

Quantum Cyber Security

Lecture 11: Secure Two-Parties Functionalities

Petros Wallden

University of Edinburgh

26th February 2026



- 1 What is Secure Multiparty Computation
- 2 Basic Primitives and Their Relations
- 3 Information Theoretic Security: Classical Impossibility
- 4 Could Quantum Communications achieve ITS: a naive attempt
- 5 Information Theoretic Security: Quantum Impossibility
- 6 Side-Stepping the No-Go Results

The Millionaire's Problem

The Problem

Two millionaires (Alice and Bob) want to:

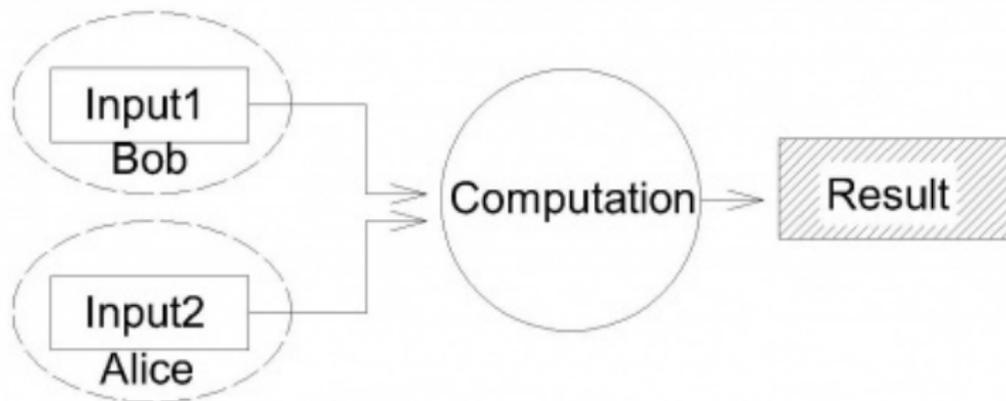
- 1 Determine **who is wealthier** ($a \stackrel{?}{\geq} b$)
- 2 Not reveal anything else about their properties

The Millionaire's Problem

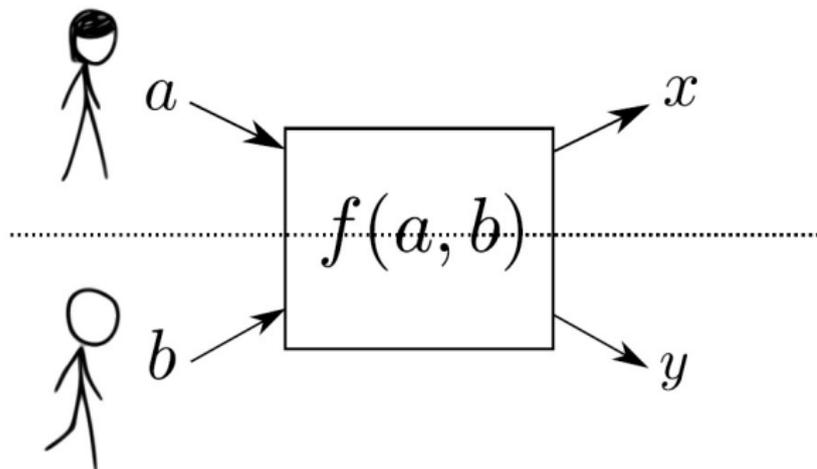
The Problem

Two millionaires (Alice and Bob) want to:

- 1 Determine **who is wealthier** ($a \stackrel{?}{\geq} b$)
- 2 Not reveal anything else about their properties



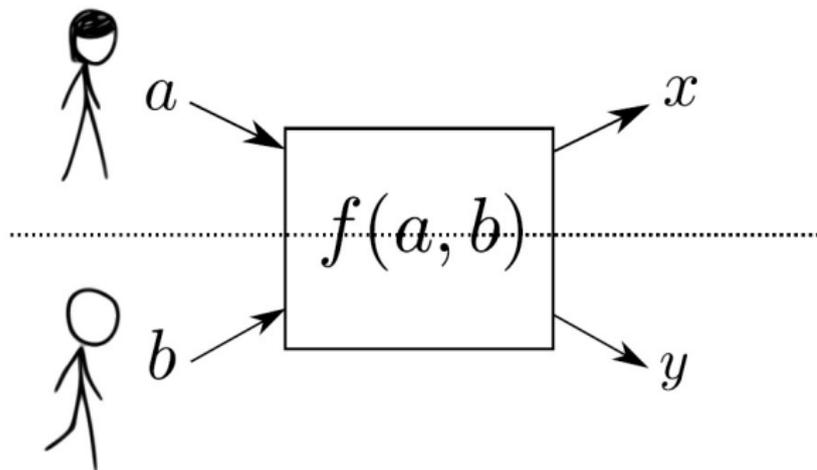
Secure Multiparty Computation



Some figures taken from F. Dupuis

$$f(a, b) = (x, y)$$

Secure Multiparty Computation

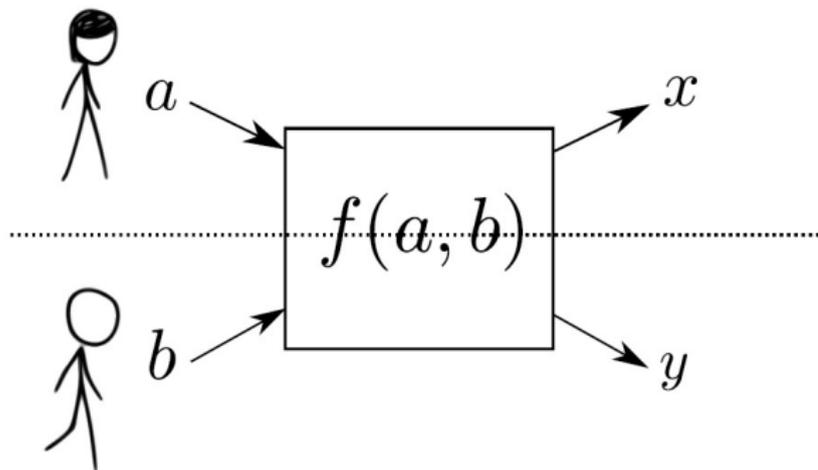


Some figures taken from F. Dupuis

$$f(a, b) = (x, y)$$

Example: Function $f(a, b) = (a \wedge b, a \wedge b)$

Secure Multiparty Computation



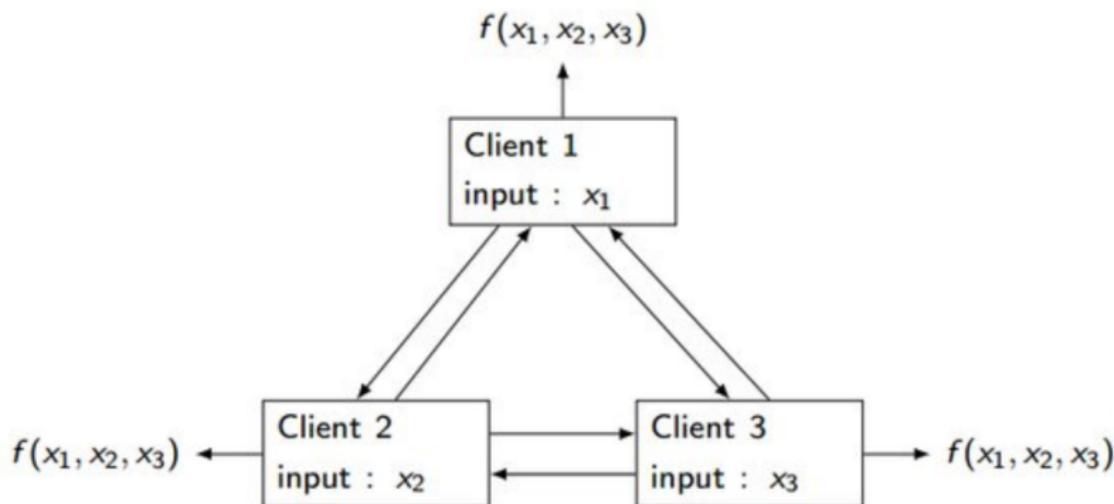
Some figures taken from F. Dupuis

$$f(a, b) = (x, y)$$

Example: Function $f(a, b) = (a \wedge b, a \wedge b)$

- If $a = 0$ Alice learns nothing on Bob's input
- If $a = 1$ Alice learns exactly Bob's input
- Protocol is **secure** because this information Alice would learn even in the ideal case!

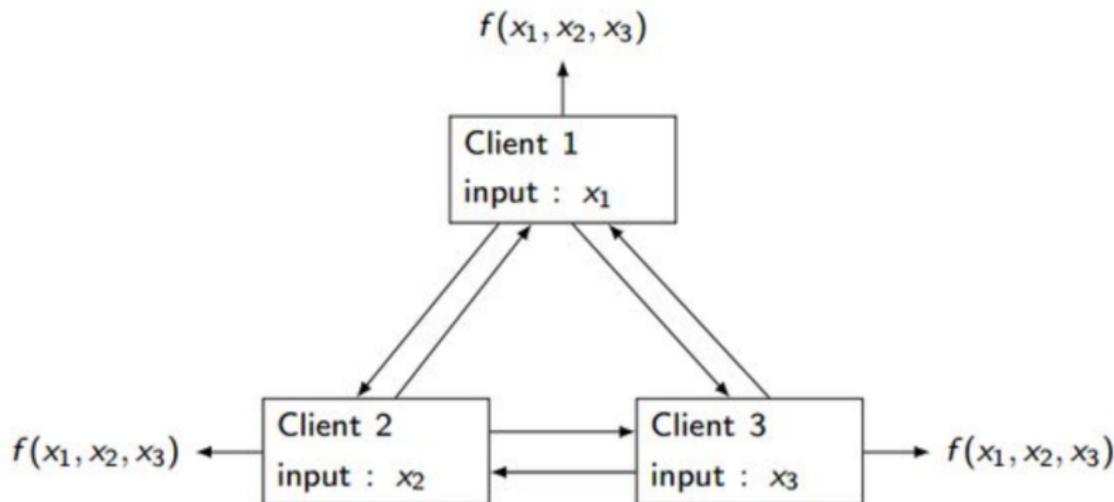
Secure Multiparty Computation



$$f(x_1, x_2, x_3) = (y_1, y_2, y_3)$$

(In many cases the output is the same for all parties)

Secure Multiparty Computation

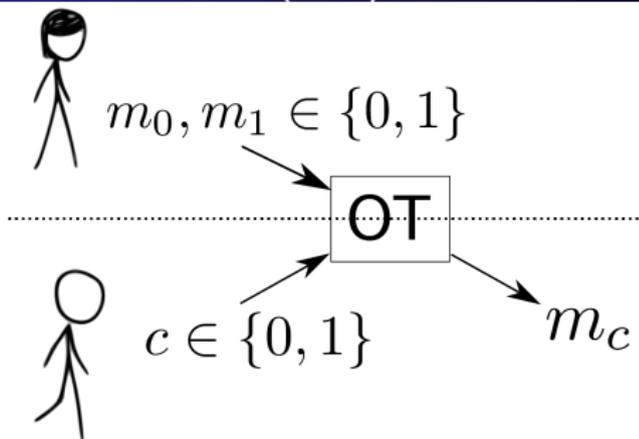


$$f(x_1, x_2, x_3) = (y_1, y_2, y_3)$$

(In many cases the output is the same for all parties)

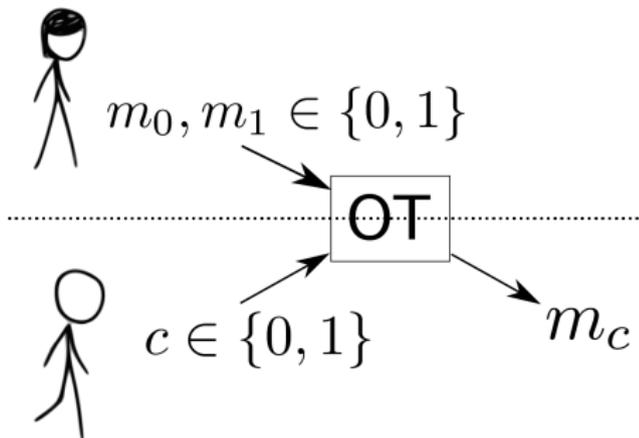
- **Applications:** E-voting, auctions, private information retrieval, privacy-preserving data mining, etc

1 out of 2 Oblivious Transfer (OT)



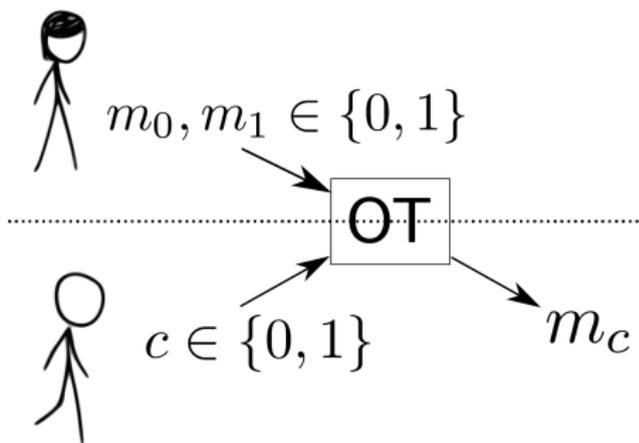
- **Alice:** Inputs two (single-bit) messages m_0, m_1
- **Bob:** Inputs a single bit c

1 out of 2 Oblivious Transfer (OT)



- **Bob:** Receives the message m_c (Output)

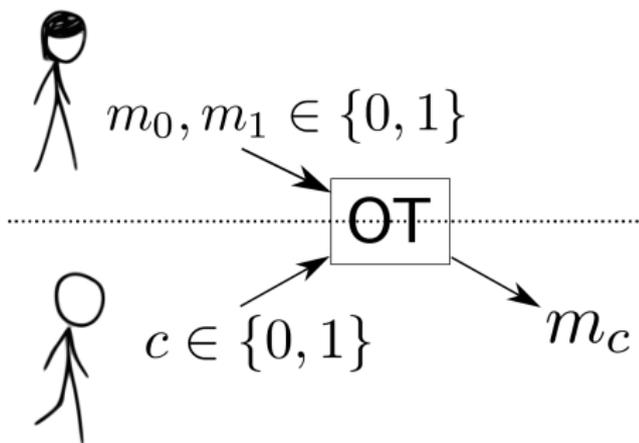
1 out of 2 Oblivious Transfer (OT)



Security

- **Alice:** Does **not** learn c ; ie which message Bob received
- **Bob:** Learns **nothing** about the message $m_{c \oplus 1}$

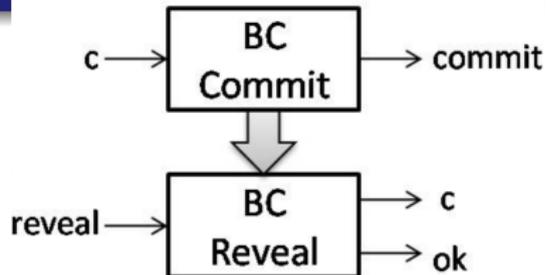
1 out of 2 Oblivious Transfer (OT)



Security

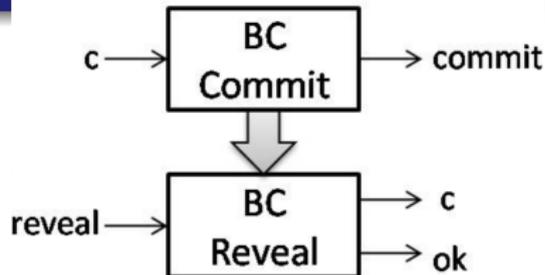
- **Alice:** Does **not** learn c ; i.e. which message Bob received
- **Bob:** Learns **nothing** about the message $m_{c \oplus 1}$

OT is Universal for Secure Multiparty Computation



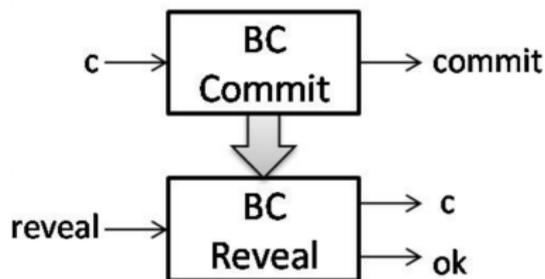
Commit Phase

- Alice: Inputs a single-bit c (commits)
- Bob: receives `commit`



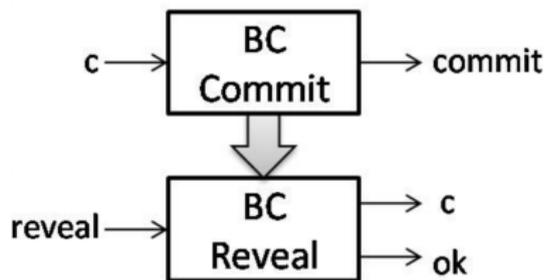
Reveal Phase

- **Alice:** sends the message/request “**reveal**”
- **Bob:** Receives c & confirmation that matches commitment



Security

- **Alice:** Cannot open the commitment to another value than the one she inputs in the commit phase (**Binding**)
- **Bob:** Learns nothing about c before `reveal` (**Concealing**)



Security

- **Alice:** Cannot open the commitment to another value than the one she inputs in the commit phase (**Binding**)
- **Bob:** Learns nothing about c before **reveal** (**Concealing**)

Implication

- BC can be constructed from OT.
- Any impossibility of BC **implies** impossibility of OT

BC Impossibility in ITS setting

It is impossible to achieve Bit-Commitment classically, with information-theoretic security (ITS)

BC Impossibility in ITS setting

It is impossible to achieve Bit-Commitment classically, with information-theoretic security (ITS)

Proof

At the end of commit phase: Bob has classical info that either:

- 1 Any possible **reveal** that does not abort, opens to a unique message **c**

BC Impossibility in ITS setting

It is impossible to achieve Bit-Commitment classically, with information-theoretic security (ITS)

Proof

At the end of commit phase: Bob has classical info that either:

- ① Any possible **reveal** that does not abort, opens to a unique message **c**
- Bob can brute-force trying all **reveal** and find **c**:
Not Concealing

BC Impossibility in ITS setting

It is impossible to achieve Bit-Commitment classically, with information-theoretic security (ITS)

Proof

At the end of commit phase: Bob has classical info that either:

- 1 Any possible **reveal** that does not abort, opens to a unique message c
→ Bob can brute-force trying all **reveal** and find c :
Not Concealing
- 2 There exist at least two ways to open $\text{reveal}_c, \text{reveal}_{c \oplus 1}$ that opens to different message

BC Impossibility in ITS setting

It is impossible to achieve Bit-Commitment classically, with information-theoretic security (ITS)

Proof

At the end of commit phase: Bob has classical info that either:

- 1 Any possible **reveal** that does not abort, opens to a unique message c
 - Bob can brute-force trying all **reveal** and find c :
Not Concealing
- 2 There exist at least two ways to open $\text{reveal}_c, \text{reveal}_{c\oplus 1}$ that opens to different message
 - Alice can brute-force and find both $\text{reveal}_c, \text{reveal}_{c\oplus 1}$, and thus can open commitment to either message: **Not Binding**

A Wrong Protocol for Quantum BC

Commit Phase

- Alice, to commit to 0, selects rand a state from $\{|h\rangle, |v\rangle\}$
- Alice, to commit to 1, selects rand a state from $\{|+\rangle, |-\rangle\}$
- Alice sends Qubit to Bob that stores it

A Wrong Protocol for Quantum BC

Reveal Phase

- Alice announces the **bit** and the **exact state** she send
- Bob measures in that basis and confirms the commitment

A Wrong Protocol for Quantum BC

Security

- Protocol is **Concealing**.
- Bob's state at the end of commit phase:

$$\rho_B = \frac{1}{2} (|h\rangle\langle h| + |v\rangle\langle v|) = \frac{1}{2} (|+\rangle\langle +| + |-\rangle\langle -|) = \frac{1}{2} \mathbb{I}$$

A Wrong Protocol for Quantum BC

Security

- Protocol is **not binding**
- If Alice follows protocol cannot de-commit to different value without being detected with some probability.
- If Alice deviates (commit phase), can postpone commitment until reveal phase. **0 prob being detected** (see later)!

Quantum Bit Commitment is Impossible ITS (Lo-Chau & Mayers)

It is impossible (quantumly) to achieve Bit Commitment that is Information Theoretically both **Binding** and **Concealing**

Proof

Fact (proof later): Let $|\psi\rangle_{AB}, |\chi\rangle_{AB}$ and assume that $\text{Tr}_A(|\psi\rangle\langle\psi|) = \text{Tr}_A(|\chi\rangle\langle\chi|)$. There exists U_A s.t. $(U_A \otimes \mathbb{I})|\psi\rangle_{AB} = |\chi\rangle_{AB}$.

Quantum Bit Commitment is Impossible ITS (Lo-Chau & Mayers)

It is impossible (quantumly) to achieve Bit Commitment that is Information Theoretically both **Binding** and **Concealing**

- Assume the global (Alice-Bob) state after committing to be:
 $0 \rightarrow |\phi_0\rangle_{AB} ; 1 \rightarrow |\phi_1\rangle_{AB}$
- Assume **perfectly concealing**:
 $\rho_B(0) = \text{Tr}_A(|\phi_0\rangle\langle\phi_0|) = \rho_B(1) = \text{Tr}_A(|\phi_1\rangle\langle\phi_1|)$

Quantum Bit Commitment is Impossible ITS (Lo-Chau & Mayers)

It is impossible (quantumly) to achieve Bit Commitment that is Information Theoretically both **Binding** and **Concealing**

- Assume the global (Alice-Bob) state after committing to be:
 $0 \rightarrow |\phi_0\rangle_{AB} ; 1 \rightarrow |\phi_1\rangle_{AB}$
- Assume **perfectly concealing**:
 $\rho_B(0) = \text{Tr}_A(|\phi_0\rangle\langle\phi_0|) = \rho_B(1) = \text{Tr}_A(|\phi_1\rangle\langle\phi_1|)$
- There exist unitary $(U_A \otimes \mathbb{I})|\phi_0\rangle_{AB} = |\phi_1\rangle_{AB}$
- Alice can “commit” to 0, and then if she changes her mind can apply U_A on her qubit to commit to 1.

Not Binding at all!

Quantum Bit Commitment is Impossible ITS (Lo-Chau & Mayers)

It is impossible (quantumly) to achieve Bit Commitment that is Information Theoretically both **Binding** and **Concealing**

Fact (proof later): Let $|\psi\rangle_{AB}, |\chi\rangle_{AB}$ and assume that $\text{Tr}_A(|\psi\rangle\langle\psi|) = \text{Tr}_A(|\chi\rangle\langle\chi|)$. There exists U_A s.t. $(U_A \otimes \mathbb{I})|\psi\rangle_{AB} = |\chi\rangle_{AB}$.

- **Schmidt Decomposition:** $|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |e_i\rangle_A \otimes |f_i\rangle_B$ where $|e_i\rangle_A, |f_i\rangle_B$ eigenvectors of reduced matr. $\text{Tr}_B(|\psi\rangle_{AB}\langle\psi|_{AB})$; $\text{Tr}_A(|\psi\rangle_{AB}\langle\psi|_{AB})$ resp, and λ_i joint eigenvalues.
- Having same reduced (B) states means that the second eigenvectors (and eigenvalues) of ψ, χ are the same
- U_A is simply mapping the one local basis to the other:
 $U_A |e_i^\psi\rangle = |e_i^\chi\rangle$ (always possible)

Quantum Bit Commitment is Impossible ITS (Lo-Chau & Mayers)

It is impossible (quantumly) to achieve Bit Commitment that is Information Theoretically both **Binding** and **Concealing**

Approximate Concealing:

- Let $\rho_B(0) \stackrel{\epsilon}{\approx} \rho_B(1)$ in trace-distance
- Then following same argument can show that the protocol is at most ϵ -binding

Quantum Bit Commitment is Impossible ITS (Lo-Chau & Mayers)

It is impossible (quantumly) to achieve Bit Commitment that is Information Theoretically both **Binding** and **Concealing**

Attack on Naive Protocol:

- Alice sends one side of a Bell pair to Bob:

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$$

- Bob sees the same reduced matrix $\rho_B = \frac{1}{2}\mathbb{I}$
- Alice can **choose her bit later**:
 - Commits to 0 Alice measures in $\{|h\rangle, |v\rangle\}$ basis
 - Commits to 1 Alice measures in $\{|+\rangle, |-\rangle\}$ basis
- Alice essentially chooses to apply H or not, before measuring in computational basis
- Bob cannot distinguish this from the ideal protocol

It is **impossible to side-step** without making some **relaxation in security requested**

Note: Majority attempts **are wrong**. Check if it is clearly stated how one evades the Lo-Chau and Mayers Thm.

Side-Stepping the Impossibility Results

It is **impossible to side-step** without making some **relaxation in security requested**

Note: Majority attempts **are wrong**. Check if it is clearly stated how one evades the Lo-Chau and Mayers Thm.

- **Bounded Storage Model:** Assume adversary cannot store quantum information for long time (or for more than a fixed number of qubits).
- The Lo-Chau-Mayers attack (de-committing) would require to store a large system until the **reveal** phase (which can be later than the bounds of storage).

It is **impossible to side-step** without making some **relaxation in security requested**

Note: Majority attempts **are wrong**. Check if it is clearly stated how one evades the Lo-Chau and Mayers Thm.

- **Relativistic:** Protocol is performed by teams located in different spacetime locations. Parties cannot communicate faster-than-the-speed-of-light.
- Commitment has **to be opened within a fixed time period** (expires/stops being binding after that)
- The Lo-Chau-Mayers attack (de-committing) would involve applying a unitary on the joint system that during the protocol is **not located in a single spacetime location** (lab).