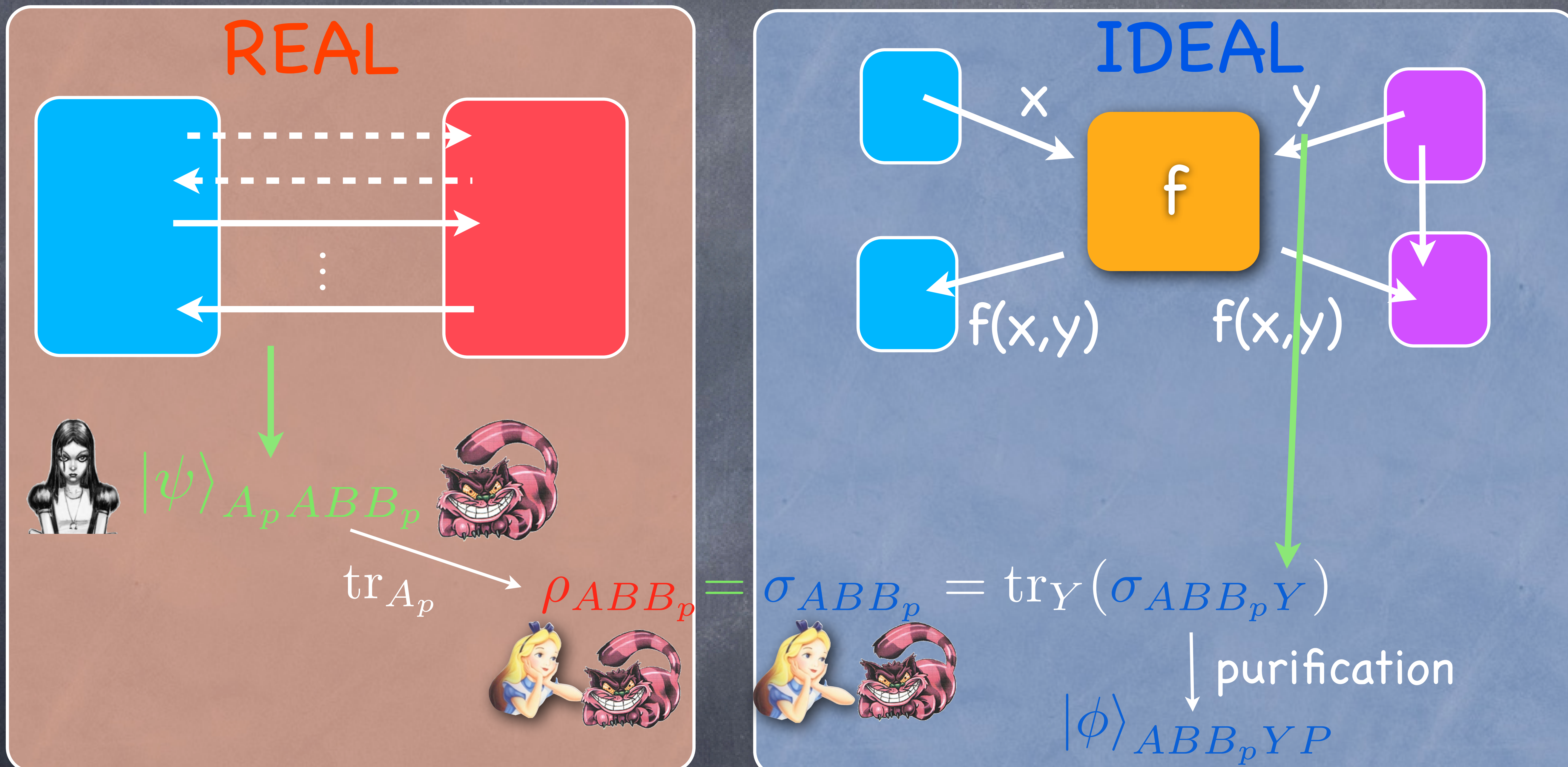
$$\rho_{ABB_p} = \sigma_{ABB_p} = \mathrm{tr}_Y(\sigma_{ABB_pY})$$

$\downarrow$ purification

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

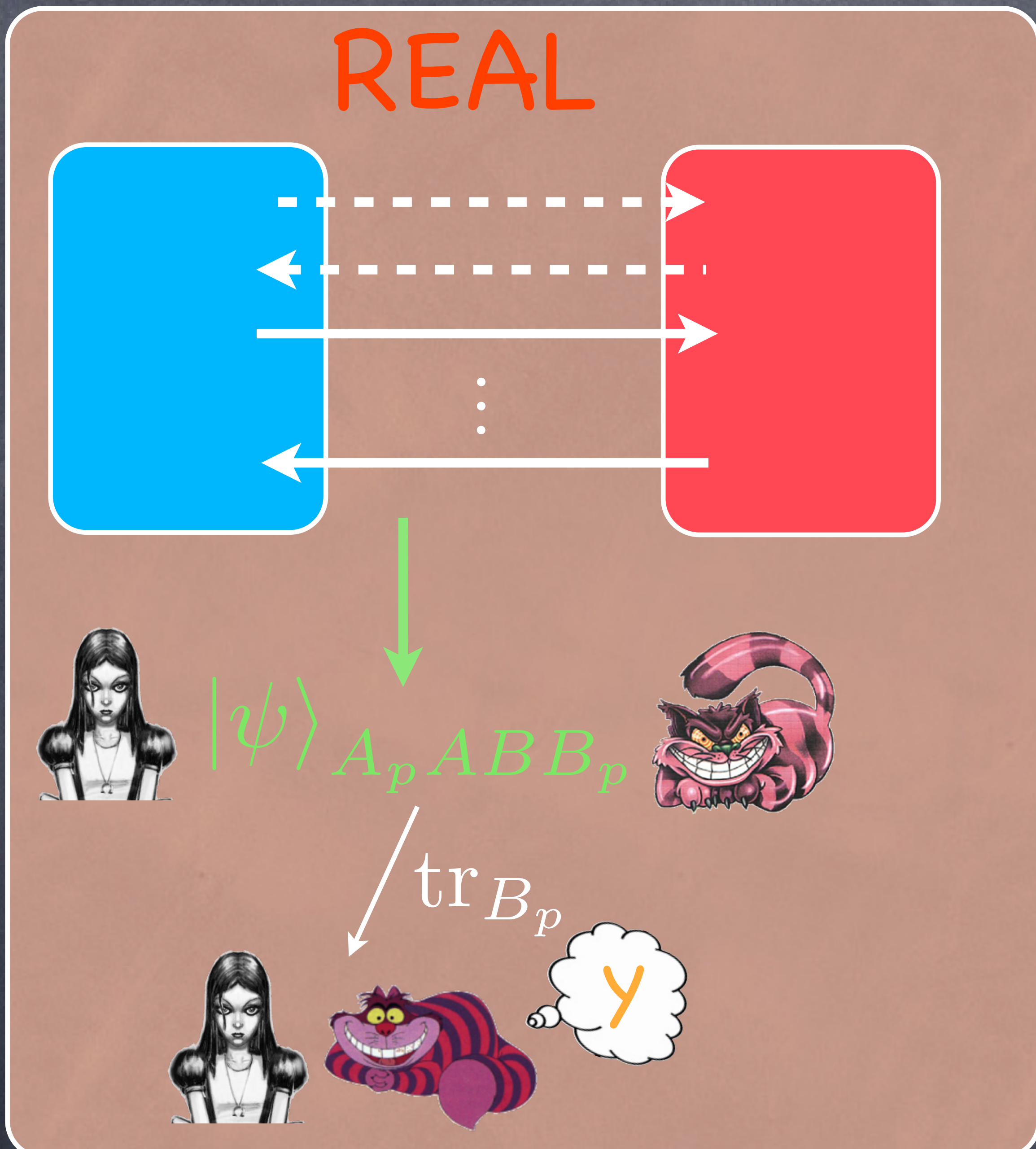
Security against Bob => Insecurity against Alice

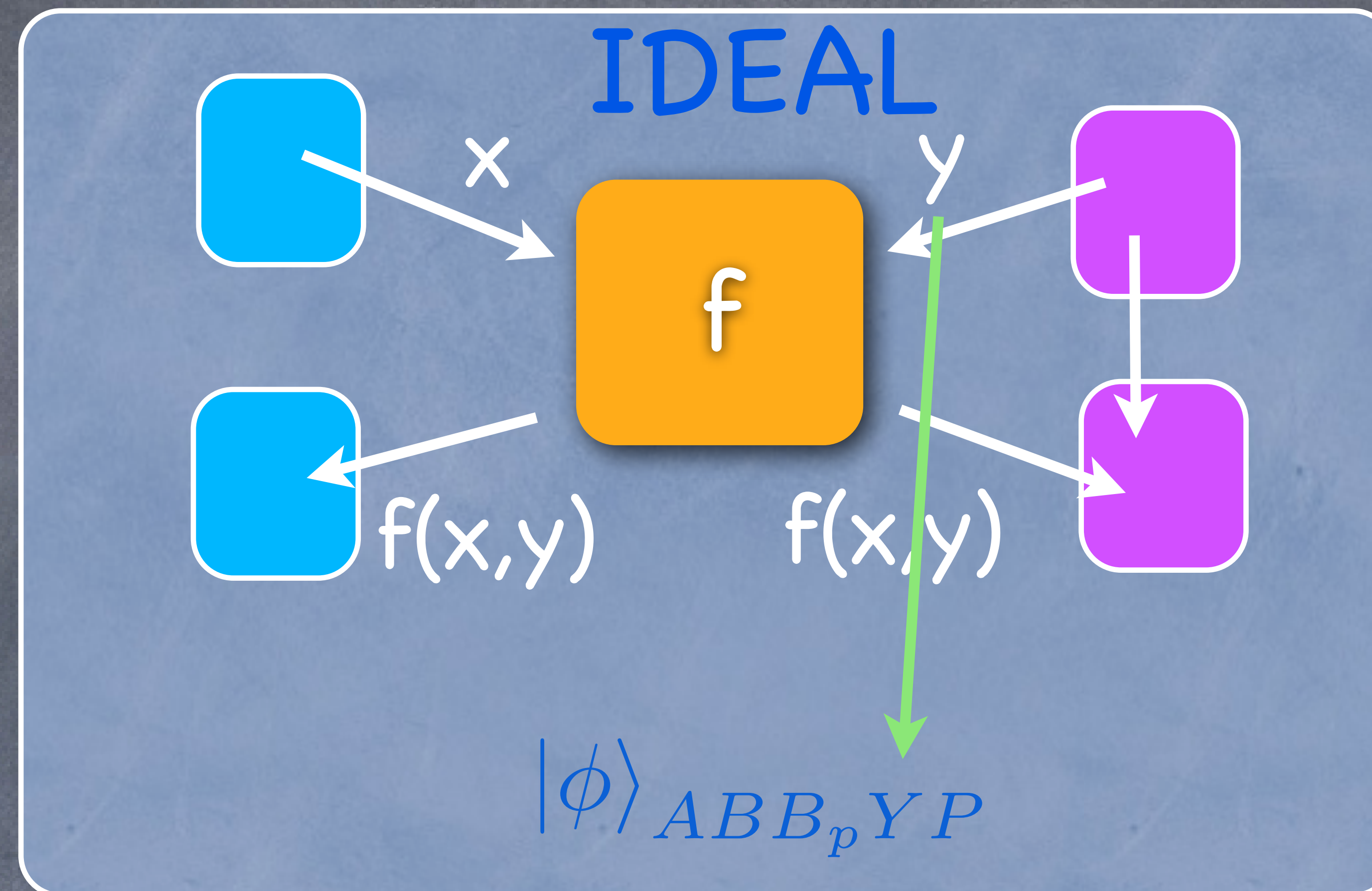
security holds if REAL looks like IDEAL to the outside world



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

Alice's Cheating Strategy





1. plays honest but purified strategy
2. she applies the cheating unitary U
3. measures register Y to obtain y.
4. due to correctness, we can show that for all x: f(x,y) = f(x,y).

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

Error Case

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

$$\|\mathrm{REAL} - \mathrm{IDEAL}\|_{\diamond} \leq \varepsilon$$

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

Conclusion & Open Problems

- completes our understanding of why nature does not allow to do two-party secure computation.
- devil lies in details 
- is such a strong security definition necessary for impossibility proof? can it be done with a weaker definition?
- randomized functions?

Thank you!