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)

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 :)


Motivation

ideally
Motivation

ideally
Motivation

ideally

\[ x \rightarrow f \rightarrow y \]
Motivation

ideally

\[ f(x, y) \quad \xrightarrow{x} \quad f \quad \xrightarrow{y} \quad f(x, y) \]
Motivation

ideally

e.g.: Yao’s millionaires’ problem: $\leq$
Motivation

ideally

\[ f(x, y) \]

\[
\begin{align*}
    &f(x, y) \\
    \quad \text{x} \quad \rightarrow \\
    \quad f(x, y) \quad \leftarrow \\
    \quad y \quad \rightarrow \\
    \quad f(x, y)
\end{align*}
\]

e.g.: Yao’s millionaires’ problem: \( \leq \)

reality
Motivation

ideally

f(x, y) \xrightarrow{\times} f

f(x, y) \xleftarrow{y} f(x, y)

e.g.: Yao’s millionaires’ problem: ≤

reality
Motivation

- ideally

\[ f(x, y) \]

\[ \leq \]

e.g.: Yao’s millionaires’ problem: \[ \leq \]

- reality
Motivation

ideally

\[ f(x, y) \]

\[ f(x, y) \]

\[ f(x, y) \]

\[ f(x, y) \]

\[ f(x, y) \]

\[ f(x, y) \]

e.g.: Yao's millionaires' problem: ≤

quantum communication
Motivation

ideally

\[ f(x, y) \]

\[ f(x, y) \]

\[ \vdots \]

\[ f(x, y) \]

\[ f(x, y) \]

e.g.: Yao's millionaires' problem: \( \leq \)

reality

quantum communication

\[ \cdots \]

\[ \vdots \]

\[ \cdots \]
Motivation

ideally

\[ f(x, y) \leftarrow f \rightarrow f(x, y) \]

\[ x \rightarrow f \leftarrow y \]

\[ x = ? \]

\[ f(x, y) \leq \]

\[ \text{e.g.: Yao's millionaires' problem: } \leq \]

reality

quantum communication

x

f(x, y)

y

x = ?

f(x, y)
Secure Function Evaluation

ideally

\[ f(x, y) \]

\[ f(x, y) \]

Alice

Cheshire Cat
Secure Function Evaluation

ideally

\[ f(x, y) \leftarrow f(x, y) \]

goal: come up with protocols that are
Secure Function Evaluation

- ideally

\[ f(x, y) \]

- goal: come up with protocols that are correct
Secure Function Evaluation

Ideally

\[ f(x, y) \]

Goal: come up with protocols that are

- correct
- secure against dishonest Alice
Secure Function Evaluation

- ideally

\[ f(x, y) \]

- 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.
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.

$\text{dishonest Bob learns no more about } x \text{ than } f(x,y).$
**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.

\[ f(x,y) \]
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.

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

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 $\varepsilon$-correct and $\varepsilon$-secure against Bob, then Alice can break the protocol with probability $1 - O(\varepsilon)$. 
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

- 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

\textbf{Theorem}: If a quantum protocol for the \textit{one-sided} evaluation of \( f \) is \textit{correct} and \textit{perfectly secure} against Bob, then Alice can \textit{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.
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

dishonest Bob learns nothing about $x$
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
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.
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 $x$. 
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.
**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 $x$.

Lo's Result: proof fails for two-sided computations

Error increases with number of inputs
Lo's Proof
Lo's Proof
Lo's Proof

\[ f(x, y) \]

only Alice gets output
Lo's Proof

\[ f(x, y) \]

\[ |\psi^{x,y}_{AB}\rangle \]

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

\[ f(x,y) \quad \arrow{\vdots}\quad |\psi^{x,y}_{AB}\rangle \quad \downarrow \]

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

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

\[ f(x,y) \quad |\psi^{x,y}_{AB}\rangle \quad \downarrow \]

\[
|\psi^{x_0}_{AB}\rangle = \sum_y |\psi^{x_0,y}_{AB_1}\rangle |y\rangle_{B_2}
\]
Lo's Proof

only Alice gets output

wlog measurements are moved to the end, final state is pure

dishonest Bob inputs superposition

\[
|\psi^{x_0, y}\rangle_{AB} = \sum_{y} |\psi^{x_0, y}\rangle_{AB_1} |y\rangle_{B_2}
\]

security against dishonest Bob:

\[
\text{tr}_A (|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho^{x_0}_B = \rho^{x_1}_B = \text{tr}_A (|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})
\]
Lo’s Proof

security against dishonest Bob:

$$\text{tr}_A (\ketbra{x_0}{x_0}_{AB}) = \rho_{x_0}^B = \rho_{x_1}^B = \text{tr}_A (\ketbra{x_1}{x_1}_{AB})$$
Lo's Proof

security against dishonest Bob:
\[
\text{tr}_A (|\psi^{x_0}_\alpha \rangle \langle \psi^{x_0}_\alpha|_A)_B = \rho^{x_0}_B = \rho^{x_1}_B = \text{tr}_A (|\psi^{x_1}_\alpha \rangle \langle \psi^{x_1}_\alpha|_A)_B
\]

implies existence of cheating unitary for Alice: (not dep on y)
\[
(U_A \otimes \mathbb{I}_B) |\psi^{x_0}_\alpha \rangle_A = |\psi^{x_1}_\alpha \rangle_A
\]
Lo's Proof

security against dishonest Bob:

\[ \text{tr}_A (\ket{\psi^x_0} \bra{\psi^x_0}_{AB}) = \rho^x_B = \rho^{x_1}_B = \text{tr}_B (\ket{\psi^{x_1}_0} \bra{\psi^{x_1}_0}_{AB}) \]

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

\[ (U_A \otimes I_B) \ket{\psi^x_0}_{AB} = \ket{\psi^x_1}_{AB} \]
Lo's Proof

security against dishonest Bob:

security against dishonest Bob:

implies existence of cheating unitary for Alice: (not dep on $y$)
Lo's Proof

security against dishonest Bob:
\[ \operatorname{tr}_A (|\psi^{x_0}\rangle\langle\psi^{x_0}|_A)_B = \rho_B^{x_0} = \rho_B^{x_1} = \operatorname{tr}_A (|\psi^{x_0}\rangle\langle\psi^{x_1}|_A)_B \]

implies existence of cheating unitary for Alice: (not dep on y)
\[
(U_A \otimes I_B) |\psi^{x_0}\rangle_A \otimes |y\rangle_B = |\psi^{x_1}\rangle_A \otimes |y\rangle_B \\
(U_A \otimes I_B) |\psi^{x_0},y\rangle_A \otimes |y\rangle_B = |\psi^{x_1},y\rangle_A \otimes |y\rangle_B
\]
Lo's Proof

security against dishonest Bob:
\[
\text{tr}_A (|\psi^{x_0} \rangle \langle \psi^{x_0}|_AB) = \rho_B^{x_0} = e^{x_1} = \text{tr}_B (|\psi^{x_1} \rangle \langle \psi^{x_1}|_AB)
\]

implies existence of cheating unitary for Alice: (not dep on y)
\[
(U_A \otimes I_B) |\psi^{x_0} \rangle_{AB} = |\psi^{x_1} \rangle_{AB}
\]
\[
(U_A \otimes I_B) |\psi^{x_0}, y \rangle_{AB} = |\psi^{x_1}, y \rangle_{AB}
\]

dishonest Alice: input \(x_0 \rightarrow f(x_0, y)\), switches to \(x_1 \rightarrow f(x_1, y)\) ...
Lo's Proof

\[ f(x_0, y), f(x_1, y), \ldots \quad |\psi^{x, y}\rangle_{AB} \]

security against dishonest Bob:

\[ \text{tr}_A (|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho_B^{x_0} = e^{x_1} = \text{tr}_B (|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB}) \]

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

\[ (U_A \otimes I_B) |\psi^{x_0}\rangle_{AB} = |\psi^{x_1}\rangle_{AB} \]
\[ (U_A \otimes I_B) |\psi^{x_0, y}\rangle_{AB} = |\psi^{x_1, y}\rangle_{AB} \]

dishonest Alice: input \( x_0 \rightarrow f(x_0, y) \), switches to \( x_1 \rightarrow f(x_1, y) \) \ldots
Lo's Proof

\[ f(x_0, y), f(x_1, y), \ldots \quad \left| \psi^{x, y} \right\rangle_{AB} \]

security against dishonest Bob:

\[ \text{tr}_A \left( \left| \psi^{x_0} \right\rangle_{AB} \langle \psi^{x_0} \right|_{AB} \right) = \rho^x_B = \rho^y = \text{tr}_B \left( \left| \psi^{x_1} \right\rangle_{AB} \langle \psi^{x_1} \right|_{AB} \right) \]

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

\((U_A \otimes I_B) \left| \psi^{x_0} \right\rangle_{AB} = \left| \psi^{x_1} \right\rangle_{AB}\)

\((U_A \otimes I_B) \left| \psi^{x_0, y} \right\rangle_{AB} = \left| \psi^{x_1, y} \right\rangle_{AB}\)

dishonest Alice: input \(x_0 \to f(x_0, y)\), switches to \(x_1 \to f(x_1, y)\) ...
Lo's Proof

security against dishonest Bob without output:

\[
\text{tr}_A (|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho^0 = \rho_1 = \text{tr}_A (|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB})
\]
Lo's Proof

security against dishonest Bob without output:

\[ \text{tr}_A (|\psi^x_0\rangle\langle\psi^x_0|_AB) = \rho^x_B = \rho^x_B = \text{tr}_A (|\psi^x_1\rangle\langle\psi^x_1|_AB) \]

\(\cdots\)

\(\psi^{x,y}_A B\)

f(x,y)

\(\times\)

\(\times = ?\)

\(\dag \)

\(\text{crucial step!}\)
Lo's Proof

security against dishonest Bob without output:

\[ \text{tr}_A (|\psi^{x, y}_0\rangle\langle \psi^{x, y}_0|_{AB}) = \rho^{x, y}_B = \rho^{x, y}_B = \text{tr}_A (|\psi^{x, y}_1\rangle\langle \psi^{x, y}_1|_{AB}) \]

what if Bob has \( f(x, y) \)? In general \( \rho^{x, y}_B \neq \rho^{x, y}_B \)
Lo's Proof

security against dishonest Bob without output:

\[ \text{tr}_A (|\psi^{x_0}\rangle\langle\psi^{x_0}|_{AB}) = \rho^{x_0}_B = \rho^{x_1}_B = \text{tr}_A (|\psi^{x_1}\rangle\langle\psi^{x_1}|_{AB}) \]

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

precise formalisation of “not learning more about \( x \) than \( f(x,y) \)”?
Lo's Proof

security against dishonest Bob without output:
\[ \text{tr}_A (|\psi^{x_0}x_0\rangle\langle\psi^{x_0}|_{AB}) = \rho^{x_0}_B = \rho^{x_1}_B = \text{tr}_A (|\psi^{x_1}x_1\rangle\langle\psi^{x_1}|_{AB}) \]

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

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

\[ f(x, y) \]
Informal Security Definition

we want

we have
Informal Security Definition

we want

we have

IDEAL
Informal Security Definition

we want

\[ \times \quad f(x,y) \quad \leftarrow \quad f \quad \rightarrow \quad y \quad \rightarrow \quad f(x,y) \]  

IDEAL

we have

\[ \rightarrow \quad \cdots \quad \rightarrow \quad f(x,y) \quad \rightarrow \quad \cdots \quad \rightarrow \quad f(x,y) \]  

REAL
Informal Security Definition

we want

\[ f(x, y) \]

security holds if REAL looks like IDEAL to the outside world

we have

\[ f(x, y) \]
Formal Security Definition

security holds if \textcolor{red}{REAL} looks like \textcolor{blue}{IDEAL} to the outside world
security holds if \textbf{REAL} looks like \textbf{IDEAL} to the outside world
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
security holds if **REAL** looks like **IDEAL** to the outside world
Formal Security Definition

security holds if \textit{REAL} looks like \textit{IDEAL} to the outside world

protocol is secure against 	extit{dishonest} \textit{Bob} if
Formal Security Definition

security holds if \textit{REAL} looks like \textit{IDEAL} to the outside world

\[ \rho_{XY} = \sum_{x,y} P(x, y) |x\rangle\langle x|_A |y\rangle\langle y|_B \]

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 \( \text{REAL} \) looks like \( \text{IDEAL} \) to the outside world

protocol is secure against dishonest Bob if

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

Formal Security Definition:

$$\rho_{XY} = \sum_{x,y} P(x,y) |x\rangle \langle x|_A |y\rangle \langle y|_B$$
Formal Security Definition

protocol is secure against dishonest Bob if
for every input distribution $P(x,y)$, i.e.
for every dishonest Bob $B$ in the real world,
there exists a dishonest Bob $B$ in the ideal world
such that $\text{REAL}(\rho_{XY}) = \text{IDEAL}(\rho_{XY})$
Formal Security Definition

security holds if $\text{REAL}$ looks like $\text{IDEAL}$ 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 $\text{REAL}(\rho_{XY}) = \text{IDEAL}(\rho_{XY})$

also relative to purification
Proof of Insecurity

Security against Bob $\Rightarrow$ Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world
Proof of Insecurity

Security against Bob $\Rightarrow$ 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 $\Rightarrow$ Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world

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

Security against Bob \implies Insecurity against Alice

security holds if \text{REAL} looks like \text{IDEAL} to the outside world

\text{REAL}

\text{IDEAL}

\rho_{ABB_p} = \sigma_{ABB_p} = \text{tr}_Y(\sigma_{ABB_p} Y)

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

\[ |\psi\rangle_{A_p} ABB_p \]
\[ \text{tr}_{A_p} \]
\[ \rho_{ABB_p} = \sigma_{ABB_p} = \text{tr}_Y (\sigma_{ABB_p} Y) \]

state after the real protocol if both parties play "dishonestly" by purifying their actions.
Proof of Insecurity

Security against Bob $\implies$ Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world

\[ \rho_{ABB_p} = \sigma_{ABB_p} = \text{tr}_Y(\sigma_{ABB_p}Y) \]

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

\[ \langle \psi \rangle_{B_p}ABB_p \]

\[ \text{tr}_{A_p} \]
Proof of Insecurity

Security against Bob $\implies$ Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world

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

$|\psi\rangle_{A_p} ABB_p$  
$\text{tr}_{A_p}$  

$\rho_{ABBP_p} = \sigma_{ABBP_p} = \text{tr}_Y (\sigma_{ABBP_p} Y)$
Proof of Insecurity

Security against Bob $\Rightarrow$ Insecurity against Alice

security holds if REAL looks like IDEAL to the outside world

\[ f(x, y) \]

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

\[
\rho_{ABB_p} = \sigma_{ABB_p} = \text{tr}_Y(\sigma_{ABB_p} Y) \\
|\phi\rangle_{ABB_p Y P}
\]

purification
Proof of Insecurity

security holds if REAL looks like IDEAL to the outside world

REAL

\[
\begin{align*}
|\psi\rangle_{A_p ABB_p} & \xrightarrow{\text{tr}_{A_p}} \rho_{ABB_p} \\
\end{align*}
\]

\[
\sigma_{ABB_p} = \text{tr}_Y (\sigma_{ABB_p} Y)
\]

purification

\[
|\phi\rangle_{ABB_p Y P}
\]
Proof of Insecurity

security holds if \textbf{REAL} looks like \textbf{IDEAL} to the outside world

- by Uhlmann’s theorem: there exists a **cheating unitary** \( U \) such that
  \[
  U_{A_p \rightarrow Y P} |\psi\rangle_{A_p ABB_p} = |\phi\rangle_{ABB_p Y P}
  \]
Proof of Insecurity

REAL

\[ |\psi\rangle_{A_p ABB_p} \]

IDEAL

\[ f(x,y) \]

\[ |\phi\rangle_{ABB_p Y P} \]
Proof of Insecurity

\[ U_{A_p \rightarrow YP} |\psi\rangle_{A_p ABB_p} = |\phi\rangle_{YP ABB_p} \]

IDEAL

\[ f(x,y) \]

\[ \psi \]

REAL

\[ \phi \]

ABB

YP
Proof of Insecurity

\[ |\psi\rangle_{A_p ABB_p} \]

\[ U_{A_p \rightarrow YP} |\psi\rangle_{A_p ABB_p} = |\phi\rangle_{YP ABB_p} \]

measure Y

\[ y' \]
Proof of Insecurity

\[ U_{A_p \rightarrow YP} |\psi\rangle_{A_p ABB_p} = |\phi\rangle_{YP ABB_p} \]

\[ \text{measure } Y \]

\[ y', \quad \text{tr}_{B_p} Y \]
Proof of Insecurity

**REAL**

\[ |\psi\rangle_{A_p ABB_p} \]

\[ U_{A_p \rightarrow YP} |\psi\rangle_{A_p ABB_p} = |\phi\rangle_{YP ABB_p} \]

Measure $Y$

$y'$

**IDEAL**

\[ f(x, y) \]

\[ f(x, y) \]

\[ |\phi\rangle_{ABB_p YP} \]
Proof of Insecurity

1. Alice plays "dishonestly" by purifying, Bob plays honestly
1. Alice plays "dishonestly" by purifying, Bob plays honestly
2. Alice applies cheating unitary $U$
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
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 $x$: $f(x, y') = f(x, y)$.
Error Case
Error Case

our results also hold for \( \varepsilon \)-correctness and \( \varepsilon \)-security
our results also hold for $\varepsilon$-correctness and $\varepsilon$-security

Alice gets a value $y'$ with distribution $Q(y'|y)$ such that for all $x$: $\Pr_{y'}[ f(x,y)=f(x,y') ] \geq 1-O(\varepsilon)$
our results also hold for $\varepsilon$-correctness and $\varepsilon$-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 $\varepsilon$-correctness and $\varepsilon$-security
- Alice gets a value $y'$ with distribution $Q(y'|y)$ such that for all $x$: $\Pr_y[f(x,y) = f(x,y')] \geq 1 - O(\varepsilon)$
- in contrast to Lo's proof where the overall error increases linearly with the number of inputs.
Error Case

- our results also hold for \(\varepsilon\)-correctness and \(\varepsilon\)-security

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

- 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

  motivated from strong no bit commitment result

  [D'Ariano Kretschmann Schlingemann Werner, 2007]
Conclusion & Open Problems

\[ x \quad \leftrightarrow \quad f(x, y) \quad \leftrightarrow \quad y \quad \leftrightarrow \quad f(x, y) \]
secure two-party computation not possible
secure two-party computation not possible
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!