Composable security in relativistic quantum cryptography

V. Vilasini[1] Christopher Portmann[2] Lídia del Rio[3]

[1]Department of Mathematics, University of York, Heslington, York, YO10 5DD, UK

[2]Department of Computer Science, ETH Zürich, 8092 Zürich, Switzerland

[3]Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland

CEQIP, 14th June 2018

Based on: arXiv:1708.00433

MOTIVATION

What is this talk about? (in 3 haikus)

What is this talk about? (in 3 haikus)

Start with resources,
Build a new one that's secure
If parts are secure.

} **Cryptography, Composable security**

Protocols remain secure even when used as a subroutine in others

What is this talk about? (in 3 haikus)

Start with resources,
Build a new one that's secure
If parts are secure.

} **Cryptography, Composable security**

Protocols remain secure even when used as a subroutine in others

Agents in space-time
Exchanging quantum systems,
Building resources.

} **Relativistic protocols**

Security from relativistic causality. E.g., Kent's 2012 bit commitment protocol

What is this talk about? (in 3 haikus)

Start with resources,
Build a new one that's secure
If parts are secure.

} **Cryptography, Composable security**

Protocols remain secure even when used as a subroutine in others

Agents in space-time
Exchanging quantum systems,
Building resources.

} **Relativistic protocols**

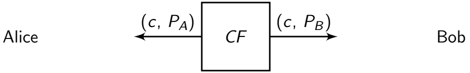
Security from relativistic causality. E.g., Kent's 2012 bit commitment protocol

No model for this.
We propose one here and prove
What can, can't be done.

} **What we do**

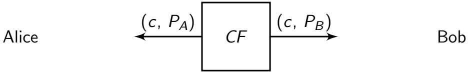
Framework + new possibility, impossibility results

A simple relativistic coin flipping protocol



An unbiased coin flipping resource: c is an independent, uniformly random classical bit.

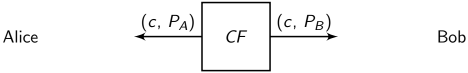
A simple relativistic coin flipping protocol



An unbiased coin flipping resource: c is an independent, uniformly random classical bit.

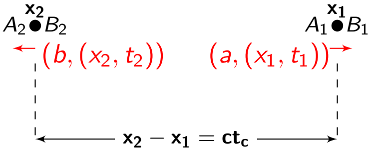
Relativistic case: Alice and Bob consist of 2 agents each.

A simple relativistic coin flipping protocol



An unbiased coin flipping resource: c is an independent, uniformly random classical bit.

Relativistic case: Alice and Bob consist of 2 agents each.



Output: $c = a \oplus b$ (in joint causal future) if $|t_1 - t_2| < \frac{t_c}{2}$

Composability issues

Composability issues

(WO)MAN IN THE MIDDLE ATTACK

Anoushka

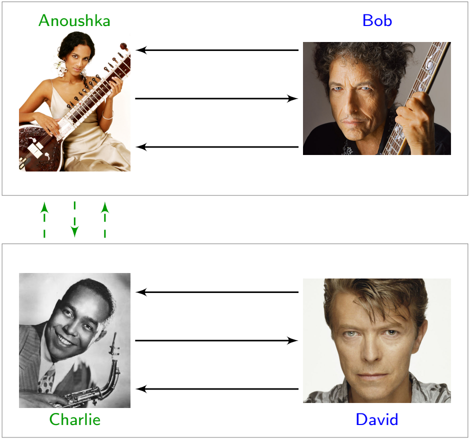
Bob

Charlie

David

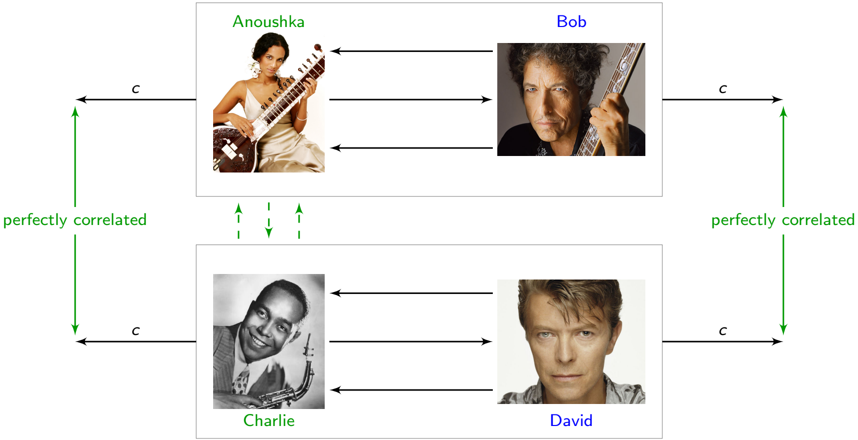
Composability issues

(WO)MAN IN THE MIDDLE ATTACK



Composability issues

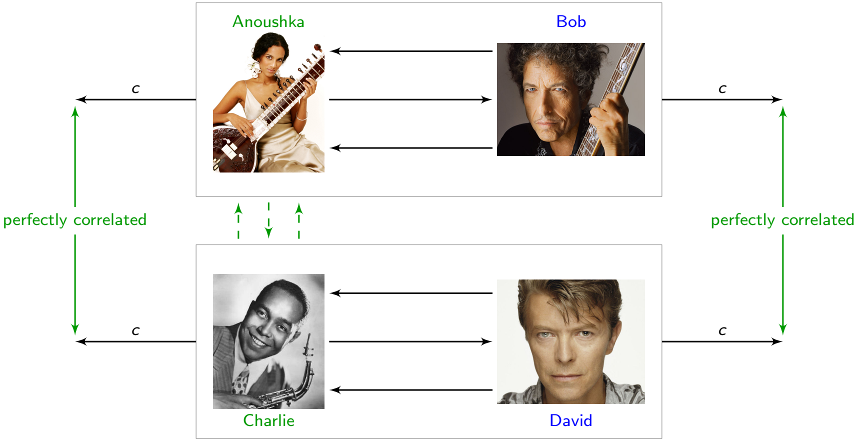
(WO)MAN IN THE MIDDLE ATTACK



- MITM $\Rightarrow$ pairs of parties cannot settle disputes independently i.e. $\mathcal{CF}$ not secure.

Composability issues

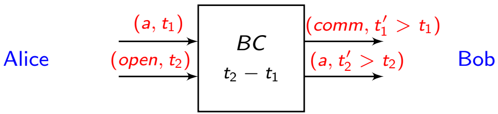
(WO)MAN IN THE MIDDLE ATTACK



- MITM ⇒ pairs of parties cannot settle disputes independently i.e. $\mathcal{CF}$ not secure.
- Such an attack can be avoided if parties pre-share a bit commitment resource $\mathcal{BC}$.

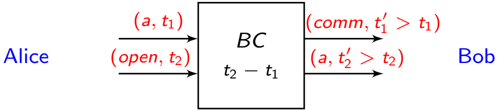
So what is bit commitment?

So what is bit commitment?



A Bit Commitment resource ($a \in \{0, 1\}$).

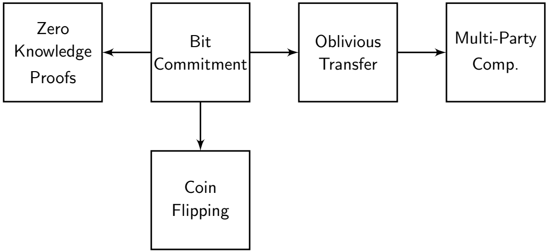
So what is bit commitment?



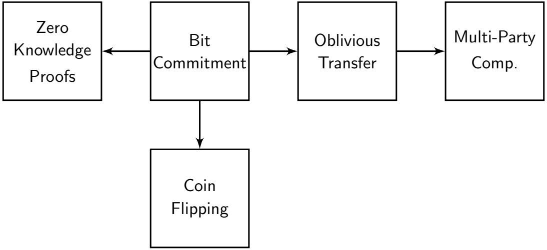
A Bit Commitment resource ($a \in \{0,1\}$).

- Arbitrarily long commitments.
- Committer can choose when to open or not to open at all.
- Relativistic protocols only allow for timed commitments of fixed duration. E.g., this makes protocols like Kent 2012 more like a "channel with delay".

State-of-the-art: BC solely through exchange of messages

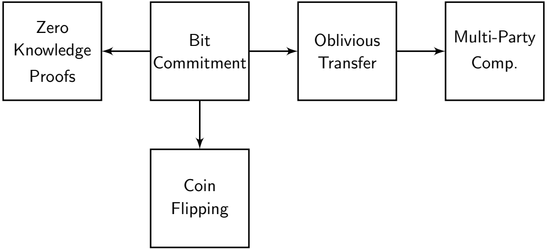


State-of-the-art: BC solely through exchange of messages



- **Non-relativistic protocols:** Impossible!
  - **Stand-alone security:**No! quantum attack (MLC): Mayers, Lo, Chau 1996-1997.
  - **Composable security:**No! classical man in the middle attack (MITM): Canetti et. al 2001.

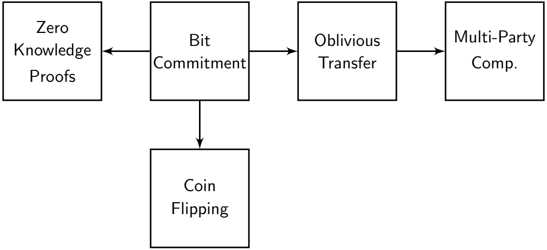
State-of-the-art: BC solely through exchange of messages



- **Non-relativistic protocols:** Impossible!
  - **Stand-alone security:** No! quantum attack (MLC): Mayers, Lo, Chau 1996-1997.
  - **Composable security:** No! classical man in the middle attack (MITM): Canetti et. al 2001.

- **Relativistic protocols:** Possible?
  - **Stand-alone security:** Yes! Kent 2012 secure against MLC attack: Kaniewski et. al 2013.
  - **Composable security:** No? Argument against non-composability of Kent 2012: Kaniewski et. al. 2013.

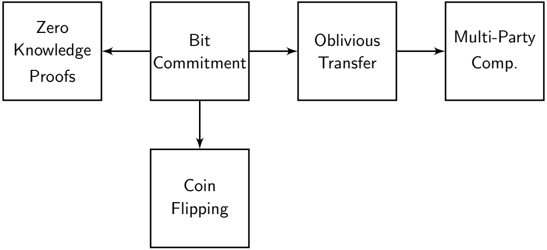
State-of-the-art: BC solely through exchange of messages



- **Non-relativistic protocols:** Impossible!
  - **Stand-alone security:**No! quantum attack (MLC): Mayers, Lo, Chau 1996-1997.
  - **Composable security:**No! classical man in the middle attack (MITM): Canetti et. al 2001.
- **Relativistic protocols:** Possible?
  - **Stand-alone security:**Yes! Kent 2012 secure against MLC attack: Kaniewski et. al 2013.
  - **Composable security:**No? Argument against non-composability of Kent 2012: Kaniewski et. al. 2013.

No general framework for modelling composable security of relativistic protocols against classical, quantum, non-signalling adversaries.

State-of-the-art: BC solely through exchange of messages



- **Non-relativistic protocols:** Impossible!
  - **Stand-alone security:**No! quantum attack (MLC): Mayers, Lo, Chau 1996-1997.
  - **Composable security:**No! classical man in the middle attack (MITM): Canetti et. al 2001.

- **Relativistic protocols:** Possible?
  - **Stand-alone security:**Yes! Kent 2012 secure against MLC attack: Kaniewski et. al 2013.
  - **Composable security:**No? Argument against non-composability of Kent 2012: Kaniewski et. al. 2013.

No general framework for modelling composable security of relativistic protocols against classical, quantum, non-signalling adversaries.

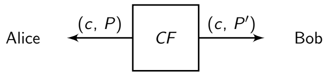
Our Work: Framework+new possibility/impossibility results.

THE FRAMEWORK

Resources (Abstract Cryptography[1])

- A resource is a system with interfaces, one for each player Alice and Bob providing them with certain controls.
- The resources available to the players are given by a tuple $\mathcal{R} = \{R, R_A, R_B\}$, defined by three resources: R when both parties are honest and R_i when party $i \in \{A, B\}$ is dishonest.

Example: coin flipping



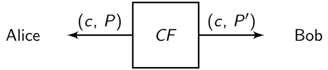
(a) **An unbiased resource:** CF, CF_A, CF_B same.

[1] U. Maurer, R. Renner. The Second Symposium on Innovations in Computer Science. Tsinghua University Press (2011).

Resources (Abstract Cryptography[1])

- A resource is a system with interfaces, one for each player Alice and Bob providing them with certain controls.
- The resources available to the players are given by a tuple $\mathcal{R} = \{R, R_A, R_B\}$, defined by three resources: R when both parties are honest and R_i when party $i \in \{A, B\}$ is dishonest.

Example: coin flipping



(a) **An unbiased resource:** CF, CF_A, CF_B same.

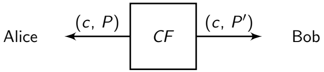
By varying the resources for dishonest parties, we obtain weaker resources.

[1] U. Maurer, R. Renner. The Second Symposium on Innovations in Computer Science. Tsinghua University Press (2011).

Resources (Abstract Cryptography[1])

- A resource is a system with interfaces, one for each player Alice and Bob providing them with certain controls.
- The resources available to the players are given by a tuple $\mathcal{R} = \{R, R_A, R_B\}$, defined by three resources: R when both parties are honest and R_i when party $i \in \{A, B\}$ is dishonest.

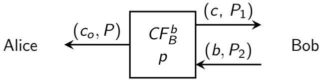
Example: coin flipping



(a) **An unbiased resource:** CF, CF_A, CF_B same.

By varying the resources for dishonest parties, we obtain weaker resources.

$$c_o = \begin{cases} b & \text{with prob. p} \\ c & \text{with prob. (1-p)} \end{cases}$$



$P_1 \prec P_2 \prec P$

(b) **A p biased resource:** The dishonest player can bias the value of honest player's output c_o towards a chosen bit b.

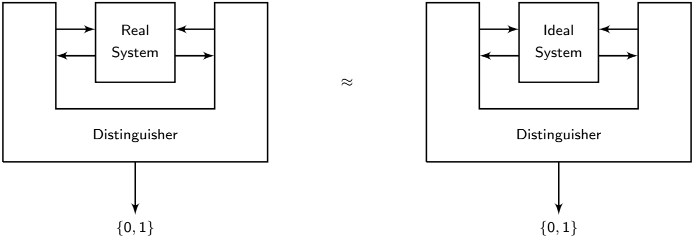
[1] U. Maurer, R. Renner. The Second Symposium on Innovations in Computer Science. Tsinghua University Press (2011).

Distance between resources: distinguishing advantage

Distance between resources: distinguishing advantage

- Security is defined in terms of the indistinguishability of real systems from the corresponding ideal systems.

- $\mathcal{R} \approx_\epsilon \mathcal{S}$ for a class of distinguishers $\mathbb{D}$ if any distinguisher $\mathcal{D} \in \mathbb{D}$ when given black-box access to either one of the resources can distinguish between the two (by outputting 0 or 1) with a maximum probability of $(\epsilon + 1)/2$.

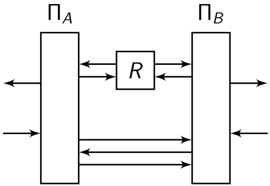


Security

- 3 security conditions: when both honest, Alice dishonest, Bob dishonest.

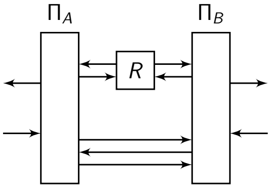
Security

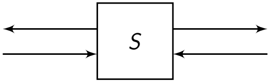
- 3 security conditions: when both honest, Alice dishonest, Bob dishonest.



Security

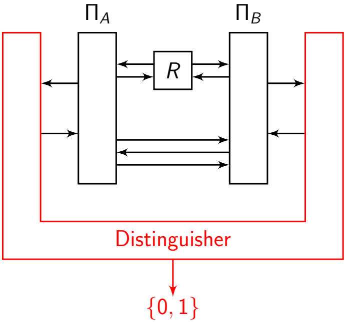
- 3 security conditions: when both honest, Alice dishonest, Bob dishonest.



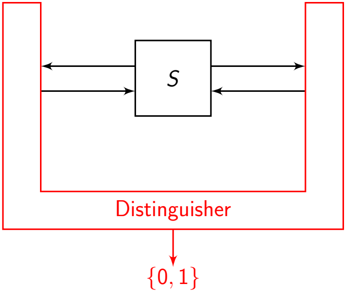


Security

- 3 security conditions: when both honest, Alice dishonest, Bob dishonest.

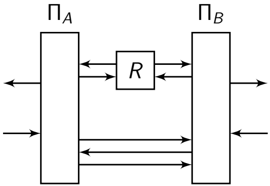


$\approx_\epsilon$

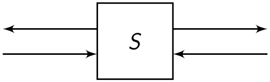


Security

- 3 security conditions: when both honest, Alice dishonest, Bob dishonest.

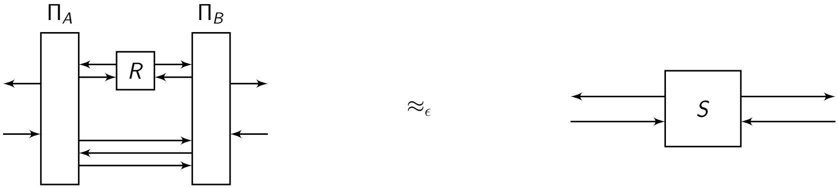


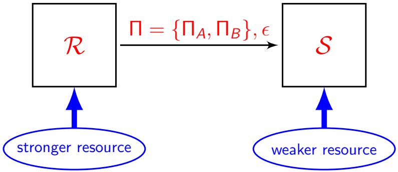
$$\approx_\epsilon$$



Security

- 3 security conditions: when both honest, Alice dishonest, Bob dishonest.





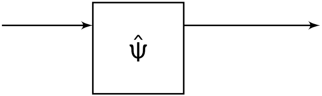
Causality (Causal Boxes[2])

Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.

[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

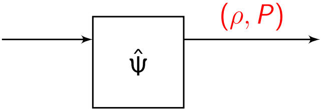
Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

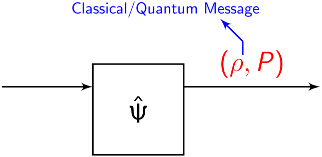
Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

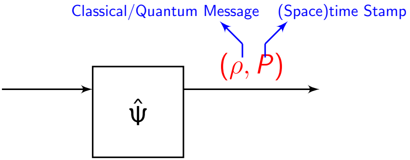
Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

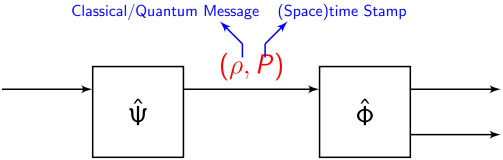
Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

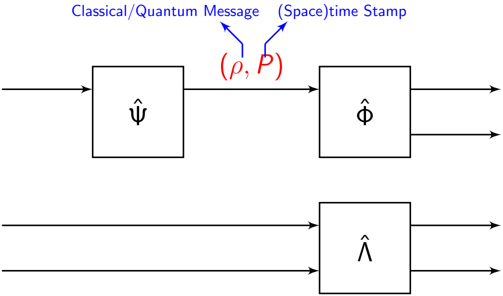
Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

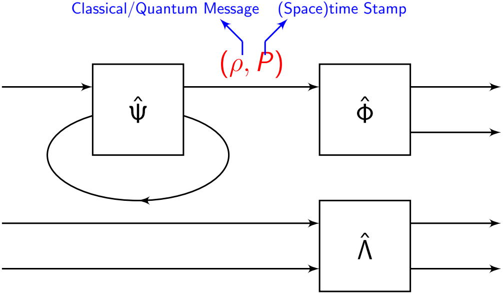
Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

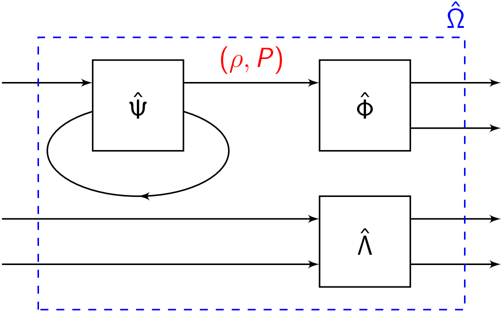
Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

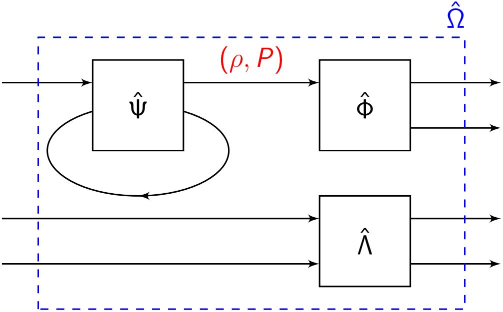
Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

Causality (Causal Boxes[2])

Each system (resource, protocol, distinguisher etc.) is modelled as a **causal box**.



Composition: Arbitrary composition of CBs is a new CB, irrespecitve of order of composition.

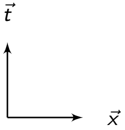
Causality: An output of a system can only depend on inputs produced in its causal past.

Can model messages sent in superpositions of orders in space-time.

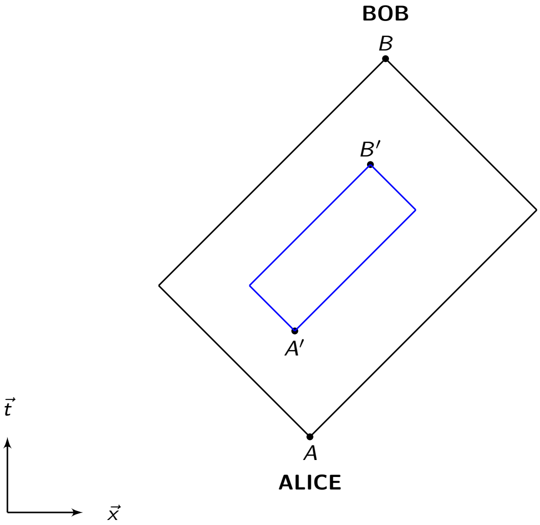
[2] C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).

New resource: channel with delay ($\mathcal{CD}$)

- $\mathcal{CD} = \{CD, CD_A, CD_B\}$ is characterised by the 4 space-time points $A \prec A' \prec B' \prec B$

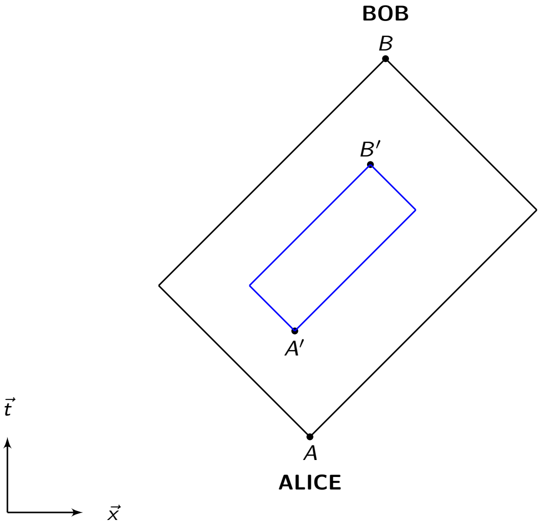


New resource: channel with delay ($\mathcal{CD}$)



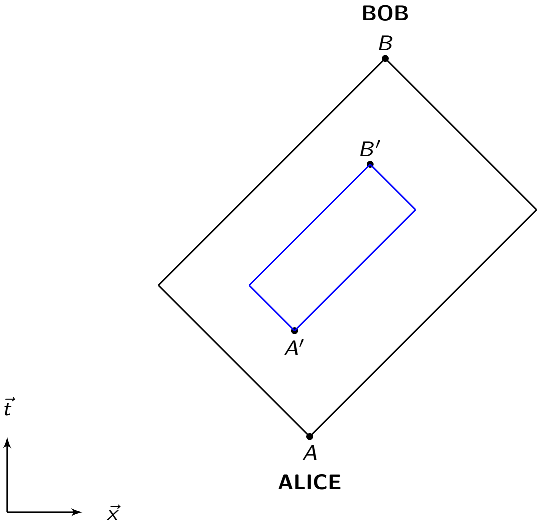
- $\mathcal{CD} = \{CD, CD_A, CD_B\}$ is characterised by the 4 space-time points $A \prec A' \prec B' \prec B$

New resource: channel with delay ($\mathcal{CD}$)



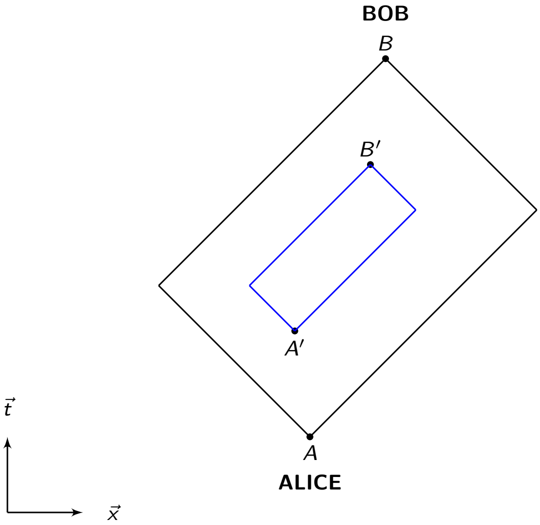
- $\mathcal{CD} = \{CD, CD_A, CD_B\}$ is characterised by the 4 space-time points $A \prec A' \prec B' \prec B$
- CD**:** Alice inputs c/q-bit at A , Bob receives the same bit at B

New resource: channel with delay ($\mathcal{CD}$)



- $\mathcal{CD} = \{CD, CD_A, CD_B\}$ is characterised by the 4 space-time points $A \prec A' \prec B' \prec B$
- CD: Alice inputs c/q-bit at A , Bob receives the same bit at B
- CD_A: Alice inputs c/q-bit at $A' \succ A$, Bob receives the same bit at B

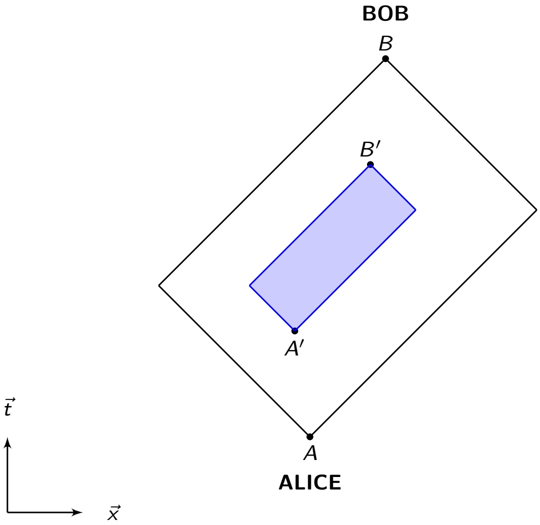
New resource: channel with delay ($\mathcal{CD}$)



- $\mathcal{CD} = \{CD, CD_A, CD_B\}$ is characterised by the 4 space-time points $A \prec A' \prec B' \prec B$

- CD**:** Alice inputs c/q-bit at A , Bob receives the same bit at B
- CD_A**:** Alice inputs c/q-bit at $A' \succ A$, Bob receives the same bit at B
- CD_B**:** Alice inputs c/q-bit at A, Bob receives the same bit at $B' \prec B$

New resource: channel with delay ($\mathcal{CD}$)



- $\mathcal{CD} = \{CD, CD_A, CD_B\}$ is characterised by the 4 space-time points $A \prec A' \prec B' \prec B$

- CD**:** Alice inputs c/q-bit at A , Bob receives the same bit at B
- CD_A**:** Alice inputs c/q-bit at $A' \succ A$, Bob receives the same bit at B
- CD_B**:** Alice inputs c/q-bit at A, Bob receives the same bit at $B' \prec B$

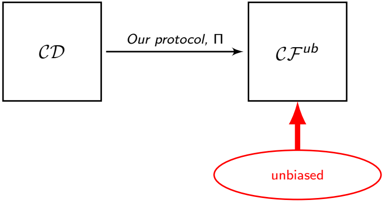
trusted region: region within which neither dishonest party can access the bit

RESULTS

Results: Constructibility of $\mathcal{CF}$ from $\mathcal{CD}$

Theorem 1

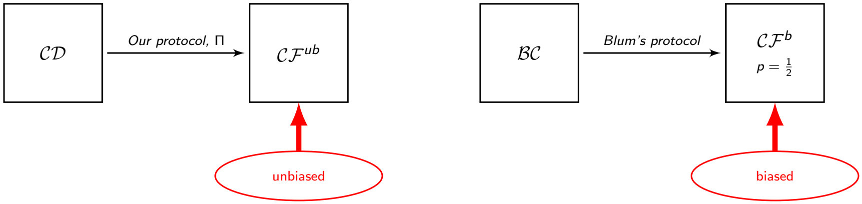
Given a classical Channel with Delay resource $\mathcal{CD}$, there exists a protocol $\Pi = \{\Pi_A, \Pi_B\}$ that perfectly constructs an unbiased Coin Flipping resource $\mathcal{CF}^{ub}$.



Results: Constructibility of $\mathcal{CF}$ from $\mathcal{CD}$

Theorem 1

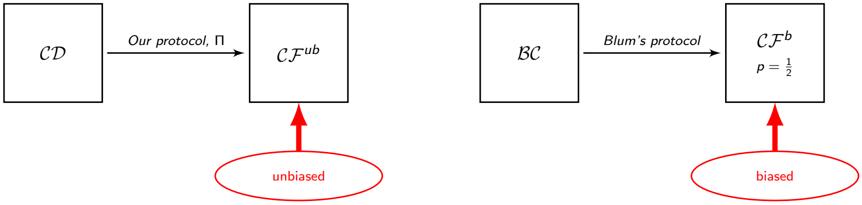
Given a classical Channel with Delay resource $\mathcal{CD}$, there exists a protocol $\Pi = \{\Pi_A, \Pi_B\}$ that perfectly constructs an unbiased Coin Flipping resource $\mathcal{CF}^{ub}$.



Results: Constructibility of $\mathcal{CF}$ from $\mathcal{CD}$

Theorem 1

Given a classical Channel with Delay resource $\mathcal{CD}$, there exists a protocol $\Pi = \{\Pi_A, \Pi_B\}$ that perfectly constructs an unbiased Coin Flipping resource $\mathcal{CF}^{ub}$.



Π constructs a stronger resource as compared to Blum's protocol.

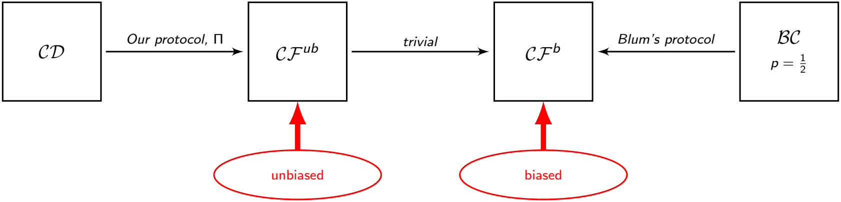
Secure against quantum and non-signalling adversaries

Results: Impossibility of relativistic bit commitment

Results: Impossibility of relativistic bit commitment

Theorem 2

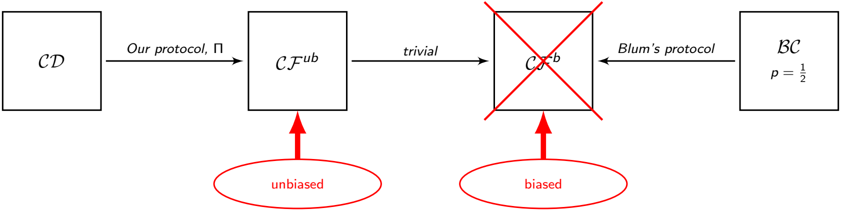
It is impossible to construct, with $\epsilon < \frac{1}{6}(1-p)$, a p-biased Coin Flipping resource between two mutually distrusting parties solely through the exchange of messages through any relativistic or non-relativistic protocol, be it classical, quantum or non-signalling.



Results: Impossibility of relativistic bit commitment

Theorem 2

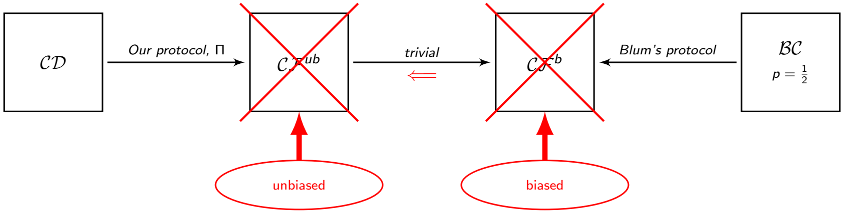
It is impossible to construct, with $\epsilon < \frac{1}{6}(1-p)$, a p-biased Coin Flipping resource between two mutually distrusting parties solely through the exchange of messages through any relativistic or non-relativistic protocol, be it classical, quantum or non-signalling.



Results: Impossibility of relativistic bit commitment

Theorem 2

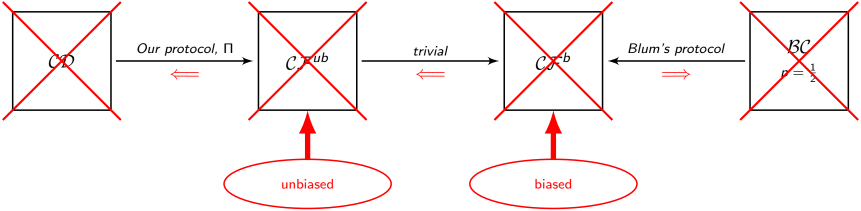
It is impossible to construct, with $\epsilon < \frac{1}{6}(1-p)$, a p-biased Coin Flipping resource between two mutually distrusting parties solely through the exchange of messages through any relativistic or non-relativistic protocol, be it classical, quantum or non-signalling.



Results: Impossibility of relativistic bit commitment

Theorem 2

It is impossible to construct, with $\epsilon < \frac{1}{6}(1-p)$, a p-biased Coin Flipping resource between two mutually distrusting parties solely through the exchange of messages through any relativistic or non-relativistic protocol, be it classical, quantum or non-signalling.

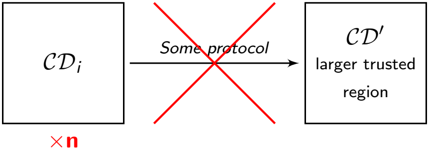


$\Rightarrow$ Existing protocols are not secure when composed, even in bounded/noisy storage models.

Results: Impossibility of "improving" a $\mathcal{CD}$

Theorem 3

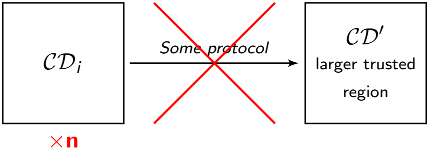
Given n channel's $\mathcal{CD}^1$,...,$\mathcal{CD}^n$ between Alice and Bob, it is impossible to construct with $\epsilon \leq \frac{1}{8}$, a channel $\mathcal{CD}'$ between the two parties with a larger trusted region than that of all of the channels used.



Results: Impossibility of "improving" a $\mathcal{CD}$

Theorem 3

Given n channel's $\mathcal{CD}^1,\ldots,\mathcal{CD}^n$ between Alice and Bob, it is impossible to construct with $\epsilon \leq \frac{1}{8}$, a channel $\mathcal{CD}'$ between the two parties with a larger trusted region than that of all of the channels used.

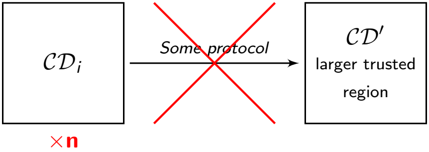


Impossible even if honest players send messages in a superposition of orders through the channels.

Results: Impossibility of "improving" a $\mathcal{CD}$

Theorem 3

Given n channel's $\mathcal{CD}^1$,...,$\mathcal{CD}^n$ between Alice and Bob, it is impossible to construct with $\epsilon \leq \frac{1}{8}$, a channel $\mathcal{CD}'$ between the two parties with a larger trusted region than that of all of the channels used.



Impossible even if honest players send messages in a superposition of orders through the channels.

⇒ Cannot increase trusted region.

⇒ Cannot increase "effective commitment time" even with n channels.

Conclusions and Outlook

Conclusions and Outlook

- Minimal resource(s) required to construct $\mathcal{BC}$, $\mathcal{CD}$?

Conclusions and Outlook

- Minimal resource(s) required to construct $\mathcal{BC}$, $\mathcal{CD}$?
- Novel possibility and impossibility results in relativistic cryptography, classifying possible and impossible tasks.

Conclusions and Outlook

- Minimal resource(s) required to construct $\mathcal{BC}$, $\mathcal{CD}$?
- Novel possibility and impossibility results in relativistic cryptography, classifying possible and impossible tasks.
- Modelling cryptographic protocols involving superposition of temporal orders and dynamic ordering of messages.

Conclusions and Outlook

- Minimal resource(s) required to construct $\mathcal{BC}$, $\mathcal{CD}$?
- Novel possibility and impossibility results in relativistic cryptography, classifying possible and impossible tasks.
- Modelling cryptographic protocols involving superposition of temporal orders and dynamic ordering of messages.
- Physically motivated framework for studying spatio-temporal correlations and their applications to relativistic cryptography.

Conclusions and Outlook

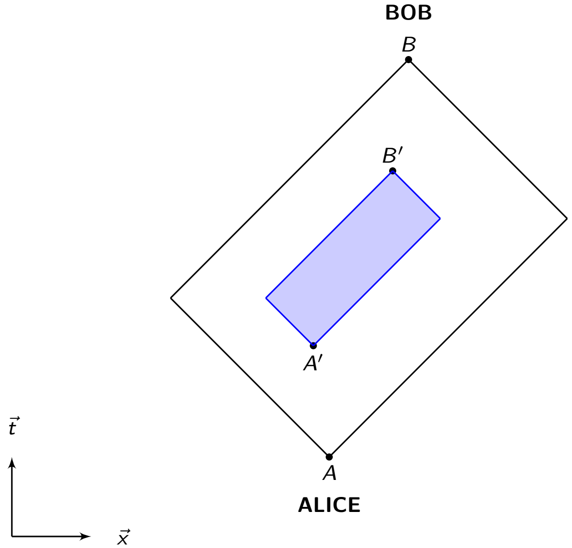
- Minimal resource(s) required to construct $\mathcal{BC}$, $\mathcal{CD}$?
- Novel possibility and impossibility results in relativistic cryptography, classifying possible and impossible tasks.
- Modelling cryptographic protocols involving superposition of temporal orders and dynamic ordering of messages.
- Physically motivated framework for studying spatio-temporal correlations and their applications to relativistic cryptography.
- Generalise to dynamical and indefinite causal structures, e.g., QM+GR.

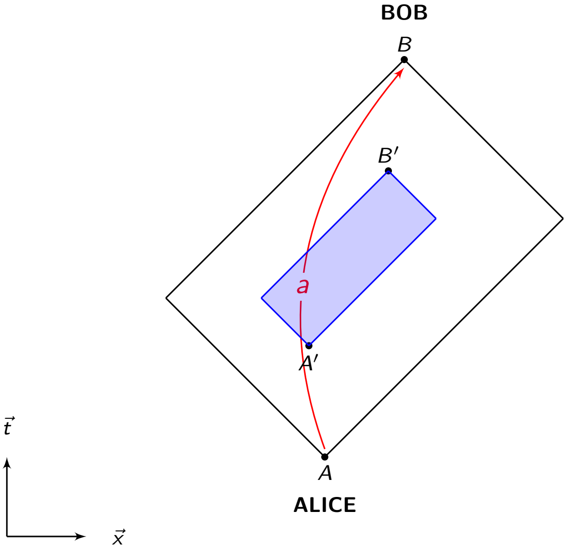
Thank you for your attention!

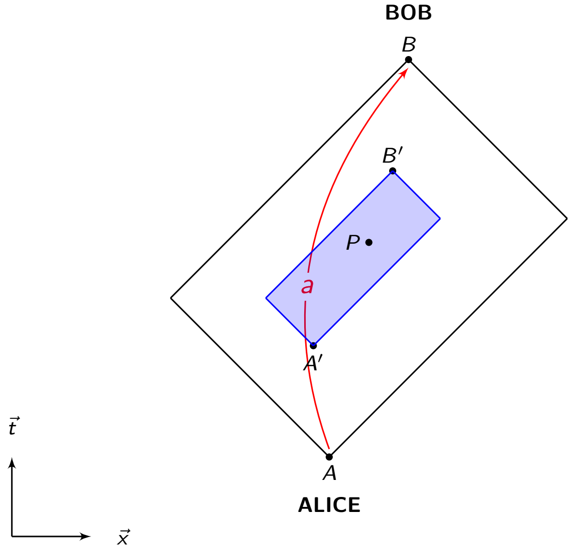
References

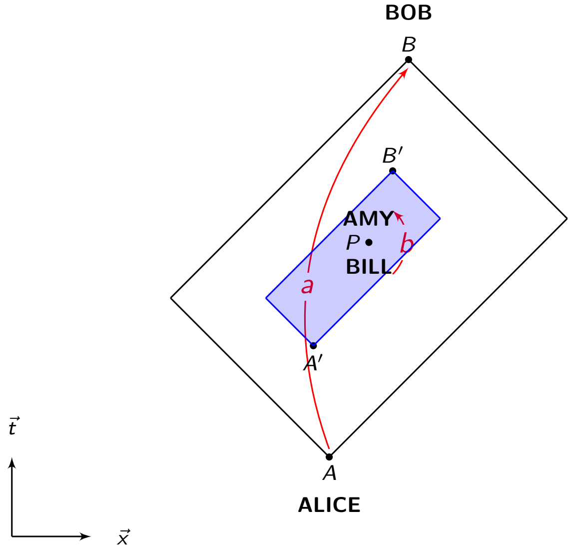
- U. Maurer, R. Renner. The Second Symposium on Innovations in Computer Science. Tsinghua University Press (2011).
- C. Portmann , C. Matt, U. Maurer , R. Renner, B. Tackmann. IEEE Transactions on Information Theory, Vol. 63, No. 5 (2017).
- J. Kaniewski. PhD Thesis, Centre for Quantum Technologies, National University of Singapore. arXiv:1512.00602 [quant-ph] (2015).
- A. Kent. Physical Review Letters, Vol. 109 (2012).
- J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner. IEEE Transactions on Information Theory, Vol. 59, No. 7 (2013).
- G. Demay, U. Maurer. Proceedings of the 2013 IEEE International Symposium on Information Theory,Turkey (2013).
- T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden. Physical Review Letters, Vol. 115, Pages 030502 (2015).

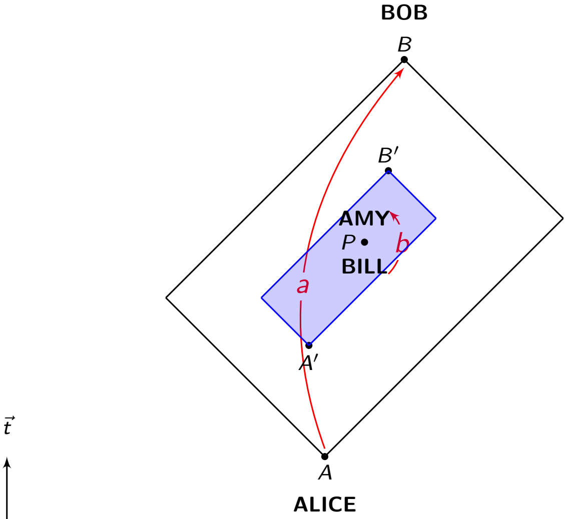
Additional Slides


BOB
B
B'
A'
A
ALICE
$\vec{t}$
$\vec{x}$


BOB
B
B'
a
A'
A
ALICE
$\vec{t}$
$\vec{x}$

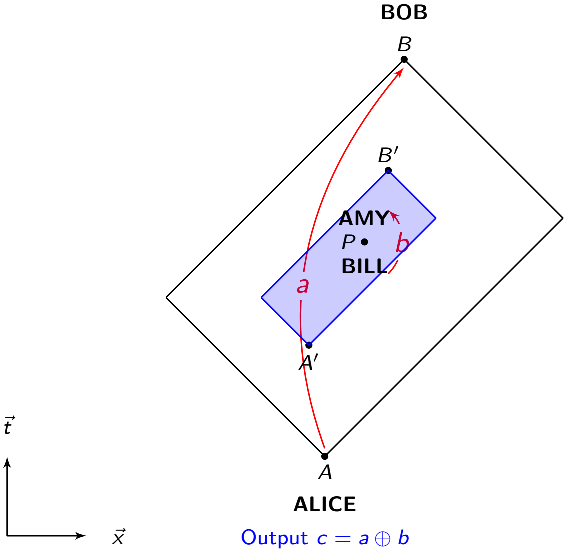

BOB
B
B'
P
a
A'
A
ALICE
$\vec{t}$
$\vec{x}$


BOB
B
B′
AMY
P
BILL
a
b
A′
A
ALICE
$\vec{t}$
$\vec{x}$



Output $c = a \oplus b$

Alice at $P_A \succ P$, Bob at $P_B \succ B$

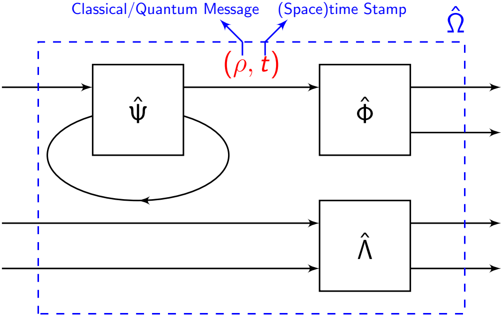


Output $c = a \oplus b$

Alice at $P_A \succ P$, Bob at $P_B \succ B$

Secure against quantum and non-signalling adversaries

Discussion: indefinite causal structures



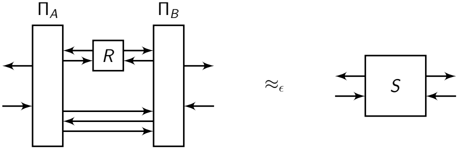
Causal Boxes (Portmann et. al. 2017)

- global and local order
- some indefinite causal structures (QS)
- quantum and NS (PR boxes)
- physically motivated

Process Matrices (Oreshkov et. al. 2012)

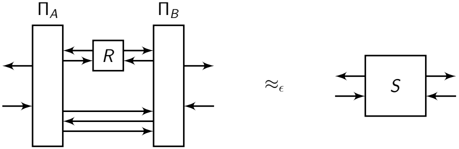
- no global, only local order
- QS+more general causal structures
- local quantum operations
- theoretical

Insights into properties of physical causal structures?

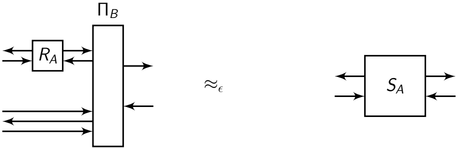


(a) $\Pi_A \, \mathrm{R} \, \Pi_B \approx_\epsilon \mathrm{S}$

- For every resource $\mathcal{R}$, three ideal functionalities are defined: R when both players are honest and R_i when player $i \in \{A, B\}$ is dishonest.

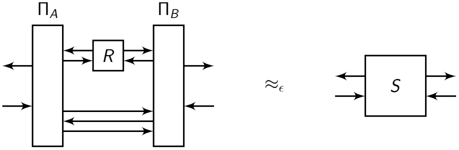


(a) $\Pi_A \, \mathrm{R} \, \Pi_B \approx_\epsilon \mathrm{S}$

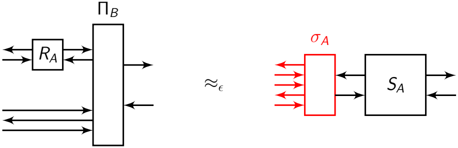


(b) $\mathrm{R_A} \, \Pi_B \approx_\epsilon \quad \mathrm{S_A}$

- For every resource $\mathcal{R}$, three ideal functionalities are defined: R when both players are honest and R_i when player $i \in \{A, B\}$ is dishonest.

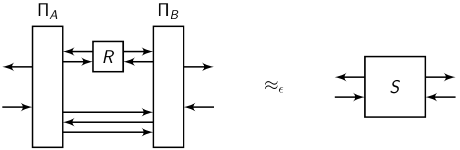


(a) $\Pi_A \, \mathrm{R} \, \Pi_B \approx_\epsilon \mathrm{S}$

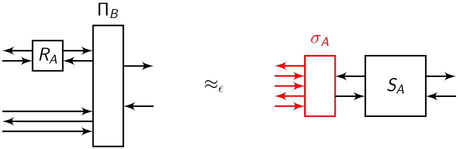


(b) $\mathrm{R_A} \, \Pi_B \approx_\epsilon \sigma_\mathrm{A} \, \mathrm{S_A}$

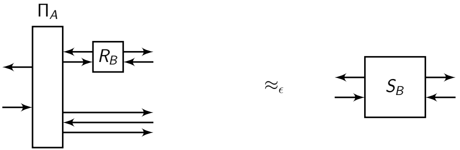
- For every resource $\mathcal{R}$, three ideal functionalities are defined: R when both players are honest and R_i when player $i \in \{A, B\}$ is dishonest.



(a) $\Pi_A \, \mathrm{R} \, \Pi_B \approx_\epsilon \mathrm{S}$

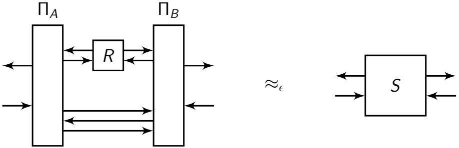


(b) $\mathrm{R_A} \, \Pi_B \approx_\epsilon \sigma_\mathrm{A} \, \mathrm{S_A}$

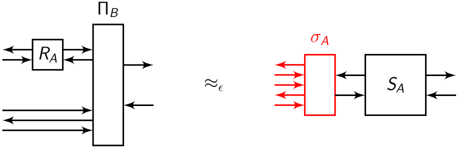


(c) $\Pi_A \, \mathrm{R_B} \approx_\epsilon \mathrm{S_B}$

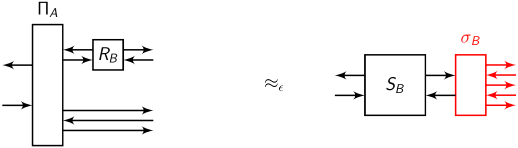
- For every resource $\mathcal{R}$, three ideal functionalities are defined: R when both players are honest and R_i when player $i \in \{A, B\}$ is dishonest.



(a) $\Pi_A \, \mathrm{R} \, \Pi_B \approx_\epsilon \mathrm{S}$

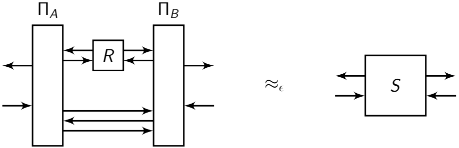


(b) $\mathrm{R_A} \, \Pi_B \approx_\epsilon \sigma_\mathrm{A} \, \mathrm{S_A}$

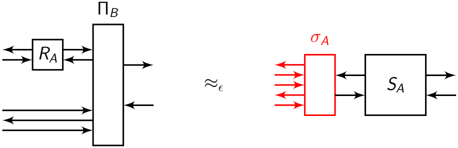


(c) $\Pi_A \, \mathrm{R_B} \approx_\epsilon \mathrm{S_B} \, \sigma_\mathrm{B}$

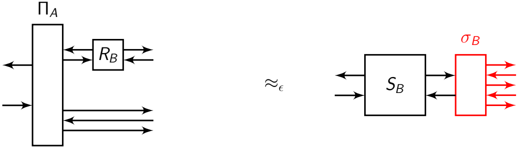
- For every resource $\mathcal{R}$, three ideal functionalities are defined: R when both players are honest and R_i when player $i \in \{A, B\}$ is dishonest.



(a) $\Pi_A \, \mathrm{R} \, \Pi_B \approx_\epsilon \mathrm{S}$



(b) $\mathrm{R_A} \, \Pi_B \approx_\epsilon \sigma_{\mathrm{A}} \, \mathrm{S_A}$



(c) $\Pi_A \, \mathrm{R_B} \approx_\epsilon \mathrm{S_B} \, \sigma_{\mathrm{B}}$

- For every resource $\mathcal{R}$, three ideal functionalities are defined: R when both players are honest and R_i when player $i \in \{A, B\}$ is dishonest.

- Composable Security: A protocol (Π_A, Π_B) constructs $\mathcal{S} = \{\mathrm{S}, \mathrm{S_A}, \mathrm{S_B}\}$ from $\mathcal{R} = \{\mathrm{R}, \mathrm{R_A}, \mathrm{R_B}\}$ securely within ϵ if $\exists \, \sigma_{\mathrm{A}}$ *and* σ_{B} for which the three conditions (a)-(c) hold.