PAPER • OPEN ACCESS

Composable security in relativistic quantum cryptography

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
22 November 2018

REVISED
8 February 2019

ACCEPTED FOR PUBLICATION
8 March 2019

PUBLISHED
30 April 2019

PAPER

Composable security in relativistic quantum cryptography

V Vilasini[1,2,4], Christopher Portmann[3] and Lídia del Rio[2]

[1] Department of Mathematics, University of York, Heslington, York, YO10 5DD, United Kingdom
[2] Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland
[3] Department of Computer Science, ETH Zürich, 8092 Zürich, Switzerland
[4] Author to whom any correspondence should be addressed.

E-mail: vv577@york.ac.uk, chportma@ethz.ch and lidia@phys.ethz.ch

Keywords: quantum cryptography, relativistic quantum cryptography, bit commitment, composable security, relativistic quantum communication, abstract cryptography, quantum resource theories

Abstract

Relativistic protocols have been proposed to overcome certain impossibility results in classical and quantum cryptography. In such a setting, one takes the location of honest players into account, and uses the signalling limit given by the speed of light to constraint the abilities of dishonest agents. However, composing such protocols with each other to construct new cryptographic resources is known to be insecure in some cases. To make general statements about such constructions, a composable framework for modelling cryptographic security in Minkowski space is required. Here, we introduce a framework for performing such a modular security analysis of classical and quantum cryptographic schemes in Minkowski space. As an application, we show that (1) fair and unbiased coin flipping can be constructed from a simple resource called channel with delay; (2) biased coin flipping, bit commitment and channel with delay through any classical, quantum or post-quantum relativistic protocols are all impossible without further setup assumptions; (3) it is impossible to securely increase the delay of a channel, given several short-delay channels as ingredients. Results (1) and (3) imply in particular the non-composability of existing relativistic bit commitment and coin flipping protocols.

1. Introduction

1.1. Motivation

As global efforts for quantum communication in space boom with the first satellite implementations of quantum key distribution [1–3], it becomes crucial to develop the theoretical tools to guarantee that these communications are secure. In order to do so, we must take into account not only quantum effects but also relativistic ones. Our manuscript is the first to provide a complete framework for composable security analysis of quantum and post-quantum cryptography in relativistic settings. As a first application of this tool set, we prove several construction and impossibility results.

Composability. To understand composability and why it matters, it is helpful to look at a classical example. In modern chess, the Elo ranking system is vulnerable to man-in-the-middle attacks (MITMs), where a weak player could play two online games in parallel against stronger players, playing a different colour in each game, and simply forward the moves of the opponents to each other. At the end, the player will lose one of the games and win the other (or tie in both games), but given that the Elo system favours lower-rated players, the attacker ends up with a net gain of points, independently of the result. Such a vulnerability could not be detected by a stand-alone security analysis (which checks what happens if the games are considered individually), but only by a composable security analysis, which considers the possibility of games being used in a modular fashion, as part of a larger strategy. Similarly, several known proposals for quantum cryptographic protocols that exploit relativistic constraints are proven insecure by our paper.

Cryptography as a resource theory. We follow the approach of Abstract Cryptography [4], which views cryptography as a resource theory: a protocol between some players constructs a resource (e.g. a system that

produces a random coin flip) from some other resource (e.g. a system that allows bit commitment)[5]. Here we address construction of resources in relativistic quantum cryptography, and security definitions that are robust under composition of constructions. By 'relativistic' we mean simple special relativity: Minkowski space–time with limited signalling speed.

A cryptographic resource: bit commitment. To illustrate the need for a composable analysis of relativistic quantum cryptography, we focus on bit commitment protocols, which have attracted interest in recent years [6–9]. Bit commitment is a crucial cryptographic primitive, from which we can construct oblivious transfer[6] [10], multi-party computation (see footnote 5) [10], coin flipping [12], and zero-knowledge proofs [13, 14].

A bit commitment protocol ($\mathcal{BC}$) between two players (say Alice and Bob) typically involves two phases. In the *commit phase*, Alice commits to a bit $a \in \{0, 1\}$ with Bob by exchanging information with him. In the *open phase*, Alice chooses to open her commitment to Bob and reveals her bit to him through an exchange of information. Intuitively speaking, security of bit commitment has three requirements.

Hiding: when Alice is honest, Bob has no information about a before the open phase.

Binding: when Bob is honest, Alice must not be able to change the value of a between the commit and open phases without him detecting her malicious behavior.

Complete: honest Alice always has the possibility of opening her commitment, and in this case, Bob always receives a.

These requirements can be formalized under different security definitions. Not all models of security of $\mathcal{BC}$ are composable: for example the ϵ-weakly binding definition of [8] is not. There, Alice is allowed to commit to a bit without knowing its value, which if used as a subroutine in a coin flipping protocol, would allow dishonest players to perfectly correlate the coin flips from different coins. Similar weaknesses in current definitions of relativistic bit commitment have been exploited to show that using these protocols as subroutine in a larger cryptosystem is insecure [15, appendix A]. In this work, we model security such that the constructed $\mathcal{BC}$ resource can be securely used in arbitrary context. Let us first review some known results.

1.2. Previous results

Impossiblity of classical bit commitment. In 2001, Canetti and Fischlin showed that constructing a $\mathcal{BC}$ resource without any setup assumptions is impossible [16]. They proved this for a classical non-relativistic setting through a classical MITM. Consider a cheating Alice simultaneously running two $\mathcal{BC}$ protocols: one with Bob, in which she is the committer, and one with Charlie, in which she is the receiver. She can commit to Charlie's bit with Bob by simply forwarding their messages to each other during the commit phase. Note that the proof from [16] is restricted to the classical setting, and does not imply the impossibility of constructing a $\mathcal{BC}$ resource in either quantum or relativistic settings.

Impossibility of quantum bit commitment. Using a stand-alone definition with information-theoretic security, Mayers, and Lo and Chau [17–19] independently showed between 1996 and 1997 that no secure quantum bit commitment protocol can be constructed without further assumptions (for example regarding the operations that (dishonest) parties can perform on their systems), because due to Uhlmann's theorem, if Bob cannot distinguish between the commitment to a 0 or a 1, then there exists a unitary on Alice's system allowing her to change the commitment from 0 to 1.

Possibility results. Positive results are obtained by either restricting the adversary's capabilities or making extra setup assumptions. For example, along with their impossiblity result, Canetti and Fischlin also show that a $\mathcal{BC}$ resource can be constructed if we assume a common reference string (CRS) shared between the players and computationally bounded players [16]. In the quantum case, Unruh showed in [20] that if the adversary has bounded quantum memory, bit commitment that is composable in certain restricted settings is possible[7]. In [21] Unruh also shows that everlasting quantum bit commitment is achievable, if we assume signature cards as trusted setup.

Relativistic protocols. In the hope of avoiding such attacks without making unrealistic setup assumptions or unproven assumptions on the adversary's capabilities, one turns to relativistic protocols and imposes relativistic causal constraints on agents located in Minkowski space—no-signalling between space-like separated agents and a maximum propagation speed for signals. An example is Kent's 2012 relativistic $\mathcal{BC}$ protocol [7], which is immune to the Mayers-Lo-Chau attack, since the sender splits into two space-like separated agents who can no

[5] For comparison, in the universal Composability (UC) framework [5], resources correspond to ideal functionalities.

[6] Constructing oblivious transfer (and thus multi-party computation) from bit commitment requires agents to have access to quantum operations [10]. An alternative model and construction of (delegated) quantum multi-party computation has been proposed in [11].

[7] The model used in [20] does not guarantee security when a protocol is composed with itself. There is thus no contradiction with the impossibility proof for bit commitment in the bounded storage model in this work, which shows that any bit commitment protocol run in parallel with another instance of itself is insecure.

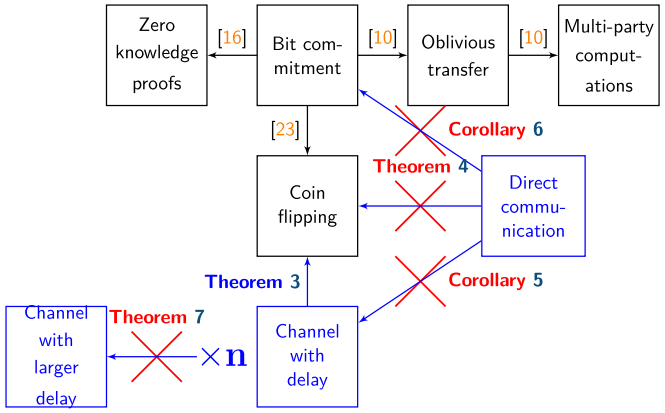


Figure 1. Summary of our results. We assume Minkowski space–time with limited speed of signalling (upper-bounded by the speed of light). Existing results are represented in black and the new contributions of this paper in blue and red. An arrow $\mathcal{R} \rightarrow \mathcal{S}$ means that it is possible to construct resource $\mathcal{S}$ from resource $\mathcal{R}$. When the arrow is crossed, that means that no such construction exists without further setup assumptions such as shared resources. For example, theorem 3 shows that Coin Flipping between 2 parties can be securely constructed from a Channel with Delay, and theorem 7, corollaries 5 and 6 show that it is impossible to construct Coin Flipping (biased or unbiased), Channel with Delay or Bit Commitment between two mutually distrusting parties solely through direct communication between them. Theorem 7 implies that starting with n channels with delay, it is impossible to construct a channel with a 'larger delay' without further setup assumptions. Note that all impossibility results in this figure hold for any classical, quantum or relativistic protocol. For $\mathcal{BC}$ and $\mathcal{CF}$, impossibility through classical/quantum protocols was previously known [16–18] but the generalisation to the relativistic case is one of the key contributions of this paper.

longer perform suitable unitaries on their joint systems. Like other relativistic $\mathcal{BC}$ protocols, this protocol implements a timed commitment which is secure only within a time window given by the time taken by light to travel between remote agents. However, it only satisfies a non-composable, weakly-binding security definition [8]. As we will see, this protocol is susceptible to a MITM and therefore cannot be securely run as a subroutine in arbitrary protocols[8].

Composability of relativistic protocols. In relativistic settings, the existing negative results are obtained by analyzing specific examples of protocols and attacks where composition fails [8, 15]. However, without an overall coherent framework for modelling composability in relativistic cryptography, it is impossible to obtain general positive and negative results.

1.3. Overview and scope of our results

In this work we introduce a framework for modelling composable cryptographic security in the presence of classical, quantum and no-signalling adversaries, and apply it to prove new positive and negative results in relativistic quantum cryptography. We do this by modelling the abstract information-processing systems of the *Abstract Cryptography* framework [4] as *Causal Boxes* [22], which we instantiate with Minkowski space–time. Our framework can also be applied to situations where agents exchange a superposition of different numbers of messages in a superposition of orders in time, and provides an operational formalism for studying indefinite causal structures. We note that the model of computation used in the UC framework [20] does not support Minkowski space–time, so UC cannot be used to analyze relativistic protocols.

We analyse three cryptographic resources, defined in section 2. Coin flipping ($\mathcal{CF}$, including biased variations) and bit commitment ($\mathcal{BC}$) are standard in the composable security literature, though in this work our formalization involves space–time—inputs and outputs are produced at certain locations in Minkowski space. We also introduce a channel with delay ($\mathcal{CD}$), which is motivated by the fact that in relativistic bit commitment protocols, the commitment is automatically opened after some (predefined) time, thus resembling a $\mathcal{CD}$ more than a $\mathcal{BC}$[9]. The following results are summarized in figure 1.

Constructibility results. We show that an unbiased coin flipping resource $\mathcal{CF}$ can be constructed from a channel with delay resource, $\mathcal{CD}$ (theorem 3). For comparison, Blum's protocol [12], constructs a weaker, biased[10] coin flipping resource from a bit commitment resource [23]. We provide an explicit protocol to

[8] Sharing an authentic channel does not help the players to avoid the MITM attack, since the issue is not a third party intercepting and changing the messages, but a dishonest player running two protocols in parallel, and forwarding the messages from one protocol to the other.

[9] There may be different ways of modeling a relativistic bit commitment resource, e.g. the committer may have the option of aborting before the commitment is opened, see the discussion in section 2.3.3.

[10] Originally, Blum's protocol constructs an *unfair* coin flip, in which one party can abort after seeing the flip [12]. This may be transformed into a *biased* coin flip if the honest party flips a coin locally when the dishonest party aborts [23].

construct $\mathcal{CF}$ from $\mathcal{CD}$ and prove its security. The proof holds even in the presence of adversaries that are not bounded by quantum physics, but only non-signalling constraints.

Impossibility results. In theorem 4 we show that constructing a (biased) coin flipping resource is impossible in the relativistic setting without additional setup assumptions (e.g. the presence of a shared resource such as $\mathcal{CD}$). This result holds even if the players are only bounded by non-signalling constraints[11], or if we restrict the adversary to being computationally bounded or having bounded storage[12]. Impossibility of bit commitment follows from Blum's construction [12, 23] of $\mathcal{CF}$ from $\mathcal{BC}$ (corollary 6), and impossibility of constructing a channel with delay $\mathcal{CD}$ follows from theorem 3 (corollary 5).

Since the literature on relativistic bit commitment also studies the case of extending the time during which such a commitment remains secure, we also look at the task of constructing a channel with a long delay $\mathcal{CD}_{\text{long}}$ from multiple channels (labelled by i) with shorter delays $\{\mathcal{CD}^i_{\text{short}}\}_i$. We show that this again is impossible without other setup assumptions than the assumed channels with delays $\{\mathcal{CD}^i_{\text{short}}\}_i$ (theorem 7). This impossibility result holds irrespective of whether the protocol is classical, quantum or non-signalling (see footnote 10), and also holds if the adversary is computationally bounded.

Consequences of these results. Many quantum protocols have been proposed in the relativistic setting to circumvent classical impossibility results for $\mathcal{BC}$. To the best of our knowledge, none of these protocols have been successfully used as subroutines in larger cryptosystems (which is the main motivation for constructing such primitives), and some attempts to do so are known to be insecure [15, appendix A]. But due to the lack of composable framework that can model Minkowski space, it has been impossible to prove whether composable constructions of these resources do exist. Our results show that allowing quantum (and even non-signalling (see footnote 10)) protocols that respect relativistic constraints is not sufficient to construct $\mathcal{BC}$, $\mathcal{CF}$, or $\mathcal{CD}$ without additional assumptions. This implies that none of the proposed relativistic bit commitment schemes are composable (e.g. [6–9]). This also extends to the non-relativistic setting (e.g. [24]), since a non-relativistic protocol corresponds to the special case where all players are in the same position in space (and thus do not have any constraints on the speed of communication). Our proof also holds against computationally bounded adversaries, and adversaries with bounded storage, which implies that results in the bounded storage model are not composable either (e.g. [25]).

Another problem considered in the literature on relativistic bit commitment is that of extending the time during which commitment remains secure. Our results show that this cannot be done with a composable definition of timed relativistic commitment (see the definition of $\mathcal{CD}$ in section 2.3 and following discussion), even when one starts off with arbitrarily many (composably) secure commitments of shorter duration. Hence the techniques used in [9, 26] to extend the time of a relativistic bit commitment cannot be used in a composable way. Just as the previous results, this also holds when the adversary is computationally limited or has bounded quantum memory.

The framework naturally allows positive results to be proven as well—by making extra setup assumptions. This approach was used by Canetti and Fischlin [16] who show that one can construct a $\mathcal{BC}$ resource assuming a shared CRS and computationally bounded players, and Unruh [21], who showed (everlasting) quantum bit commitment is achievable if we assume signature cards as trusted setup. In this work we construct a $\mathcal{CF}$ resource from a $\mathcal{CD}$, and leave open the problem of finding weaker assumptions that still allow $\mathcal{CF}$ or $\mathcal{BC}$ to be constructed.

A takeaway message from this work is that one cannot achieve $\mathcal{BC}$ or $\mathcal{CF}$ simply from relativity or quantum mechanics without further setup assumptions. This implies that existing quantum and relativistic protocols for these primitives can not be securely used as subroutines in arbitrary constructions. It is currently unknown whether there exist assumptions weaker than what is possible classically to justify the use of such quantum or relativistic protocols.

1.4. Structure of this paper

In section 2 we introduce the model that we use to prove our results. We provide a pedagogical introduction to the Abstract Cryptography framework in section 2.1. We give an overview of Causal Boxes instantiated with Minkowski space in section 2.2—a formal presentation of Causal Boxes is given in appendix A. And in section 2.3 we define the two party resources $\mathcal{CF}$, $\mathcal{CD}$, and $\mathcal{BC}$. Our results are then presented in section 3 and the proofs are given in appendix B. Finally, we conclude in section 4 with a discussion of these results.

[11] A non-signalling player can generate non-signalling correlations between their own trusted agents at different locations. Note however that if we were to allow two distrusting players (Alice and Bob) to generate non-signalling correlations between them, this would have to be modeled as an extra setup assumption, namely a shared resource.

[12] This excludes in particular protocols where players are not necessarily spatially separated, but can meet at some location, as do the impossiblity results in the classical case [16].

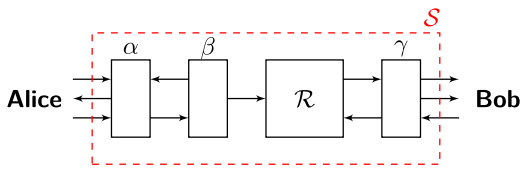


Figure 2. Starting from a resource $\mathcal{R}$, converters α, β and γ construct a new resource $\mathcal{S} = \alpha_A\beta_A\gamma_B\mathcal{R}$. The sequences of arrows at the interfaces between objects represent (arbitrary) rounds of communication. For simplicity, we may omit the indices, $\mathcal{S} = \alpha\beta\mathcal{R}\gamma$, so that converters to the left of the resource (α, β) are implicitly connected to Alice's interface, and converters on the right (γ) are connected to Bob's.

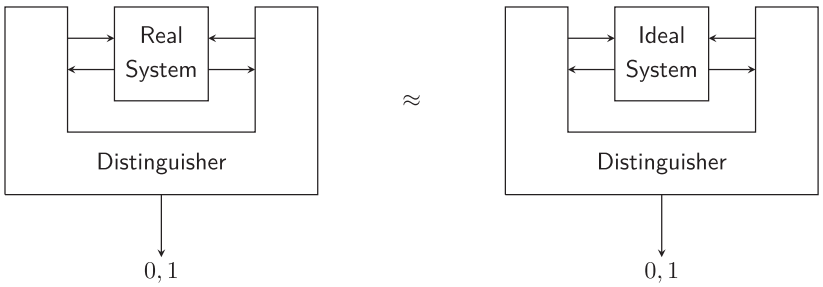


Figure 3. *Security in terms of distinguishers.* Composable security of a real resource is defined in terms of the success probability of a class of distinguishers (for example computationally bounded or unbounded, classical, quantum or non-signalling) in distinguishing the real system from the ideal one. A distinguisher, modelling all the environment of a resource, is given black-box access to either the real or the ideal systems and a complete description of the input–output behaviour of both systems and must guess which one it was interacting with by outputting either a 0 or a 1. The distinguishing advantage is then given by the statistical distance between the two random bits output when interacting with the real and ideal systems, respectively.

2. Framework

2.1. Composable security: the abstract cryptography framework [4]

2.1.1. Resources, converters and distinguishers

Let us review the basics of the abstract cryptography framework [4]. The following is adapted from [27] for the case of protocols between two mutually distrusting parties (e.g. bit commitment, coin flipping) and has been simplified for our purposes. We refer the reader to [4, 27] for more general definitions and further examples.

Abstract systems. Abstract cryptography views cryptography as a resource theory: a protocol constructs a resource from some other resource, e.g. Blum's protocol [12] constructs a coin flipping resource from a bit commitment resource. In this section we introduce the building blocks of the framework—resources, converters (e.g. protocols) and a notion of distance (distinguishability) between resources—and in section 2.2 we explain how these objects are instantiated with Causal Boxes [22].

A *resource* $\mathcal{R}$ in a two party setting is an (abstract) system with interfaces $i \in \{A, B\}$, each accessible to a user i (and their trusted agents) providing them with certain controls. An operation that is performed by a party at their interface is modeled as a *converter*: a system α with an outside and an inside interface, the inner interface connects to an interface i of the resource, and the outer interface becomes the new interface of the resulting resource. We write $\alpha_i\mathcal{R}$ to denote the resource resulting from connecting α to the i interface of $\mathcal{R}$. This is illustrated in figure 2.

Distinguishing resources. The security of a cryptographic system is quantified in terms of *distinguishability* from a corresponding ideal system (figure 3). For example, the ideal resource 'random bit generator', $\mathcal{S}$, would be a black box that generates and outputs a uniformly random bit at a time t which is independent of everything outside the box. A specific practical implementation $\mathcal{R}$ of this functionality could be a quantum protocol: prepare a qubit in a state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, measure it in the Z-basis and output the measurement result at time t. Treated as black boxes, both resources $\mathcal{R}$ and $\mathcal{S}$ output a uniformly random classical bit and cannot be distinguished by an outsider.

For more complex resources, we may ask: distinguishability from whose perspective? Here, the traditional notion of an adversary is generalized to an arbitrary *distinguisher* which models not only possible adversarial behaviour but also the whole environment of a cryptographic protocol/resource. The main motivation for composable security is that a resource remains secure even when it is used as a sub-routine in arbitrary protocols. While doing so, protocols can in general access all interfaces of the resource and perform information processing

steps before, after or during the protocol run by the resource under consideration. The distinguisher models all such operations. Standard property-based security notions (e.g. a ciphertext is uncorrelated to a plaintext; or with high probability the message received is the same as the message sent) are covered by such a distinguisher-based notion of security: the ideal system has the required property, and if the real system does not, then a distinguisher will be able to guess with which system it is interacting by verifying whether this property holds.

Definition 1 (**Distinguishing advantage** [27]). A *distinguisher* (figure 3) for two resources $\mathcal{R},\ \mathcal{S}$ is a system $\mathcal{D}$ with two interfaces: an inside interface that connects to all the interfaces of a resource, $\mathcal{R}$ or $\mathcal{S}$, and an outside interface that outputs a single bit: a guess whether it is interacting with $\mathcal{R}$ or $\mathcal{S}$. The advantage of a specific distinguisher $\mathcal{D}$ is then given by

$$d^{\mathcal{D}}(\mathcal{R},\ \mathcal{S}) = |\Pr[\mathcal{D}(\mathcal{R}) = 0] - \Pr[\mathcal{D}(\mathcal{S}) = 0]|,$$

where $\mathcal{D}(\mathcal{R})$ is the output of $\mathcal{D}$ when interacting with $\mathcal{R}$.

The distinguishing advantage for a class of distinguishers $\mathbb{D}$ is defined as

$$d^{\mathbb{D}}(\mathcal{R},\ \mathcal{S}) = \sup_{\mathcal{D}\in\mathbb{D}} d^{\mathcal{D}}(\mathcal{R},\ \mathcal{S}).$$

The distinguishing advantage is a pseudo-metric on the space of resources satisfying the identity, symmetry and triangle inequality properties [27]. If a class of distinguishers $\mathbb{D}$ is such that for every $\mathcal{D} \in \mathbb{D}$, $\mathcal{D}\alpha \in \mathbb{D}$, then the pseudo-metric is non-increasing under application of the converter α, i.e. $d^{\mathbb{D}}(\alpha R,\ \alpha S) \leqslant d^{\mathbb{D}}(R,\ S)$.

Classes of distinguishers. Changing the power of the distinguisher (e.g. with some computational or memory bound, or performing only classical, quantum or non-signalling operations) results in different metrics and different levels of security. For example, if a protocol provides classical computational security, this means that the resource constructed may be perfectly indistinguishable from an ideal resource when considering only computationally bounded distinguishers, but they could be easily distinguished using computationally unbounded (or quantum) distinguishers. This is addressed in more detail in the following.

2.1.2. Cryptographic security

We want to address questions such as 'does a protocol Π construct the ideal resource $\mathcal{S}$ from an initial resource $\mathcal{R}$?' The resource constructed will essentially depend on which players may be honest. For example, in the case of coin flipping, if both parties are honest we expect the protocol to construct a resource that provides each party with a copy of the same uniformly random bit. But if a party is dishonest, this might be a too strong requirement. Instead, we 'only' construct a resource that allows the dishonest party to either abort if she does not like the value of the generated bit, or to bias the bit towards either 0 or 1. [23]

In the case of two party protocols, we want to make a statement about three cases: where both parties are honest, Alice is dishonest, and Bob is dishonest. The resources available to the players are given by a tuple $(R,\ R_A,\ R_B)$, where R denotes the shared resource when both are honest, R_A is available to an honest Bob and dishonest Alice (presumably, providing more functionalities to Alice than R), and R_B is shared between an honest Alice and dishonest Bob. For example, R could be a perfectly fair coin, R_A a coin biased in favour of Alice and R_B a coin that Bob can bias (we will explore this and other examples in section 2.3). Likewise, the constructed resources are also given by such a tuple $(S,\ S_A,\ S_B)$. The reason for considering three distinct resources as above is that dishonest players, by virtue of their dishonesty could, in general gain access to additional controls on their interface.

A two-player protocol $\Pi = (\Pi_A,\ \Pi_B)$ is essentially a pair of converters that can be connected to the interfaces of the shared resources $(R,\ R_A,\ R_B)$. When both are honest, the resulting system is given by $\Pi_A R\ \Pi_B$ which denotes the 'real system' where Alice and Bob share the resource R and implement their protocols Π_A and Π_B at their respective interfaces of R. This should be close to indistinguishable from the ideal resource S.

When Alice is dishonest, the protocol Π_A is removed in the corresponding real system, because we do not know what protocol a dishonest player would follow. On the 'real' side we now have $R_A\Pi_B$. On the ideal side, we have S_A, but in most cases $R_A\Pi_B$ and S_A are trivially distinguishable since Alice's interface of $R_A\Pi_B$ is generally very different from her interface of S_A: S_A provides an idealized interface, which, in the case of coin flipping, might allow Alice to abort. In the real system, $R_A\Pi_B$ Alice receives messages from Bob, and could provoke an abort by sending invalid messages or not responding.

To allow for the comparison and define security against dishonest Alice, we require the existence of a converter (or *simulator*) σ_A which when connected to Alice's interface of S_A makes these two systems close to indistinguishable. Note that connecting this simulator σ_A only makes Alice weaker, since any operation performed by the simulator could equivalently be performed by an adversary connected directly to the interface

of the ideal resource. Further, the simulator's behaviour is independent of the internal workings of the ideal functionality S_A. Security in the case of a dishonest Bob is defined similarly.

Definition 2 (**Cryptographic security** [27]). A protocol $\Pi = (\Pi_A, \Pi_B)$ constructs $\mathcal{S} = (S, S_A, S_B)$ from $\mathcal{R} = (R, R_A, R_B)$ within a distance ϵ, with respect to a set $\mathbb{D}$ of distinguishers and a set $\mathbb{S} \ni \Pi_A, \Pi_B$ of converters, if the following conditions hold:

$$\begin{aligned} &d^{\mathbb{D}}(\Pi_A R \Pi_B, S) \leqslant \varepsilon, \\ &\exists\, \sigma_A \in \mathbb{S}, \quad d^{\mathbb{D}}(R_A \Pi_B, \sigma_A S_A) \leqslant \varepsilon, \\ &\exists\, \sigma_B \in \mathbb{S}, \quad d^{\mathbb{D}}(\Pi_A R_B, S_B \sigma_B) \leqslant \varepsilon. \end{aligned}$$

We sometimes write $\mathcal{R} \overset{\Pi}{\rightarrow} \mathcal{S}$ to denote such constructions. These conditions are illustrated in figure 4.

A *possibility result* for a construction $\mathcal{R} \overset{\Pi}{\rightarrow} \mathcal{S}$ with parameters $(\varepsilon, \mathbb{S}, \mathbb{D})$ is a statement of the form: there exists a protocol $\Pi = (\Pi_A, \Pi_B)$ that ε-constructs $\mathcal{S}$ from $\mathcal{R}$, i.e.

$$\exists\ \Pi_A, \Pi_B, \sigma_A, \sigma_B \in \mathbb{S}, \quad \forall\ \mathcal{D} \in \mathbb{D}, \quad d^{\mathcal{D}}(\Pi_A R \Pi_B, S) \leqslant \varepsilon, \tag{1}$$

$$d^{\mathcal{D}}(R_A \Pi_B, \sigma_A S_A) \leqslant \varepsilon, \tag{2}$$

$$d^{\mathcal{D}}(\Pi_A R_B, S_B \sigma_B) \leqslant \varepsilon. \tag{3}$$

We then say that $\mathcal{R}$ is *stronger* than $\mathcal{S}$. An *impossibility result* with the same parameters has the form: there exists no protocol $\Pi = (\Pi_A, \Pi_B)$ that ε-constructs $\mathcal{S}$ from $\mathcal{R}$,

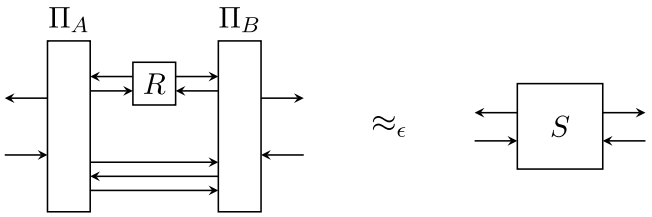
$$\forall\ \Pi_A, \Pi_B, \sigma_A, \sigma_B \in \mathbb{S}, \quad \exists\ \mathcal{D} \in \mathbb{D}, \quad \text{either condition (1), (2), or (3) does not hold.}$$

The strength of a security proof depends on the range of the class $\mathbb{S}$ of simulators and protocols, the class $\mathbb{D}$ of distinguishers used in the security definition, as well as the assumed and constructed resources $\mathcal{R}$ and $\mathcal{S}$. For construction results, a strong statement has the form 'we can easily construct $\mathcal{S}$ from $\mathcal{R}$, and we can easily simulate any cheating behaviour, such that even a very powerful distinguisher could not tell apart our construction from the ideal system.' Therefore, ideally we would want $\mathbb{S}$ to be restricted to converters that are easy to implement physically, and we want the set of distinguishers $\mathbb{D}$ to be as general as possible. For impossibility results, a strong statement has the form 'we can always easily distinguish any system constructed from $\mathcal{R}$ from the resource $\mathcal{S}$, even if we allow for very powerful protocols and simulators.' Therefore, we try to make $\mathbb{S}$ to be as general as possible, and we restrict $\mathbb{D}$ to correspond to efficient or otherwise easy to implement distinguishers[13].

We do not specify what $\mathbb{S}$ and $\mathbb{D}$ should be used in definition 2, since this will be different for different theorems. For example, when we prove that no protocol can construct a biased coin flipping resource in theorem 4, the proof holds for converters $\Pi_A, \Pi_B, \sigma_A, \sigma_B \in \mathbb{S}$ that have unbounded memory, unbounded computational power, and are post-quantum—they are only restricted to be non-signalling. The distinguisher $\mathcal{D}$ that is used to distinguish the real from ideal system runs these converters internally, and thus has the same computational and memory requirements as these converters.

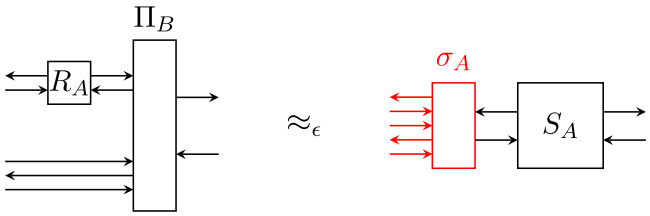
Remark 1 (**Capturing bounded systems**). Note that when a statement we want to prove involves an existence quantifier (over the set of converters $\mathbb{S}$ for a possibility result, and over the set of distinguishers $\mathbb{D}$ for an impossibility proof), it is not necessary to define the entire set $(\mathbb{S}, \mathbb{D})$, it is sufficient to convince oneself that the corresponding system does belong in this set. We use this to prove impossibility results for computationally bounded adversaries as well as in the bounded and noisy storage models in section 3 without defining either the complexity of the systems or the bound on the storage. We achieve this by finding a distinguisher that can distinguish real from ideal systems, and does so by internally running instances of these systems. This means that security already breaks down when the rest of the world (captured by the distinguisher $\mathcal{D}$) has the same memory bounds as the honest players and simulator in the protocol. Since a model needs the distinguisher to have at least the same power as the players and simulator for a protocol to be composable with itself, our impossibility results holds for any such model, regardless of the exact bounds on the computational power or storage, and irrespective of how this is defined.

[13] In some settings, we may want to give more power to one of the players. This is the case for blind computation results [28–30], where for example Bob represents a client with limited computational power and Alice a powerful server (which may for example perform arbitrary quantum operations). In other examples, we may want to restrict honest players to use efficient protocols, while allowing the simulators of dishonest behaviour to be arbitrary. In these and other cases, we can adjust the sets for $\Pi_A, \Pi_B, \sigma_A, \sigma_B$ and $\mathcal{D}$ to suit the scenario. For the results in this paper, this will not be necessary.



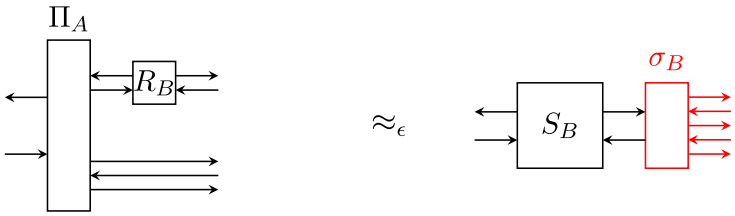
$$d^{\mathbb{D}}(\Pi_A\, R\, \Pi_B, S) \leq \varepsilon$$

(a)



$$\exists\, \sigma_A \in \mathbb{S}, \quad d^{\mathbb{D}}(R_A\, \Pi_B, \sigma_A\, S_A) \leq \varepsilon$$

(b)



$$\exists\, \sigma_B \in \mathbb{S}, \quad d^{\mathbb{D}}(\Pi_A\, R_B, S_B\, \sigma_B) \leq \varepsilon$$

(c)

Figure 4. (a) When both parties are honest, the composition of Alice's and Bob's protocol with their shared resource must be ε-indistinguishable from the constructed resource S. (b) When Alice is dishonest and Bob is honest, the resulting real system obtained by removing Alice's honest protocol must be ε-simulatable by connecting a converter σ_A (called a *simulator*) to Alice's interface of corresponding ideal system, S_A. (c) When Bob is dishonest and Alice is honest, the resulting real system obtained by removing Bob's honest protocol must be ε-simulatable by connecting a converter σ_B to Bob's interface of the corresponding ideal system, S_B. The three conditions from definition 2.

2.2. Cryptography in relativistic settings: the causal boxes framework [22]

The abstract cryptography framework [4] follows a top-down approach to modelling cryptographic security starting from the highest level of abstraction and proceeding downwards, introducing at each level only the minimum necessary specifications. The composability of abstract systems in the abstract cryptography framework makes it possible to provide a general, composable security definition, which is independent from the models of communication or computation. It can then be instantiated with whatever model is needed—here, Causal Boxes to model relativistic cryptography. In this section we give a brief, informal overview of the Causal Boxes framework. A formal introduction may be found in appendix A.

Causal boxes [22] are a model of information-processing systems which may interact with each other in arbitrary ways, so long as they respect causality (figure 5(a)). In broad lines, a causal box $\hat{\Phi}$ is a system with input and output wires which may carry quantum or classical information. A concrete example is a physical box

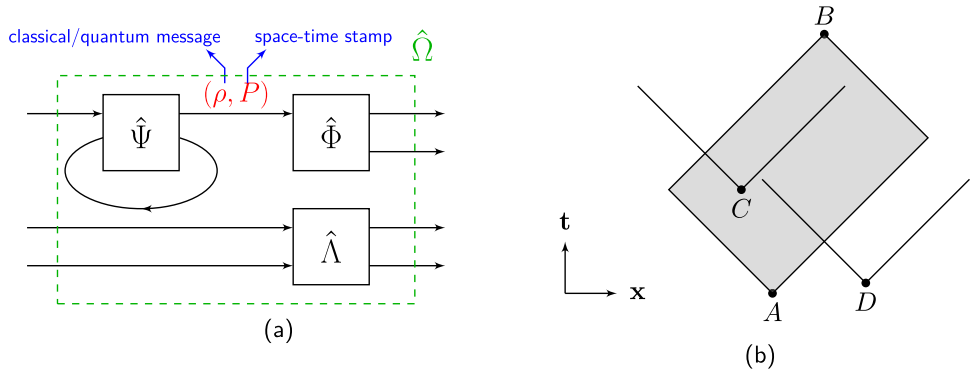


Figure 5. (a) Causal boxes are information-processing systems that respect causality and are closed under composition (serial, parallel or loops). Arbitrary composition of the causal boxes $\hat{\Phi}$, $\hat{\Psi}$ and $\hat{\Lambda}$ is a causal box $\hat{\Omega}$. (b) Minkowski space–time. The causal diamond of the space–time points A and B (shaded in gray) with $A \prec B$ is denoted by $D(A, B)$. In this figure, point $C \in D(A, B)$, and point D is space-like separated from A since the future light cone of neither of the points completely contains the future light cone of the other.

containing some optical elements (like beam-splitters) and connected to optical fiber cables: each wire may carry several messages at different times (or even in a superposition of different times). A single instance of a message is modelled as a quantum state in the joint Hilbert space $\mathcal{H} \otimes l^2(\mathcal{T})$, where $\mathcal{H}$ is the Hilbert space of the actual classical/quantum message, $\mathcal{T}$ is a partially ordered set that defines an ordering on the space of messages and $l^2(\mathcal{T})$ is the sequence space with bounded two-norm[14]. In the simple cases where a quantum state $\rho \in \mathcal{H}$ is sent at a well-defined space–time coordinate $P \in \mathcal{T}$, $\mathcal{T}$ can be taken to be Minkowski space–time and we can simply represent the total state as a pair (ρ, P). In this paper we only need to consider such cases.

Causality condition. Causality requires that outputs produced at space–time point $P \in \mathcal{T}$ can depend only on inputs produced in its causal past, $P' \prec P$ (at this stage, $\mathcal{T}$ could be any set of points equipped with any partial order to represent causality). In general, a causal box is a map from the space of the inputs to the space of the outputs that respects this notion of causality[15]. Composition of causal boxes may be done in series, in parallel or through (feedback) loops (figure 5(a)), and arbitrary composition of causal boxes results in a causal box. A more technical and detailed description of the framework can be found in appendix A.

Minkowski space–time. In this paper we apply the formalism of Causal Boxes to Minkowski space–time $\mathcal{T}$, where each coordinate corresponds to a vector $P = (\mathbf{x}, t)$ with three dimensions of space and one of time. In special relativity, $\mathcal{T}$ has a natural partial order, '$P_1 = (\mathbf{x}_1, t_1) \prec P_2 = (\mathbf{x}_2, t_2)$ if light can reach $\mathbf{x}_2$ from $\mathbf{x}_1$ in time $t_2 - t_1$, that is if $\|\mathbf{x}_2 - \mathbf{x}_1\| \leqslant c(t_2 - t_1)$, where c is the speed of light.' In this case we say that space–time point P_1 is in the causal past of P_2. If two points are not ordered, we say that they are space-like separated. The causal diamond of a pair of space–time points, $P_1 \prec P_2$, denoted by $D(P_1, P_2)$ is the intersection of the future light cone of P_1 with the past light cone of P_2. This represents the maximal space–time region that can be affected by events at P_1 and also affect events at P_2 (figure 5(b)). So that there is no ambiguity in the space–time locations at which various agents are supposed to meet during the protocol, the players must agree upon a coordinate system to represent all space–time points. The players are allowed to have different proper frames to describe their own operations. Security does however not depend on this choice of reference, but only on the partial order between the points, which is invariant under a Lorenz transformation.

Remark 2 (Range of causal boxes). Causal Boxes can model not only quantum processes, but also non-signalling systems with quantum and classical inputs (for example, PR-boxes are causal boxes) [22]. This will be useful in security proofs, for example to cover very powerful adversaries, so let us denote by $\mathbb{C}$ the set of all allowed causal boxes in $\mathcal{T}$, and by $\mathbb{D}_{\mathbb{C}} \subset \mathbb{C}$ the subset of systems that are valid distinguishers.

When proving the possibility result in section 3.1 (theorem 3), we show that

$$\exists\, \Pi,\ \sigma \in \mathbb{S}, \quad \forall\ \mathcal{D} \in \mathbb{D}_{\mathbb{C}}, \quad d^{\mathcal{D}}(\Pi\, R,\ S\, \sigma) \leqslant \varepsilon,$$

where $\mathbb{S}$ are just efficient classical systems. This means that even distinguishers bounded only by non-signalling constraints cannot distinguish the real from ideal systems, and the construction still holds in the presence of such unrestricted adversaries.

[14] This is the state space of a single input/output message. More generally, wires which can carry messages in a superposition of different numbers and time orderings can be represented by the symmetric Fock space of this message space [22]. The symmetry comes from the fact that there is no special ordering of the messages other than the space–time ordering, which is already given in the state description itself. See appendix A for further details.

[15] Technically, this implies that there must necessarily be a finite time gap between an input to a causal box and an output that depends on this input modelling the fact that any causal information processing task takes a strictly non-zero amount of time.

When proving impossibility results in sections 3.2 and 3.3, we show that

$$\forall\, \Pi,\ \sigma \in \mathbb{S}, \quad \exists\ \mathcal{D} \in \mathbb{D}_{\mathbb{S}}, \quad d^{\mathcal{D}}(\Pi\, R,\ S\, \sigma) > \varepsilon,$$

where $\mathbb{S} \subset \mathbb{C}$ is any set of systems (e.g. classical, computationally limited or with bounded memory) and $\mathbb{D}_{\mathbb{S}}$ is a set of distinguishers with similar requirements. This means firstly that our impossibility results hold even if we consider protocols that are bounded only by non-signalling constraints (the case were $\mathbb{S} = \mathbb{C}$). And secondly, if we consider a setting where adversaries are limited, then the results carry over to this setting. For example, our impossibility proofs also hold in the bounded storage model (where $\mathbb{S}$ and $\mathbb{D}_{\mathbb{S}}$ have bounded memory) or a computational setting (where $\mathbb{S}$ and $\mathbb{D}_{\mathbb{S}}$ are computationally limited). See also remark 1 in section 2.1.

2.3. Two-party resources

We may now define the resources needed to model and prove our results. In this section, we model these resources by defining their output values and space–time positions given input values and space–time positions. As in illustration of how this is a special case of the more complete Causal Box model instantiated with Minkowski space, we provide in appendix A.5 a formal definition of a $\mathcal{CD}$ as a causal box.

2.3.1. Coin flipping ($\mathcal{CF}$)

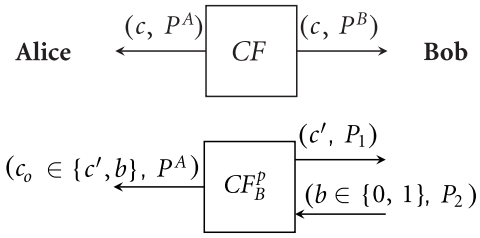
A coin flip resource provides two distrustful players with a random coin flip—if they both behave honestly. If one of them is dishonest, then the literature defines different resources that could be constructed. The most common, e.g. [12], is to allow the coin flip to be *unfair*: a dishonest player who does not like the outcome can abort before the honest player gets to see this outcome. In [23], the authors define a *biased* coin flip, where instead of aborting, a dishonest party can bias the outcome. In this section we follow [23] and define a p-biased coin flip $\mathcal{CF}^p$. We define an unfair coin flip $\mathcal{CF}^{\text{uf}}$ in appendix C.1, where we prove that $\mathcal{CF}^{1/2}$ can be constructed from $\mathcal{CF}^{\text{uf}}$.

Definition 3 (Coin flipping, $\mathcal{CF}^p$). A p-biased coin flip, $\mathcal{CF}^p = \{CF,\ CF_A^p,\ CF_B^p\}$, is defined as follows.

CF: Alice receives a uniformly random bit c at space–time location P^A, and Bob receives the same bit at another location P^B.

CF_B^p: Dishonest Bob receives his uniformly random coin flip output, c' before Alice at $P_1 \prec P^A$ and at $P_2 \succ P_1$ he may input a bit b (which may depend on the value of c'). Alice receives a bit c_o^A at location $P^A \succ P_2$: with probability p she receives $c_o^A = b$, else $c_o^A = c'$. Causality requirement: $P_1 \prec P_2 \prec P^A$.

CF_A^p: analogous to CF_B^p, with the roles reversed.



Note that by definition of CF, it should be clear that the uniformly random bit, c is generated independently by the resource CF and cannot be correlated with anything outside it because the honest resource CF takes no inputs that could possibly influence this output. This is the reason why we label the outputs of CF at P^B and that of CF_B^p at P_1 differently (c and c' respectively) even though they are both uniformly distributed, they are generated independently by different coin flip resources[16]. Further, a bias of 0 means that the coin flip is uniform, a bias of 1 means that the dishonest player has complete control over the outcome, and a bias of p means that any outcome can occur with probability at most $1/2 + p/2$.

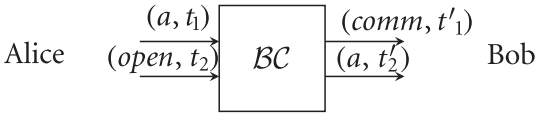
2.3.2. Bit commitment ($\mathcal{BC}$)

As mentioned in the introduction, bit commitment is an important cryptographic primitive and its security relates to its *hiding* and *binding* properties which were also introduced in section 1. Here, we formally define what an ideal bit commitment resource behaves like in Minkowski space–time.

[16] In order to reduce the number of variables in the proofs, we may drop this distinction in places where it is inconsequential. Nevertheless, it is to be kept in mind.

Definition 4 (Bit commitment, $\mathcal{BC}$). A bit commitment resource tuple $\mathcal{BC} := \{BC, BC_A, BC_B\}$ is defined by the single resource BC (with BC_A and BC_B identical to BC), which behaves as follows.

1. Alice selects a classical bit $a \in \{0, 1\}$ to commit to and inputs it at her interface of BC at a time of her choice t_1.
2. Bob receives the message '*comm*' at time $t_1' > t_1$ at his interface, indicating that Alice has committed to a bit.
3. Alice then inputs the command '*open*' at her interface at a time of her choice t_2.
4. Her original commitment 'a' is then revealed to Bob at time $t_2' > t_2$.



For simplicity, we only mention the times at which the messages are input and output in definition 4. This should naturally also include the location in space of the players. We chose this formalization of the $\mathcal{BC}$ resource as it is the closest to the standard, non-relativistic references, e.g. from Blum's and Demay *et al*'s works [12, 23]; we only added the space–time stamps. Nevertheless, our proofs go through even in the cases mentioned by the reviewer, such as when Alice chooses the commitment time and Bob gets the commit message, when Bob can infer Alice's commitment, or when agree on all the time stamps beforehand.

In relativistic protocols (like Kent's [7]), the commit message may be absent, and the commitments may be valid only within a time window (depending on the time taken by light to travel between multiple agents) and thus, relativistic bit commitment looks more like a channel with delay, which we formalize in the next section.

2.3.3. Channel with delay ($\mathcal{CD}$)

In special relativity, unless two agents meet at the exact same space–time location to exchange messages, there is necessarily a finite communication delay between them. A *channel with delay* is a cryptographic primitive between two parties based on this physical intuition: Alice sends a message and Bob receives it unaltered with some delay.

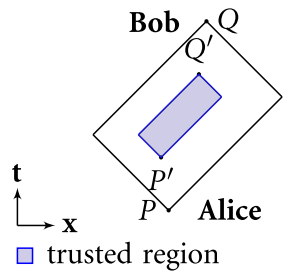
Definition 5 (Channel with delay). A channel with delay $\mathcal{CD} = (CD, CD_A, CD_B)$ between a sender Alice and a receiver Bob is a tuple of resources characterized by four space–time locations, $P \prec P' \prec Q' \prec Q$, and defined as follows.

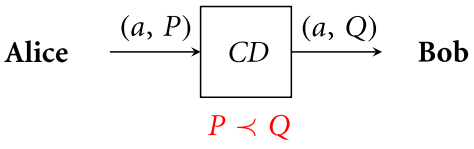
CD: honest Alice inputs a quantum state a into the channel at location P, i.e. the input message is (a, P). Honest Bob receives (a, Q) at location Q.

CD_A: dishonest Alice inputs (a, P'). Honest Bob receives (a, Q).

CD_B: honest Alice inputs (a, P). Dishonest Bob receives (a, Q').

The *trusted region* of the channel is defined as the causal diamond of P' and Q': the set $D(P', Q') := \{S: P' \prec S \prec Q'\}$.





The dishonest resources CD_A and CD_B are the same except with P replaced by $P' \succ P$ in the former and Q replaced by $Q' \prec Q$ in the latter case.

That is, the $\mathcal{CD}$ acts as an identity channel on the message, and as a shift on the space–time stamp. Furthermore, it allows dishonest players to send (respectively, receive) the message after (respectively, before) the honest player. A formal definition of the causal box that implements the $\mathcal{CD}$ can be found in appendix A.5. The trusted region of the $\mathcal{CD}$ is the region where both players can be sure that the information in the channel remains secure, even when the other is dishonest; as we will see, it is the region where the $\mathcal{CD}$ can be used to construct other resources such as $\mathcal{CF}$ (section 3.1).

Relation to relativistic bit commitment protocols. Typically, in a non-relativistic bit commitment resource, Alice is free to choose when to open her commitment and also has the choice to not open her commitment at all. In relativistic protocols, however, the commitment time is usually restricted by the time taken by light to travel between the remote agents, in which case Alice does not have the freedom of choosing arbitrary t_1 and t_2 as in definition 4: once t_1 is fixed, the commitment must be opened at the latest by $t_1 + \Delta t$ for some Δt which depends on the protocol. Bob typically does not know whether Alice is committed before time $t_1 + \Delta t$. If the opening is successful, then Bob knows that Alice ran the honest protocol at t_1, and retroactively decide that she has been committed to her bit. Furthermore, in some relativistic protocols, e.g. [7], Alice cannot choose to not open: if she honestly committed at time t_1, then after Δt, the commitment is always opened. The $\mathcal{CD}$ resource from definition 5 captures exactly this, and hence we analyze the (im)possibility of extending the delay of such a channel in this work.

Other protocols, e.g. [9], additionally offer the possibility to Alice of aborting before Bob receives the bit to which she committed. We thus define a variation of definition 5 in appendix C.2, where after inputting her message into the channel, Alice may still change her mind and abort before Bob receives it. We prove in appendix C.2 that our main results presented in section 3 still go through with this alternative definition of a channel with delay.

3. Results

3.1. Constructing $\mathcal{CF}$

It was shown in [23] that a 1/2-biased coin flipping resource can be perfectly constructed from a bit commitment resource (definition 4), by using Blum's protocol [12]. Here we show that it is in fact possible to construct an even stronger resource (an unbiased coin flip) from a channel with delay.

Theorem 3 (**Construction** $\mathcal{CD} \rightarrow \mathcal{CF}$). *Given a classical channel with delay $\mathcal{CD}$, there exists a classical protocol $\Pi_{\mathcal{CD}\rightarrow\mathcal{CF}} = \{\Pi_A, \Pi_B\}$ that perfectly constructs an unbiased coin flipping resource $\mathcal{CF}$*[0].

The constructed and ideal resources are indistinguishable for any possible distinguisher (including quantum and non-signalling distinguishers, see remark 2 in section 2.2). The honest protocol as well as the simulator require only elementary local operations and classical communication.

The protocol is described in definition 6, and the security proof is given in appendix B.1.

Definition 6 (**Protocol** $\Pi_{\mathcal{CD}\rightarrow\mathcal{CF}}$). Given a channel with delay $\mathcal{CD} = (\mathrm{CD}, \mathrm{CD}_A, \mathrm{CD}_B)$ characterized by locations $A \prec A' \prec B' \prec B$ (see definition 5), we define the following honest protocol $\Pi_{\mathcal{CD}\rightarrow\mathcal{CF}} = (\Pi_A, \Pi_B)$.

1. Alice picks a uniformly random bit, a and sends it through CD from her space–time location A. Bob receives this bit from CD at his location B.
2. Bob meets Alice at S in the trusted region, i.e. the causal diamond $D(A', B')$ to pass on Bob's uniformly random bit, b.
3. After receiving b from her agent, Alice computes $a \oplus b = c$ and outputs this value at some point $P^A \succ S$. If Bob did not turn up for the meeting at S, she picks a uniform b herself, and outputs $a \oplus b = c$ as before.
4. After receiving a from the channel, Bob computes $a \oplus b = c$ and outputs the result at a point $P^B \succ B$. If Bob does not receiving anything from the channel, he picks a uniform a himself, and outputs $a \oplus b = c$ as before.

In this case, if both players are honest (and in particular their inputs a and b are uniformly random), then their output $c = a \oplus b$ is also perfectly random and the protocol succeeds. If one of the players (say Alice) is dishonest, we only care about whether Bob's output is uniformly random; but since Bob is honest, b is uniformly random, and so is c (independently of a).

Note that it is important that the point S in the above protocol lies in the trusted region, otherwise the protocol would not be secure[17]. Furthermore, this protocol can be run by a single player on each side without the need for trusted agents since S lies in the causal future of A and A' and in the causal past of B and B'.

[17] The existence of the simulators σ_A and σ_B used in the proof of theorem 3 relies crucially on $S \in D(A', B')$.

In appendix C.2 we define a weaker channel with delay, namely one which allows Alice to abort and prevent her message from reaching Bob, $\mathcal{CD}^{\perp}$. We show in the same appendix (lemma 11), that if the protocol above is used with $\mathcal{CD}^{\perp}$ instead of $\mathcal{CD}$, then we construct an unfair coin flip $\mathcal{CF}^{\text{uf}}$ instead of an unbiased one $\mathcal{CF}^{0}$.

3.2. Impossibility of $\mathcal{CF}$, $\mathcal{CD}$ and $\mathcal{BC}$

Impossibility of coin flipping. In the previous section, we showed that an unbiased coin flipping resource can be constructed from a suitable channel with delay. Here we show that in the absence of any such shared resource, it is impossible to construct any (biased) coin flip resource solely through the exchange of messages.

Theorem 4 (Impossibility of $\mathcal{CF}$). *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.*

The distinguisher required to distinguish the real from ideal systems has the same complexity and memory requirements as the protocol Π_A, Π_B and simulators σ_A, σ_B. In particular, if these are efficient, classical or have bounded or noisy memory, then so does the distinguisher.

Note that this theorem includes as special case protocols that may send messages in superpositions of different causal orders. This follows from the fact that the impossibility holds for any causal boxes, thus in particular for causal boxes that use such superpositions of causal orders.

The proof of theorem 4 can be found in appendix B.2. Here below we provide some intuition.

A coin flip $\mathcal{CF}^{p}$ does not only guarantee that the output bit is uniform (or biased with probability p), but also that it is independent of any other bit produced in parallel by some other resource (up to the bias). This is essential so that a dispute that is resolved with a coin flip would not only be settled fairly, but also independently from any other dispute. The man in the middle attack mentioned in section 1 would allow dishonest players to perfectly correlate the outcome of two coin flips that are expected to be independent: if Alice and Bob run a coin flipping protocol, Charlie and Danielle run a second one in parallel, and Bob and Charlie collude to forward all the communication between Alice and Danielle, Bob and Charlie could force them to agree on the same coin flip. The proof of theorem 4 consists in showing that this is essentially possible for any protocol that does not use any resource other than communication between the parties involved. A sketch of the main proof idea is provided in figure B2 in appendix B.2. It generalizes the techniques used in [4] to prove the analogous result for the non-relativistic case. Note that even though we define the p-biased coin flip resource symmetrically in definition 3 (i.e. both dishonest players have the same bias), all our results can be easily generalised to the asymmetric case and we will not consider this explicitly.

Impossibility of $\mathcal{BC}$ and $\mathcal{CD}$. Combined with theorem 3 and Blum's construction [12, 23], theorem 4 implies impossibility of constructing any channel with delay $\mathcal{CD}$ or any commitment $\mathcal{BC}$ if no initial resource is shared by the players.

Corollary 5 (Impossibility of $\mathcal{CD}$). *It is impossible to construct $\mathcal{CD}$, with $\epsilon < \frac{1}{6}$, between two mutually distrusting parties solely through the exchange of messages through any classical, quantum or relativistic protocol.*

The distinguisher required to distinguish the real from ideal systems has the same complexity and memory requirements as the distinguisher used in theorem 4 composed with the protocol Π_A, Π_B used in theorem 3. In particular, if these are efficient, classical and have bounded or noisy memory, then so does the distinguisher.

Proof. Follows directly from the impossibility of $\mathcal{CF}$ in theorem 4 together with the construction of unbiased $\mathcal{CF}$ from $\mathcal{CD}$ (theorem 3). □

Corollary 6 (Impossibility of $\mathcal{BC}$). *It is impossible to construct $\mathcal{BC}$, with $\epsilon < \frac{1}{12}$, between two mutually distrusting parties solely through the exchange of messages through any classical, quantum or relativistic protocol. This rules out both arbitrarily long and timed commitments.*

The distinguisher required to distinguish the real from ideal systems has the same complexity and memory requirements as the distinguisher used in theorem 4 composed with the protocol Π_A, Π_B used in Blum's protocol [12, 23]. In particular, if these are efficient, classical and have bounded or noisy memory, then so does the distinguisher.

Proof. Follows directly from the impossibility of $\mathcal{CF}$ in theorem 4 together with the construction of $\frac{1}{2}$-biased $\mathcal{CF}$ from $\mathcal{BC}$ using Blum's protocol [12, 23]. □

Using the same techniques, we show in appendix C.2 that an abort channel cannot be constructed either.

3.3. Impossibility of extending delays

One may wonder whether, in relativistic settings, players could extend the time commitment of a message. For example, if Alice and Bob moved further apart, perhaps this could increase the delay of a channel. However, while *honest, collaborative agents* can always increase the time taken by a message to travel between them by simply moving apart, in a cryptographic setting where agents don't trust each other, they cannot be sure that, for example, Alice is moving farther and not closer to Bob.

What our next result shows is precisely that there is no way for mutually distrustful agents to ensure that the time duration within which the message in a channel is inaccessible to *dishonest players* can increase. This notion is captured by the trusted region of the channel, and is essential for cryptographic security. Moreover, we show that it is not possible to use several channels with delay to construct a better channel with delay. We find that given n shared channels with delay between Alice and Bob, the trusted region of the constructed channel will be smaller than the trusted region of at least one of the individual channels used. In fact, the result is even stronger: the trusted region of the constructed channel is contained inside the trusted regionof at least one of the assumed channels used in the construction. This means the maximal space–time region within which the information in the channel is guaranteed to be secure from both dishonest parties cannot be increased even with n copies of a channel. If we view such a channel with delay as a relativistic bit commitment (Alice inputs a bit into the channel and is then committed to it, but the commitment is only opened when the bit arrives with a delay at Bob), this implies that it is not possible to increase the time within which the commitment is both hiding and binding even if n timed commitment resources are given.

Theorem 7 (**Impossibility of extending** $\mathcal{CD}$). *Given* n *channels with delay* $\mathcal{CD}^1, \ldots, \mathcal{CD}^n$ *between two parties, it is impossible to construct with* $\epsilon \leqslant \frac{1}{8}$ *a channel* $\mathcal{CD}'$ *between the two parties with a trusted region that is larger than the trusted region of all of the individual channels used.*

This holds for all protocols Π_A, Π_B *in* $\mathbb{C}$*, which includes inefficient and non-signalling systems. The distinguisher needed to distinguish the real from ideal system has the same complexity requirements as the protocol* Π_A, Π_B*. In particular, if it is efficient or classical, then so is the distinguisher. Furthermore, if the channels constructed and used are classical, then the distinguisher also has the same quantum memory requirements as the protocol* Π_A, Π_B.

The proof of theorem 7 is given in appendix B.3. Note that this proof includes as special case protocols and distinguishers that may send messages in a superposition of going through one channel $\mathcal{CD}^i$ or another $\mathcal{CD}^j$, or in which a channel may be in a superposition of being used and not used. This follows from the fact that the impossibility holds for any causal boxes, thus in particular for causal boxes that use such superpositions of causal orders.

One may consider variations of this result in which slightly different resources are used or constructed. For example, one could wonder whether having channels with delay going from Bob to Alice may help. It is however easy to verify from that proof, that these have no impact on the impossibility. Another variation worth considering is if the channels are abort channels, as defined in appendix C.2. We prove in the same appendix that one cannot extend the delay of abort channels either.

4. Discussion

The general framework for modelling composable security of relativistic quantum protocols developed here naturally lends itself to the study of novel possibility and impossibility results in relativistic cryptography and could provide key insights into classifying possible and impossible information-processing tasks.

Composability issues raised previously. Composability issues with Kent's 2012 protocol [7] have been briefly discussed in [8]. A definition which is labeled 'composable' is proposed in [8, appendix B], but it is not derived using any composable framework. In fact, it is argued in [8] that bit commitment in the bounded and noisy storage models could satisfy this definition. Since our results carry over to these settings as well, it follows that either the proposed definition is not composable or it cannot be satisfied. Note that the impossibility of $\mathcal{BC}$ in the bounded storage model is already hinted at in [20], where the author points out that the model he developed for concurrent composition does not guarantee that a protocol is secure when run in parallel with another instance of itself.

Superpositions of causal orders. A unique feature of the causal boxes formalism [22], is that it can model superpositions of messages exchanged in a superposition of orders in (space-)time (e.g. the quantum switch [31]) by assigning different space–time stamps (or superpositions thereof) to different messages. Combining this with the abstract cryptography framework [4], as done in this paper, allows us to model security in settings where such superpositions are actively used. For example, this allows us to consider protocols where a message is in a superposition of being sent from Alice to Bob and from Alice to Charlie, i.e. where Bob and Charlie are in a

superposition of having received no message and one message from Alice. Even for protocols that do not use such structures, possibility results consider distinguishers that have this capability. And impossibility results show that even such superpositions of causal orders, the desired resource cannot be constructed. This is the case for all our results presented in this work.

A known example of a process involving a superposition of temporal orders of operations is the quantum switch [31]. It was physically realized in [32, 33], and can be represented in the Causal Box framework as shown in [22]. Further, the quantum switch was shown to have an operational advantage over fixed ordering of (or classical mixtures thereof) operations in solving certain computational tasks [34, 35]. By modelling cryptographic protocols involving such superpositions of orders, one can study the operational advantage provided by quantum ordering of messages/operations over classical orderings. Such an approach to studying causal structures in terms of their operational advantages would be useful for characterising the properties of physically implementable causal structures. This is still an important open question since there exist more general frameworks for modelling causal structures, such as the *process matrix framework* [36] which predict causal structures that are logically possible and yet, have no known physical implementation.

Error tolerance. Realistic protocols, like those implemented with quantum preparations and measurements, always come with a small probability of error (for example, in Kent's protocol as in QKD schemes, this depends on the number of quantum states exchanged between the parties). The ideal resources we prove cannot be constructed are, by definition, not subject to any errors. But it follows directly from the composable framework used that impossibility to construct perfect resources (with some error ε) implies impossibility to construct noisy versions of the resources. To see this, consider a resource $\mathcal{CD}^{\varepsilon}$ that is ε-close to $\mathcal{CD}$ according to the distinguishing advantage. By the triangle inequality, if a real protocol implements a resource that is Δ-distinguishable from the ideal $\mathcal{CD}$, it will be at least $(\Delta - \varepsilon)$-distinguishable from $\mathcal{CD}^{\varepsilon}$. For example, for an unbiased $\mathcal{CF}$, we have $\Delta = \frac{1}{6}$, so it is still impossible to perfectly build any $\mathcal{CF}$ that has an error tolerance smaller than that.

Minimal resources for constructions. Our results show that existing bit commitment protocols [7, 9] cannot construct the target resource $\mathcal{BC}$ from an assumption of a shared resource. Nevertheless, we may still look for initial resources $\mathcal{R}$ that allow $\mathcal{BC}$ to be constructed. It would be interesting to explore the minimal resources necessary to achieve this. For example, an assumption (or assurance) that dishonest players cannot interact with third parties is a good candidate for such an initial resource $\mathcal{R}$. It remains open to formalize such a resource $\mathcal{R}$ within the framework and prove that it is sufficient to construct $\mathcal{BC}$. We note however that in the classical case one can construct $\mathcal{BC}$ assuming a CRS shared between all parties and standard complexity assumptions [16]. Thus, to justify a quantum or relativistic protocol, one would need weaker assumptions.

Alternative space–time. We have proved our results taking the background physical theory to be special relativity (in the sense of Minkowski space–time with a finite speed of signalling). The results would still hold even for other space–time geometries with a *fixed* background causal structure i.e. for different choices of the partially ordered set $\mathcal{T}$. However, if we consider a general relativistic framework (one where the causal order is not fixed until one solves for the metric by considering the mass distribution) that is compatible with quantum mechanics, there could arise situations where the background causal structure itself is subject to quantum uncertainty and is no longer fixed[18]. Such causal structures can no longer be explained by a single partially ordered set $\mathcal{T}$ and cannot be modelled within the Causal Boxes framework. In fact, there is currently no framework that can model this and has the properties required to define cryptographic security[19]. Thus it remains open to define a quantum, general relativistic framework for composable cryptography, and study the problem of constructing bit commitment using it.

Acknowledgments

We thank Renato Renner for discussions on security definitions. VV acknowledges support from FQXi for the funding to present this work at Oxford Quantum Networks 2017, the ETH Masters Scholarship (VV) from ETH Zurich, Switzerland, the Inlaks Scholarship from Inlaks Shivdasani Foundation, Mumbai, India for funding tuition and living expenses during her Masters and the funding from the Department of Mathematics, University of York towards her ongoing PhD. CP acknowledges support from the Zurich Information Security and Privacy Center. LdR acknowledges support from the Swiss National Science Foundation through SNSF

[18] This can arise when large masses are superposed, resulting in the space–time geometry and hence the causal structure being in a superposition [37].

[19] While Process Matrices [36] and Causaloids [38] are examples of frameworks that are capable of modeling such causal structures, they do not provide a model of discrete systems that can be composed, which is needed for cryptography.

project No. 200020_165843 and through the National Centre of Competence in Research *Quantum Science and Technology* (QSIT), and from the FQXi grant *Physics of the observer*.

Author contributions

All authors contributed equally to the ideas in this work, and to revisions of the manuscript. VV wrote the proofs and the first draft of the manuscript.

Competing interests

The authors declare no competing interests.

Appendix A. The causal box framework

The causal box [22] formalism models information-processing systems that are closed under composition even when the order of operations indefinite (such as a superposition of orders) or dynamically determined during a protocol's runtime. Similar formalisms (e.g. [39–41]) have been previously developed but they are only suitable for modelling systems where the order of messages is predefined, they fail to be closed under composition when considering simple cryptographic protocols that involve dynamical ordering of messages during runtime [22]. In particular, the formalism allows us to model quantum causal systems in Minkowski space and construct new causal systems by composing them. This makes it suitable for modelling composable security of relativistic quantum protocols as done in this paper. We now review the formal definitions of the objects of the causal box framework [22].

A.1. Message space and wires

1. *Space of ordered messages:* Every message is modelled as a pair, (v, t) where $v \in \mathcal{V}$ denotes the (classical/quantum) message and $t \in \mathcal{T}$ provides ordering information, where $\mathcal{T}$ is a countable, partially ordered set. The space of a single message is thus a Hilbert space with the orthonormal basis $\{|v, t\rangle\}_{v\in\mathcal{V},t\in\mathcal{T}}$. For a finite $\mathcal{V}$ and infinite $\mathcal{T}$, this Hilbert space corresponds to $\mathbb{C}^{|\mathcal{V}|} \otimes l^2(\mathcal{T})$ where $l^2(\mathcal{T})$ is the sequence space with a bounded two-norm. Thus $|t\rangle$ can be seen as a sequence which consists of a 1 in position $t \in \mathcal{T}$ and 0 everywhere else.

2. *Wires:* The inputs and outputs to a causal box are sent/received through wires which can carry any number (or a superposition of different numbers) of messages of a fixed dimension, which defines the dimension of the wire[20]. Thus the state space of a wire is defined to be a symmetric Fock space. It is modelled as a Fock space to allow for superpositions of different numbers of messages and it is a symmetric Fock space since all ordering information associated with the arriving qudits is already contained in the label $t \in \mathcal{T}$ and given this label, there is no other ordering on the qudits. For the Hilbert space, $\mathcal{H} = \mathbb{C}^d \otimes l^2(\mathcal{T})$, the corresponding bosonic Fock space is given as

$$\mathcal{F}(\mathbb{C}^d \otimes l^2(\mathcal{T})) := \bigoplus_{n=0}^{\infty} \vee^n (\mathbb{C}^d \otimes l^2(\mathcal{T})), \tag{4}$$

   where $\vee^n\mathcal{H}$ denotes the symmetric subspace of $\mathcal{H}^{\otimes n}$ and $\mathcal{H}^{\otimes 0}$ is the one-dimensional space containing the vacuum state $|\Omega\rangle$.

For example, the state space corresponding to a wire A carrying d_A dimensional messages is denoted by $\mathcal{F}_A^{\mathcal{T}} = \mathcal{F}(\mathbb{C}^{d_A} \otimes l^2(\mathcal{T}))$. The joint space of two wires can be written as $\mathcal{F}_A^{\mathcal{T}} \otimes \mathcal{F}_B^{\mathcal{T}} = \mathcal{F}_{AB}^{\mathcal{T}}$ and it can be shown [22] that for any two Hilbert spaces $\mathcal{H}_A = \mathbb{C}^{d_A} \otimes l^2(\mathcal{T})$ and $\mathcal{H}_B = \mathbb{C}^{d_B} \otimes l^2(\mathcal{T})$,

$$F(H_A) \otimes F(H_B) \cong F(H_A \oplus H_B). \tag{5}$$

Isomorphism (5) tells us that each valid state in the combined state space of two wires, one carrying d_A dimensional messages and the other carrying d_B dimensional messages, can be mapped to a valid state in the state

[20] For example a two-dimensional wire can carry any number of qubits, or can be in a superposition of carrying 2 and 3 qubits but cannot carry qutrits.

space of a single wire carrying d_A+d_B dimensional messages. Hence $\mathcal{F}_{AB}^{\mathcal{T}}$, can be interpreted as the state space of a wire carrying $(d_A + d_B)$ dimensional messages[21].

We now proceed to formally review the definition of causality that causal boxes satisfy, we first define the notion of cuts on a partially ordered set $\mathcal{T}$ which forms an important part of the definition.

A.2. Cuts and causality

Definition 7 (Cuts [22]). A cut of a partially ordered set $\mathcal{T}$ is any subset $\mathcal{C} \subseteq \mathcal{T}$ such that $\mathcal{C} = \bigcup_{t\in\mathcal{C}} \mathcal{T}^{\leqslant t}$, where $\mathcal{T} \leqslant t = \{p \in \mathcal{T}: p \leqslant t\}$. A cut $\mathcal{C}$ is *bounded* if there exists a point $t \in \mathcal{T}$ such that $\mathcal{C} \subseteq \mathcal{T}^{\leqslant t}$. The set of all cuts of $\mathcal{T}$ is denoted as $\mathfrak{C}(\mathcal{T})$ and the set of all bounded cuts as $\overline{\mathfrak{C}}(\mathcal{T})$.

In this paper, we have taken the partially order set $\mathcal{T}$ to be Minkowski space–time, this allows us to restrict to bounded cuts. This is because every cut in Minkowski space–time is a bounded cuts: any two space–time points (even those that are unordered i.e. space-like separated) necessarily share a common causal future. Note that this is not true for a general partially ordered set $\mathcal{T}$.

Definition 8 (Causality function [22]). A function χ: $\mathfrak{C}(\mathcal{T}) \rightarrow \mathfrak{C}(\mathcal{T})$ is a *causality function* if it satisfies the following conditions:

$$\forall \mathcal{C}, \mathcal{D} \in \mathfrak{C}(\mathcal{T}), \quad \chi(\mathcal{C} \bigcup \mathcal{D}) = \chi(\mathcal{C}) \bigcup \chi(\mathcal{D}), \tag{6a}$$

$$\forall \mathcal{C}, \mathcal{D} \in \mathfrak{C}(\mathcal{T}), \quad \mathcal{C} \subseteq \mathcal{D} \Rightarrow \chi(\mathcal{C}) \subseteq \chi(\mathcal{D}), \tag{6b}$$

$$\forall \mathcal{C} \in \overline{\mathfrak{C}}(\mathcal{T})\backslash\{\varnothing\}, \quad \chi(\mathcal{C}) \subset \mathcal{C}, \tag{6c}$$

$$\forall \mathcal{C} \in \overline{\mathfrak{C}}(\mathcal{T}), \forall t \in \mathcal{C}, \exists n \in \mathbb{N}, \quad t \notin \chi^n(\mathcal{C}), \tag{6d}$$

where χ^n denotes n compositions of χ with itself, $\chi^n = \chi \circ \cdots \circ \chi$.

Conditions (6*a*) and (6*b*) follow from the considerations that: If the output on $\mathcal{C}$ and $\mathcal{D}$ can be computed from $\chi(\mathcal{C})$ and $\chi(\mathcal{D})$ respectively, the output on $\mathcal{C} \cup \mathcal{D}$ can be computed from $\chi(\mathcal{C}) \cup \chi(\mathcal{D})$, if $\chi(\mathcal{C})$ is needed to compute the output on $\mathcal{C}$, then certainly it is needed to compute the output on $\mathcal{D} \supseteq \mathcal{C}$. Condition (6*c*) is essentially the causal condition that requires that outputs of a causal box can depend only on inputs produced in its causal past and Condition (6*d*) is to ensure that a causal box does not produce an infinite number of messages in a finite interval of time (see [22] for details). Definition 8 is the general definition of the causality function and it simplifies for special choices of the set $\mathcal{T}$ [22]. We are now in a position to review the formal definition of a causal box.

A.3. General definition of a causal box

Definition 9 (Causal box [22]). A (d_X, d_Y)-causal box Φ is a system with input wire X and output wire Y of dimension d_X and d_Y[22], defined by a set[23] of mutually consistent (equation (8)), completely positive, trace-preserving (CPTP) maps (equation (7))

$$\Phi = \{\Phi^C: \mathfrak{T}(F_X^{\chi(C)}) \rightarrow \mathfrak{T}(F_Y^C)\}_{C\in\overline{\mathfrak{C}}(T)}. \tag{7}$$

These maps much be such that for all $\mathcal{C}, \mathcal{D} \in \overline{\mathfrak{C}}(\mathcal{T})$ with $\mathcal{C} \subseteq \mathcal{D}$,

$$\mathrm{tr}_{\mathcal{D}\backslash\mathcal{C}} \circ \Phi^{\mathcal{D}} = \Phi^{\mathcal{C}} \circ \mathrm{tr}_{\mathcal{T}\backslash\chi(\mathcal{C})}, \tag{8}$$

where $\mathfrak{T}(\mathcal{F})$ denotes the set of all trace class operators on the space $\mathcal{F}$ and the causality function $\chi(.)$ satisfies all the conditions of definition 8. $\mathcal{F}^{\mathcal{C}}$ is the subspace of $\mathcal{F}^{\mathcal{T}}$ that contains only messages in positions $t \in \mathcal{C} \subseteq T$ and $\mathrm{tr}_{\mathcal{D}\backslash\mathcal{C}}$ traces out the messages occurring at positions in $\mathcal{D}\backslash\mathcal{C}$.

Equation (8) can be seen as the combination of the two requirements $\Phi^{\mathcal{C}} = \mathrm{tr}_{\mathcal{D}\backslash\mathcal{C}} \circ \Phi^{\mathcal{D}}$ and $\Phi^{\mathcal{C}} = \Phi^{\mathcal{C}} \circ \mathrm{tr}_{\mathcal{T}\backslash\chi(\mathcal{C})}$. The first one embodies the mutual consistency requirement while the second, that of causality.

[21] Conversely, any wire A of messages of dimension d_A can be split in two sub-wires A_1 and A_2 of messages of dimensions $d_{A_1} + d_{A_2} = d_A$: $\mathcal{F}_A^{\mathcal{T}} \cong \mathcal{F}_{A_1}^{\mathcal{T}} \otimes \mathcal{F}_{A_2}^{\mathcal{T}}$. Further, for any subset $\mathcal{P} \subseteq \mathcal{T}$, $\mathcal{F}_A^{\mathcal{T}} \cong \mathcal{F}_A^{\mathcal{P}} \otimes \mathcal{F}_A^{\widetilde{\mathcal{P}}}$, where $\widetilde{\mathcal{P}} = \mathcal{T}\backslash\mathcal{P}$ and $\mathcal{F}_A^{\mathcal{P}} = \mathbb{C}^{d_A} \otimes l^2(\mathcal{P})$.

[22] It is enough to define a causal box as a map from one input wire to one output wire since a single wire of dimension d can always be decomposed into n wires of dimensions $d_1, \ldots, d_n$ with $d = d_1 + d_2 + \ldots + d_n$ using the isomorphism of equation(5).

[23] In general, it is modelled as a set of maps and not a single map because this allows systems to be included which produce an unbounded number of messages and are thus not well-defined as a single map on the entire set $\mathcal{T}$, but only on subsets of $\mathcal{T}$ that are upper bounded by a set of unordered points. For example [22].

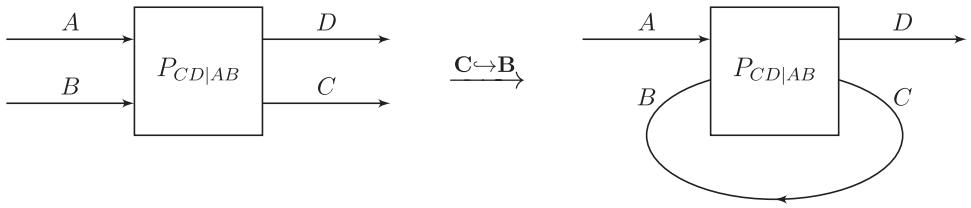


Figure A1. Classical example for loop composition: a system with classical inputs A, B and classical outputs C, D can be described by the probability distribution $P_{CD|AB}$. The new system obtained by adding a loop from the output C to input B is then described by the distribution $Q_{D|A} = \sum_c P_{CD|AB}(cd|ac)$ and is a valid probability distribution as long as the system obeys causality [22].

Remark 8. Note that definition 9 only considers trace-preserving causal boxes. The definition can be easily generalised to non-trace preserving causal boxes or *sub-normalised causal boxes* to account for post-selection. This is done in [22] by defining a suitable projector on the space of *normalised causal boxes*.

Further, just like CPTP maps on quantum states, causal boxes also admit Choi-Jamiołkowski and Stinespring representations, and in addition, they also admit sequence representations that describe their sequential action over subsequent, disjoint sets of $\mathcal{T}$. We refer the reader to the original paper [22] for details regarding these as they are not of particular relevance to the results of this paper.

A.4. Composition of causal boxes

Having defined causal boxes, we are in a position to see how they can be composed. Due to Isomorphism (5), an input/output wire to a causal box of dimension d can be split into sub-wires of dimensions d_1, d_2, …, d_n such that $d_1 + d_2 + ... + d_n = d$ and similarly, wires can also be combined to form a wire with dimensions equal to the sum of the dimensions of the individual wires. Taking *Ports*(Φ) to represent a particular partition of the input and output wires of a causal box Φ into sub-wires, arbitrary composition of causal boxes can be achieved by combining the following two steps.

1. *Parallel composition:* two causal boxes Φ and Ψ can be composed in parallel to obtain a new causal box $\Gamma = \Phi \| \Psi$ whose input and output ports are given by the union of the input and output ports of Φ and Ψ respectively.
2. *Loops:* selected output ports of the causal box Γ can be connected with input ports of the same dimension to form loops.

A classical example of composition through loops can be found in figure A1. The formal definitions of parallel composition and loop composition of causal boxes, which generalise thisintuition to the quantum case can be found in the original paper [22], where it is also shown that causal boxes are closed under these arbitrary composition operations.

A.5. The channel with delay as a causal box

The channel with delay was defined in section 2.3.3. In this section, we show how to model the channel with delay using the causal box formalism, i.e. by defining it in terms of a set of mutually consistent maps $\{\Phi^{\mathcal{C}}\}$. Recall that a channel with delay is defined by the tuple of resources $\mathcal{CD} := \{CD, CD_A, CD_B\}$, each of the resources CD, CD_A and CD_B can be equivalently described by the causal boxes Φ_{CD}, Φ_{CD_A} and Φ_{CD_B}. In the following, we consider the channel with delay resource characterised by the 4 space–time points $A \prec A' \prec B' \prec B$.

Definition 10 (Causal box Φ_{CD} description of the channel with delay resource CD). $\forall$ bounded cuts $\mathcal{C} \ni B \subseteq \mathcal{T}$ in Minkowski space $\mathcal{T}$, the causal box $\Phi_{CD} = \{\Phi^{\mathcal{C}}_{CD} \colon \mathfrak{T}(\mathcal{F}_X^{\chi(\mathcal{C})}) \to \mathfrak{T}(\mathcal{F}_Y^{\mathcal{C}})\}_{\mathcal{C}\in\overline{\mathfrak{C}}(\mathcal{T})}$ is defined by the maps $\Phi^{\mathcal{C}}_{CD} := \mathcal{I}_{A\to B} \circ \mathrm{tr}_{\chi(\mathcal{C})\setminus A}$, with $\mathcal{I}_{A\to B} = \mathcal{I}_{\mathcal{V}} \otimes [|B\rangle\langle A| + |A\rangle\langle B|]_{l^2(\mathcal{T})}$. X and Y label the input and output wires to the causal box, $\mathcal{I}_{\mathcal{V}}$ denotes the identity operation on the Hilbert space $\mathcal{V}$ of the quantum message, $l^2(\mathcal{T})$ is the sequence space (with bounded two-norm) of the space–time stamps and $\chi(\mathcal{C})$ is any causality function that satisfies the conditions of definition 8 and the condition that $B \in \mathcal{C} \Rightarrow A \in \chi(\mathcal{C})$.

Similarly, the resources CD_A and CD_B can be defined by replacing A with A' and B with B' in definition 10 respectively. Note that for any subset $\mathcal{P} \subseteq \mathcal{T}$, $\mathcal{F}^{\mathcal{T}} \cong \mathcal{F}^{\mathcal{P}} \otimes \mathcal{F}^{\tilde{\mathcal{P}}}$, where $\tilde{\mathcal{P}} = \mathcal{T}\setminus\mathcal{P}$. Further, a natural embedding of $\mathcal{F}^{\mathcal{P}}$ in $\mathcal{F}^{\mathcal{T}}$ can be obtained [22] by appending the vacuum state[24] to $\mathcal{F}^{\mathcal{P}}$

[24] $|\Omega\rangle^{\tilde{\mathcal{P}}}$ represents the one dimensional subspace of $\mathcal{F}^{\tilde{\mathcal{P}}}$ that contains the vacuum state.

$$\mathcal{F}^{\mathcal{P}} \cong \mathcal{F}^{\mathcal{T}} \otimes |\Omega\rangle^{\tilde{\mathcal{P}}} \subseteq \mathcal{F}^{\mathcal{T}}$$

This allows us to equivalently view the trace $\mathrm{tr}_{\mathcal{D}\setminus\mathcal{C}}$ for any two cuts $\mathcal{C} \subseteq \mathcal{D}$, as the operation of tracing out all the messages in space–time locations that belong to the cut $\mathcal{D}$, but not to the cut $\mathcal{C}$ and replacing all of them by the vacuum state $|\Omega\rangle$. With this, we can see that in definition 10, $\mathrm{tr}_{\chi(\mathcal{C})\setminus A}(\rho)$ for an arbitrary input state $\rho \in \mathfrak{T}(\mathcal{F}_X^{\chi(\mathcal{C})})$ will always result in a state of the form $\sigma \otimes |A\rangle\langle A| \otimes |\Omega\rangle\langle\Omega|^{\tilde{A}}$ where $\sigma \in \mathcal{F}(\mathcal{V})$, which without loss of generality, we denote by $\sigma \otimes |A\rangle\langle A|$ where it is understood that there is 'nothing' i.e. the vacuum state $|\Omega\rangle$ at all other space–time locations $\tilde{A} \in \mathcal{T}$.

It is easy to verify that Φ_{CD} is indeed a causal box i.e. that it satisfies equation (8). The left-hand side of the equation gives, for an arbitrary input state $\rho \in \mathfrak{T}(\mathcal{F}_X^{\chi(C)})$ and any cut $\mathcal{D} \ni B \supseteq \mathcal{C}$

$$\begin{aligned}\Phi^C_{CD}(\rho) &= \mathrm{tr}_{D\setminus C}\circ\Phi^D_{CD}(\rho) = \mathrm{tr}_{D\setminus C}\circ I_{A\to B}\circ\mathrm{tr}_{\chi(D)\setminus A}(\rho)\\ &= \begin{cases}\mathrm{tr}_{D\setminus C}(\sigma\otimes|B\rangle\langle B|), & A\in\chi(D)\\ |\Omega\rangle\langle\Omega|^T, & \text{otherwise}\end{cases}\\ &= \begin{cases}\sigma\otimes|B\rangle\langle B|, & B\in C\\ |\Omega\rangle\langle\Omega|^T, & \text{otherwise.}\end{cases}\end{aligned} \tag{9}$$

Similarly, the right-hand side of equation (8) becomes

$$\begin{aligned}\Phi^C_{CD}(\rho) &= \Phi^C_{CD}\circ\mathrm{tr}_{C\setminus\chi(C)}(\rho) = I_{A\to B}\circ\mathrm{tr}_{\chi(C)\setminus A}\circ\mathrm{tr}_{C\setminus\chi(C)}(\rho)\\ &= \begin{cases}\sigma\otimes|B\rangle\langle B|, & A\in\chi(C)\\ |\Omega\rangle\langle\Omega|^T, & \text{otherwise.}\end{cases}\end{aligned} \tag{10}$$

Since we have[25] $B \in \mathcal{C} \Leftrightarrow A \in \chi(\mathcal{C})$ by definition 10, and equations (9) and (10) hold for arbitrary input state ρ, the expressions in equations (9) and (10) are equal giving $\mathrm{tr}_{\mathcal{D}\setminus\mathcal{C}}\circ\Phi^{\mathcal{D}}_{CD} = \Phi^{\mathcal{C}}_{CD}\circ\mathrm{tr}_{\mathcal{C}\setminus\chi(\mathcal{C})}$ as required by definition 9 of a causal box. This shows that Φ_{CD} of definition 10 (and similarly Φ_{CD_A} and Φ_{CD_B}) is indeed a causal box.

Remark 9. Note that definition 10 and the fact that Φ_{CD} is a causal box imply that Φ_{CD} cannot produce any (non-vacuum) output on cuts that do not contain the point B. This is due to the fact that in Minkowski space, for any cut $\mathcal{C}$ with $B \notin \mathcal{C}$, we can find a cut $\mathcal{D} \supset \mathcal{C}$ containing B. The mutual consistency condition (equation (8)) would then demand that no non-vacuum outputs are produced in the cut $\mathcal{C}$ as the only non-vacuum output in $\mathcal{D}$ will be produced at $B \notin \mathcal{C}$. Thus it is enough to define Φ_{CD} only on cuts that include B as done in definition 10.

Appendix B. Proofs of all results

B.1. Constructing $\mathcal{CF}$

Theorem 3 (Construction $\mathcal{CD} \to \mathcal{CF}$). *Given a classical channel with delay $\mathcal{CD}$, there exists a classical protocol $\Pi_{\mathcal{CD}\to\mathcal{CF}} = \{\Pi_A, \Pi_B\}$ that perfectly constructs an unbiased coin flipping resource $\mathcal{CF}^0$.*

The constructed and ideal resources are indistinguishable for any possible distinguisher (including quantum and non-signalling distinguishers, see remark 2 in section 2.2). The honest protocol as well as the simulator require only elementary local operations and classical communication.

Proof. The protocol $\Pi_{\mathcal{CD}\to\mathcal{CF}}$ (definition 6) constructs $\mathcal{CF}^0$ from $\mathcal{CD}$ iff all three conditions of figure B1 are satisfied. The condition of figure B1(a) trivially holds. To see that the conditions in figures B1(b) and (c) also hold, consider the following simulators.

σ_A is defined as follows.

1. Receive the input a at the space–time location A' at the outer interface. If no a is received, pick one uniformly at random.
2. On receiving input c at P_2 at the inner interface, output $b = a \oplus c$ at the outer interface at S.

[25] Note that the implication $B \in \mathcal{C} \Rightarrow A \in \chi(\mathcal{C})$ follows from the definition of the causality function while the implication $A \in \chi(\mathcal{C}) \Rightarrow B \in \mathcal{C}$ follows from the fact that for any $\chi(\mathcal{C}) \ni A$, the causal box Φ_{CD} when acting on an arbitrary input state ρ, always produces an output on a cut containing B (by definition).

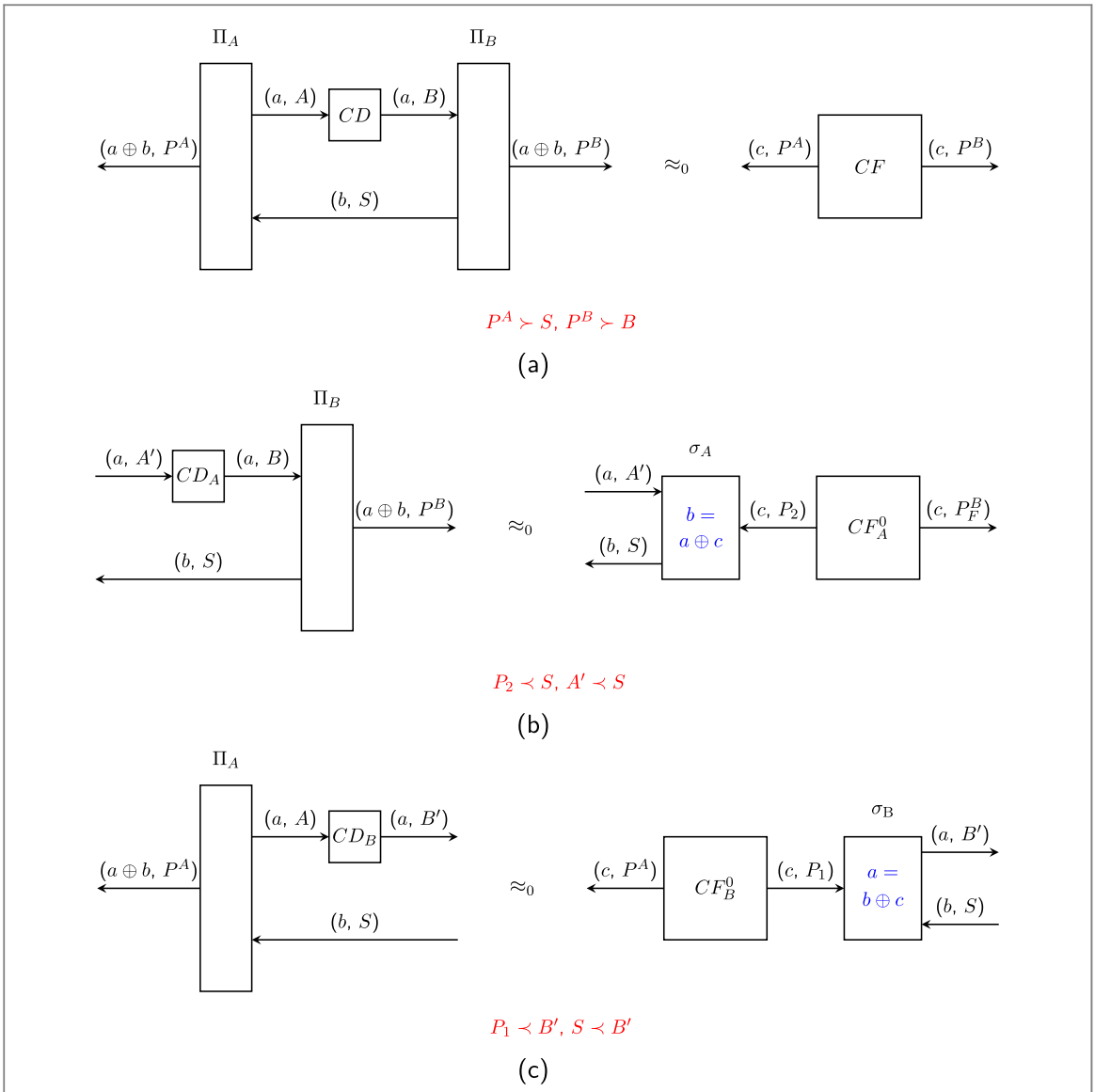


Figure B1. (a) Honest Alice and Bob: $\Pi_A CD \Pi_B \approx_0 CF$ (b) Dishonest Alice: $\exists\, \sigma_A$ such that $CD_A \Pi_B \approx_0 \sigma_A CF_A^0$. (c) Dishonest Bob: $\exists\, \sigma_B$ such that $\Pi_A CD_B \approx_0 CF_B^0 \sigma_B$. Conditions for constructibility of a fair and unbiased coin flip $\mathcal{CF}^0$ from a channel with delay $\mathcal{CD}$. Since the coin flip has $p = 0$ the biasing bit that a dishonest party may input has no effect, so we do not draw it.

For the above construction of σ_A to work, both P_2 and A' must lie in the causal past of S. Since S lies in the trusted region, $A' \prec S$ necessarily holds. Since there are no constraints on the space–time points at which CF_A^0 can produce an output, we can always make it output at a point $P_2 \prec S$.

σ_B is defined as follows.

1. Receive the input b at the space–time location S at the outer interface. If no b is received, pick one uniformly at random.
2. On receiving input c at P_1 at the inner interface, output $a = b \oplus c$ at the outer interface at B'.

For the above construction of σ_B to work, both P_1 and S must lie in the causal past of B'. Again, S being in the trusted regionensures that $S \prec B'$ necessarily holds and $P_1 \prec B'$ holds since there are no restrictions on the space–time points at which CF_B can produce an output.

It is easy to see that for the above mentioned constructions of the simulators σ_A and σ_B, the real and ideal systems of figures B1(a)–(c) are perfectly indistinguishable (for any distinguisher $\mathcal{D}$) since a, b and c always satisfy the condition that any two of them sum bit-wise to the third. Further, Alice can learn the value of both bits a and b before Bob does but she cannot bias the value of Bob's output, $a \oplus b$ in any way. Neither can she prompt Bob to abort the protocol after learning the value of her bit a, because she has to send a into the channel before he receives b at the point S (by the non empty trusted region condition). Hence the protocol perfectly constructs an unbiased coin flipping resource $\mathcal{CF}^0$ from a channel with delay $\mathcal{CD}$. □

B.2. Impossibility of $\mathcal{CF}$

Theorem 4 (Impossibility of $\mathcal{CF}$). *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.*

The distinguisher required to distinguish the real from ideal systems has the same complexity and memory requirements as the protocol Π_A, Π_B and simulators σ_A, σ_B. In particular, if these are efficient, classical or have bounded or noisy memory, then so does the distinguisher.

Proof. For the construction to be valid, all conditions of figure B2 must hold. As explained in the figure caption, the first step is to combine the three conditions and use the triangle inequality to obtain figure B2(d).

Next we will show that for any causal order of the messages c, c', b and b' in figure B2(d), the best possible classical, quantum or non-signalling strategy of σ leads to a distinguishing advantage of at least $\frac{1}{2}(1-p)$ between $CF_B^p \sigma CF_A^p$ and CF. We present here only the optimal strategy—it is a straight-forward if tedious calculation to verify that all other causal orderings and possible input–output correlations in each case do not yield a lower distinguishing advantage.

The simulator's task is to ensure to the best of its capabilities that c_o^A and c_o^B are equal. The causal order of the messages that provide σ with the maximum information to achieve this task is the one depicted by the *directed acyclic graph* (DAG)[26] in figure B3, where σ can learn the values of c and c' first and accordingly correlate the values of b and b' which are then input to CF_A^p and CF_B^p respectively. In this case, the best possible strategy that the simulator could adopt would be one where it produces the input–output correlations $b = b' = c$ or $b = b' = c'$ all the time. The probability that c_o^A equals c_o^B for such a strategy (say, $b = b' = c$) is:

$$\begin{aligned}
P(c_o^A = c_o^B) &= P(c_o^A = c_o^B |\ c = c').P(c = c') + P(c_o^A = c_o^B |\ c \neq c').P(c \neq c') \\
&= \frac{1}{2} + \frac{1}{2}[P(c_o^A = c_o^B |\ c \neq c', \text{ both biased}).P(\text{both biased}) \\
&\quad + P(c_o^A = c_o^B |\ c \neq c', A \text{ biased}).P(A \text{ biased}) \\
&\quad + P(c_o^A = c_o^B |\ c \neq c', B \text{ biased}).P(B \text{ biased}) \\
&\quad + P(c_o^A = c_o^B |\ c \neq c', \text{ none biased}).P(\text{none biased})] \\
&= \frac{1}{2} + \frac{1}{2}[1.p^2 + 0.p(1-p) + 1.p(1-p) + 0.(1-p)^2] \\
&= \frac{1}{2}(1+p).
\end{aligned}$$

A distinguisher connected to $CF_B^p \sigma CF_A^p$ or CF can access the two outputs produced at the outer interfaces of these systems. If the distinguisher guesses $CF_B^p \sigma CF_A^p$ every time the two outputs differ in value and $CF_B^p \sigma CF_A^p$ or CF with uniform probability every time the two outputs are equal, the distinguishing advantage would be:

$$3\epsilon \geqslant d(CF_B^p \sigma CF_A^p, CF) \geqslant P(c_o^A \neq c_o^B) = \frac{1}{2}(1-p). \tag{11}$$

This distinguishing advantage ϵ is equal to zero only when $p = 1$ (totally biased coin) and thus, for a non-trivial p, it is not possible to make the distinguishing advantage ϵ arbitrarily small.

The distinguisher used to distinguish the left and right-hand sides in figure B2(d) is quite a trivial system, that only needs one bit of memory and compare the two output bits. The existence of such a distinguisher with advantage 3ϵ implies that there exists another distinguisher with advantage ε that can distinguish the left and right-hand sides from either figures B2(a)–(c). We now go through the steps of this argument more slowly, to determine the exact complexity (both in terms of memory and computation) of the distinguisher that we have proven to exist. To construct figure B2(d) from the three first conditions in figure B2, we use the following two arguments several times.

The first is the triangle inequality, namely that

$$\left.\begin{array}{l} R \approx_{\varepsilon} S \\ S \approx_{\varepsilon'} T \end{array}\right\} \Longrightarrow R \approx_{\varepsilon+\varepsilon'} T.$$

Note that this holds for individual distinguishers, hence the contrapositive states that if there exists a distinguisher that can distinguish R from T with advantage $\varepsilon + \varepsilon'$, then *exactly the same* distinguisher can distinguish either R from S with advantage ε or S from T with advantage ε'.

[26] DAGs are widely used in the literature to represent causal structures. For classical causal structures (as is the case here, given that the inputs and outputs to σ are classical bits), the nodes (circles) represent random variables and the edges (arrows) represent causal influences.

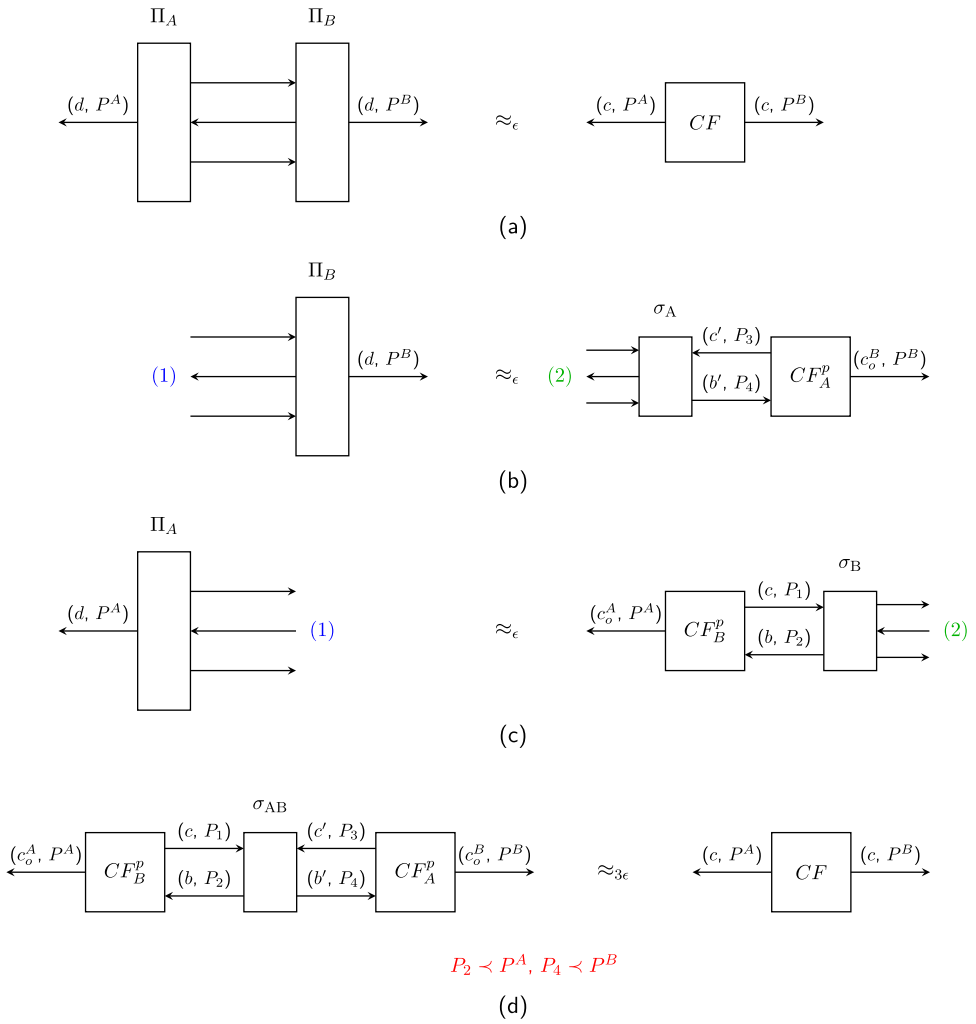


Figure B2. (a) $\Pi_A\Pi_B \approx_\epsilon CF$ (b) Dishonest Alice: $\exists\,\sigma_A$: $\Pi_B \approx_\epsilon \sigma_A CF_A^b$ (c) Dishonest Bob: $\exists\,\sigma_B$: $\Pi_A \approx_\epsilon CF_B^b\sigma_B$ (d) $\exists\,\sigma_{AB}$: $CF_B^b\ \sigma_{AB}\ CF_A^b \approx_{3\epsilon} CF$ Impossibility of coin flipping: proof sketch. For a p-biased Coin Flipping to be ϵ-constructible solely through the exchange of messages, conditions (a)–(c) must be satisfied. The composition (1) of the system on the lhs of (c) (Π_A) with that on the lhs of (b) (Π_B) yields the system on the lhs of (a) ($\Pi_A\Pi_B$) which gives the condition (d) for the corresponding right hand sides (2) with $\sigma_{AB} = \sigma_B\sigma_A$. To prove impossibility, we show in appendix B.2 that for any causal order of the messages c, c', b and b', the best possible classical, quantum or non-signalling strategy of σ leads to a distinguishing advantage of at least $3\epsilon = \frac{1}{2}(1-p)$ between $CF_B^p\sigma CF_A^p$ and CF in (d). Note that if the parties had access to a shared resource $\mathcal{R}$, a condition analogous to (d) could not be obtained by composing (b) and (c), and the same impossibility proof would no longer be applicable.

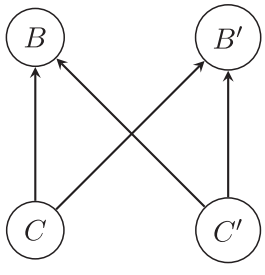


Figure B3. The causal ordering of inputs and outputs of simulator σ (see figure B2(d)) that provide it the maximum information about the outputs c_o and c_o'. C, C', B and B' ($\in\{0,\ 1\}$) represent the random variables of which the corresponding lower case alphabets are specific instances of. In addition, B and B' may causally influence each other, but this does not offer any advantage to σ because the optimal strategy is where both b and b' depend on c (or c').

The second generic argument—contractivity—uses the fact that for any resources R, S and any other system α,

$$R \approx_\varepsilon S \Longrightarrow \alpha R \approx_\varepsilon \alpha S.$$

Unlike the previous argument, this one involves a change of distinguisher, namely if for some $\mathcal{D}$, $d^{\mathcal{D}}(\alpha R,\ \alpha S) > \varepsilon$, then $d^{\mathcal{D}\alpha}(R,\ S) > \varepsilon$, where $\mathcal{D}\alpha$ corresponds to the composition of $\mathcal{D}$ with α.

We now start with the existence of the trivial distinguisher $\mathcal{D}$ for figure B2(d) described above, and which has $d^{\mathcal{D}}(CF_B^p \sigma CF_A^p,\ CF) > 3\epsilon$. From the triangle inequality we know that one of the three following conditions must hold

$$d^{\mathcal{D}}(\Pi_A \Pi_B,\ CF) > \epsilon, \tag{12}$$

$$d^{\mathcal{D}}(\Pi_A \sigma_A CF_A^p,\ \Pi_A \Pi_B) > \epsilon, \tag{13}$$

$$d^{\mathcal{D}}(CF_B^p \sigma_B \sigma_A CF_A^p,\ \Pi_A \sigma_A CF_A^p) > \epsilon. \tag{14}$$

If it is (12) that holds, we are done, since we have a trivial distinguisher that can break the condition from figure B2(a). If it is either (13) or (14), then using the contractivity rule, we find that either $\mathcal{D}\Pi_A$ can distinguish the left and right-hand sides of figure B2(b) or $\sigma_A CF_A^p \mathcal{D}$ can distinguish the left and right-hand sides of figure B2(c).

Thus, both the computational requirements and memory requirements of the distinguisher are the same as the computational and memory requirements of either Π_A or $\sigma_A CF_A^p$. □

The proof of theorem 4 is completely general and applies to quantum and non-signalling protocols as well. The apparent 'classicality' of the proof is due to the fact that all inputs and outputs are classical bits as per the definition of the resources used. However, we only talk about the input–output correlations produced by the simulator σ and not the internal machinery used to produce these correlations, which could be classical, quantum or non-signalling and the impossibility holds for all classical, quantum and non-signalling strategies that σ could adopt to produce these correlations. A particular input–output correlation could be generated through many different strategies but it turns out in this particular case that there exists a simple classical strategy that perfectly produces these correlations (look at the value of c and set $b = b' = c$ all the time), which is why we use correlations produced by σ and strategy adopted by σ quite interchangeably. But one must keep in mind that this in no way restricts the simulator to classical strategies.

B.3. Impossibility of extending delays

Theorem 7 (Impossibility of extending $\mathcal{CD}$). *Given* n *channels with delay $\mathcal{CD}^1, \ldots, \mathcal{CD}^n$ between two parties, it is impossible to construct with $\epsilon \leqslant \frac{1}{8}$ a channel $\mathcal{CD}'$ between the two parties with a trusted region that is larger than the trusted region of all of the individual channels used.*

This holds for all protocols Π_A, Π_B in $\mathbb{C}$, which includes inefficient and non-signalling systems. The distinguisher needed to distinguish the real from ideal system has the same complexity requirements as the protocol Π_A, Π_B. In particular, if it is efficient or classical, then so is the distinguisher. Furthermore, if the channels constructed and used are classical, then the distinguisher also has the same quantum memory requirements as the protocol Π_A, Π_B.

Proof. Let $\mathcal{CD}^1, \ldots, \mathcal{CD}^n$ denote the n given channels with $\mathcal{CD}^i = (CD^i,\ CD_A^i,\ CD_B^i)$ and associated locations $P_i \prec P_i' \prec Q_i' \prec Q_i$. Our goal is to construct a channel $\mathcal{CD}'$, characterized by points $P \prec P' \prec Q' \prec Q$, given those channels and additional (direct) communication taking place in a space–time region R. The conditions given in figure B4 must be satisfied such that ϵ is a small, non-negative number $\forall$ distinguishers $\mathcal{D} \in \mathbb{D}$. In the following we write $CD = CD^1 \| \cdots \| CD^n$ to denote the resource consisting of the parallel composition of the n resources CD^i that are available to Alice and Bob (similarly CD_A and CD_B for dishonest Alice and Bob respectively).

Note that for each channel with delay, there exists a converter δ_A^i such that $\delta_A^i CD_A^i = CD^i$: this is simply a system that takes the input a from Alice at position P_i and outputs it at position P_i'. Let $\delta_A = \delta_A^1 \| \cdots \| \delta_A^n$ denote the parallel composition of these converters such that $\delta_A CD_A = CD$.

From figure B4(c) we have

$$\begin{aligned} CD_A\ \Pi_B \approx_\epsilon \sigma_A\ CD_A^{'} \quad &\Longrightarrow \quad \Pi_A\ \delta_A\ CD_A\ \Pi_B \approx_\epsilon \ \Pi_A\ \delta_A\ \sigma_A CD_A^{'} \\ &\Longleftrightarrow \quad \Pi_A\ CD\ \Pi_B \approx_\epsilon \ \Pi_A\ \delta_A\ \sigma_A\ CD_A^{'}. \end{aligned} \tag{15}$$

If we look at the right-hand side of (15), the joint system $\Pi_A \delta_A \sigma_A$ produces an output at position P', but nothing after. Hence, communication that does not reach σ_A before P' cannot influence the output and is not relevant to the output of $\Pi_A \delta_A \sigma_A$. Let $\perp_A$ denote a converter that blocks all channels $\mathcal{CD}^i$ with $P_i' \not\prec P'$ and also blocks all communication in the region R at points $P_R \not\prec P'$. We then have $\Pi_A \perp_A \delta_A \sigma_A = \Pi_A \delta_A \sigma_A$. Combining this with figure B4(c), (15), and figure B4(a), we get

$$\Pi_A \perp_A \delta_A CD_A \Pi_B \approx_\epsilon \ \Pi_A \perp_A \delta_A \sigma_A CD_A' = \Pi_A \delta_A \sigma_A CD_A' \approx_\epsilon \ \Pi_A CD \Pi_B \approx_\epsilon \ CD',$$

from which we conclude that

$$\Pi_A \perp_A CD \Pi_B \approx_{3\epsilon} \ CD'. \tag{16}$$

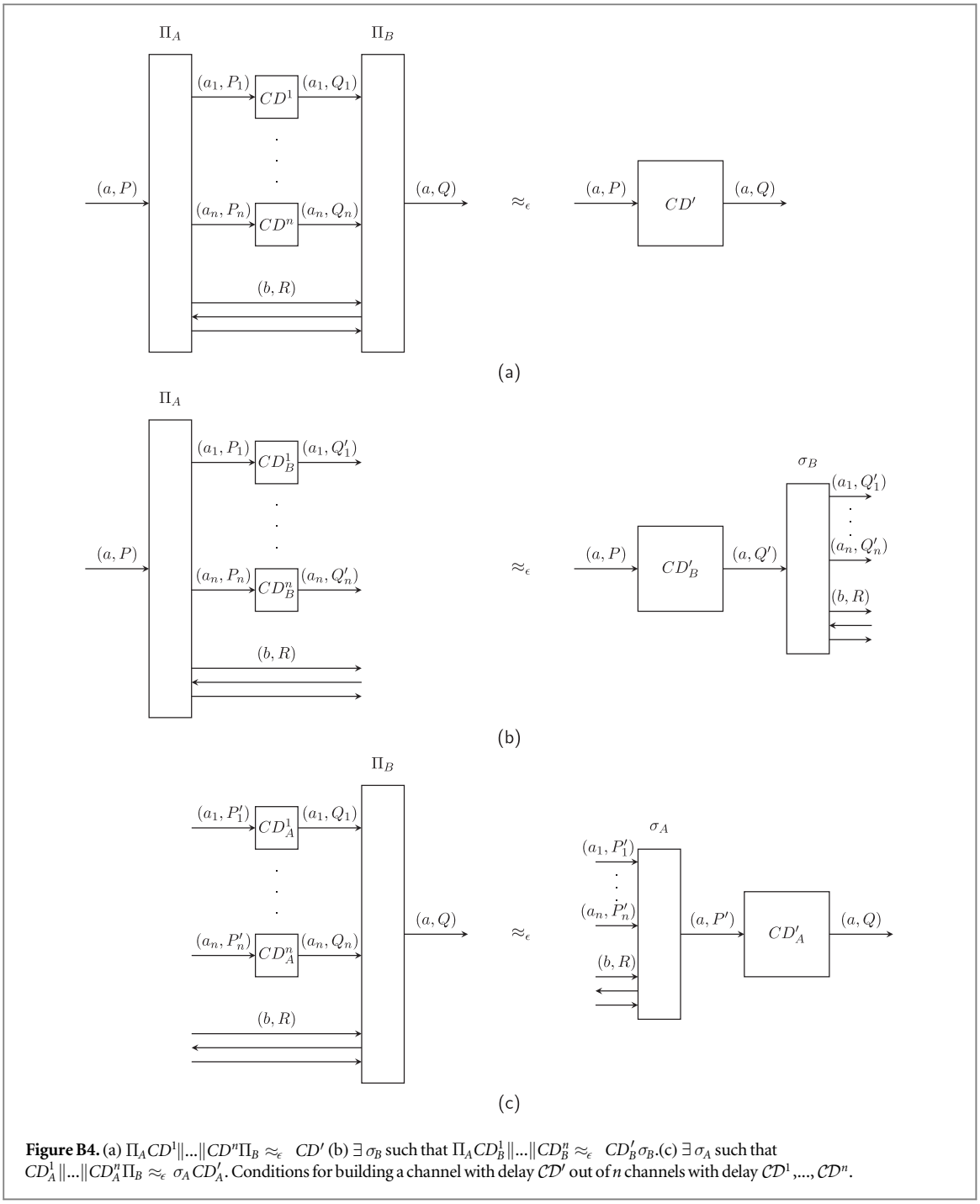


Figure B4. (a) $\Pi_A CD^1 \| ... \| CD^n \Pi_B \approx_\epsilon \; CD'$ (b) $\exists\, \sigma_B$ such that $\Pi_A CD^1_B \| ... \| CD^n_B \approx_\epsilon \; CD'_B \sigma_B$.(c) $\exists\, \sigma_A$ such that $CD^1_A \| ... \| CD^n_A \Pi_B \approx_\epsilon \; \sigma_A CD'_A$. Conditions for building a channel with delay $\mathcal{CD}'$ out of n channels with delay $\mathcal{CD}^1$,..., $\mathcal{CD}^n$.

We now turn our attention to figure B4(b). Similarly to the argument above, we define a converter δ_B such that $CD_B \delta_B = CD$ and a converter $\perp_B$ that blocks exactly the same channels and points as $\perp_A$, but which is plugged into Bob's interface. We then get from figure B4(b) that

$$\Pi_A CD_B \delta_B \perp_B \Pi_B \approx_\epsilon \; CD'_B \sigma_B \delta_B \perp_B \Pi_B. \tag{17}$$

If we look at the left-hand side of (17), we see that $CD_B \delta_B \perp_B = CD \perp_B = \perp_A CD$, hence it follows from (16) and (17) that

$$CD'_B \sigma_B \delta_B \perp_B \Pi_B \approx_{4\epsilon} \; CD'. \tag{18}$$

Equation (18) can only hold with $\epsilon < 1/8$ if information flows from the left interface of $CD_B{}'$ to the right interface of Π_B. Communication between $CD_B{}'$ and σ_B only occurs in position Q', so for the message to make its way through to Π_B, there must also be communication between σ_B and Π_B at some point $P_C \succ Q'$. The region R cannot be used for this, as $P' \prec Q'$ and $\perp_B$ blocks all communication after P'. The only remaining option is for there to exist a channel $\mathcal{CD}^i$ with $Q'_i \succ Q'$ and which is not blocked by $\perp_B$, i.e. $P'_i \prec P'$. But in this case we would have $P'_i \prec P' \prec Q' \prec Q'_i$, i.e. the trusted region of $\mathcal{CD}^i$ would contain the trusted region of $\mathcal{CD}'$.

To finish the proof, we still need to analyze the complexity of the distinguisher used to distinguish the real and ideal systems. The proof assumes that the protocol is secure, and then concludes that (18) must hold, which implies that the trusted region of the constructed channel must be contained in the trusted region of one of the assumedchannels. Taking the contrapositive, we assume that the constructed $\mathcal{CD}'$ has a larger trusted region than the assumed channels, which implies that there exists a distinguisher that can distinguisher the left and right-hand sides of (18), which in turn implies that there exists a distinguisher that can distinguisher the real from ideal in one of the equations from figure B4. We will now go through the arguments of the proof to determine the complexity of this distinguisher that we have proven to exist.

The systems on the left and right-hand sides of (18) just take a message as input and output a message of the same dimension. CD' performs an identity operation on the value of the message, whereas $CD'_B\sigma_B\delta_B\perp_B \Pi_B$ must trace out the input and output some fixed state, since by assumption $\mathcal{CD}'$ has a larger trusted region than the assumed channels, so there is no communication from Alice's interface to Bob's interface. If the channel is classical, an optimal system that distinguishes a fixed (possibly probabilistic) output from the identity channel, inputs a fixed message (that has low probability of being output by the channel on the left-hand side of (18)), and checks to see if the same message is output. This has probability of success at least $1/2$, and requires no memory and one equality check. If the channel is quantum, the distinguisher may perform the same (which then involves preparing one quantum state and performing a projective measurement). Alternatively, the distinguisher may input half of an EPR pair, keep the purification, and perform the projective measurement on the joint system of the output and the purification, which has a probability of success of at least $3/4$, but now involves quantum memory of the size of the message.

There are two generic arguments used in the proof to construct the distinguisher for one of the equations in figure B4 from the distinguisher for (18). The first is the triangle inequality, namely that

$$\left.\begin{array}{l} R \approx_\varepsilon S \\ S \approx_\varepsilon T \end{array}\right\} \Longrightarrow R \approx_{2\varepsilon} T.$$

Note that this holds for individual distinguishers, hence the contrapositive states that if there exists a distinguisher that can distinguish R from T with advantage 2ε, then *exactly the same* distinguisher can distinguish either R from S or S from T with advantage ε.

The second generic argument uses the fact that for any resources $R,\ S$ and any converter α,

$$R \approx_\varepsilon S \Longrightarrow \alpha R \approx_\varepsilon \alpha S.$$

Unlike the previous argument, this one involves a change of distinguisher, namely if for some $\mathcal{D}$, $d^{\mathcal{D}}(\alpha R,\ \alpha S) > \varepsilon$, then $d^{\mathcal{D}\alpha}(R,\ S) > \varepsilon$, where $\mathcal{D}\alpha$ corresponds to the composition of $\mathcal{D}$ with α. This was used several times in the proof with $\alpha = \Pi_A\perp_A \delta_A$, $\alpha = \Pi_A\delta_A$, and $\alpha = \delta_B\perp_B \Pi_B$. Putting this together, we prove that there exists a distinguisher than can distinguish at least one of the pairs of systems from figure B4, and this distinguisher has the same computational requirements as either Π_A or Π_B along with one extra measurement needed to distinguish the left and right-hand sides of (18) (since δ and $\perp$ and forward and trace out messages, respectively, they do not perform any computation). Furthermore, if the channels are classical, then the distinguisher has the same quantum memory requirements as either Π_A or Π_B, since δ and $\perp$ do not require any quantum memory. □

Appendix C. Unfair resources

C.1. Unfair coin flipping

In section 2.3.1, we defined the p-biased coin flipping resource tuple $\mathcal{CF}^p = \{CF,\ CF_A^p,\ CF_B^p\}$. Here we define another variation, the *unfair* coin flipping resource tuple $\mathcal{CF}^{\text{uf}}$ and prove that a $1/2$-biased coin flip resource $\mathcal{CF}^{1/2}$ can be constructed from it. Then, by reduction, theorem 7 implies the impossibility of unfair coin flipping solely through the exchange of messages.

Definition 11 (Unfair coin flipping, $\mathcal{CF}^{\text{uf}}$). An *unfair coin flip* $\mathcal{CF}^{\text{uf}} = (CF,\ CF_A^{\text{uf}},\ CF_B^{\text{uf}})$ has the same resource CF as $\mathcal{CF}^p$, and CF_A^{uf} and CF_B^{uf} are given by:

CF_B^{uf}: Bob receives a uniformly random bit c at location P_1. At location $P_2 \succ P_1$, he can input a bit $b \in \{\perp, \overline{\perp}\}$ that may depend on the value of c received at P_1. Alice then receives message c_o^A at the location $P^A \succ P_2$ depending on Bob's input b at P_2: if $b = \perp$, then $c_o^A = \perp$, else $c_o^A = c$ i.e. dishonest Bob can prompt an abort ($\perp$) on Alice's interface by setting $b = \perp$.

CF_A^{uf}: analogous to CF_B^p, with the roles reversed.

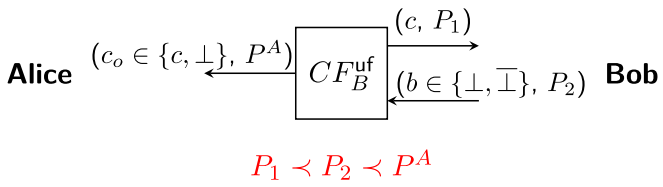


Figure C1. An unfair coin flip resource with honest Alice and dishonest Bob.

This is illustrated in figure C1.

Lemma 10. *There exists a protocol* $\Pi_{\mathcal{CF}^{\text{uf}} \to \mathcal{CF}^{1/2}} = \{\Pi_A', \Pi_B'\}$ *that perfectly constructs a 1/2-biased coin flipping resource* $\mathcal{CF}^{1/2}$ *from an unfair coin flipping resource* $\mathcal{CF}^{\text{uf}}$.

The constructed and ideal resources are indistinguishable for any possible distinguisher (including quantum and non-signalling distinguishers). The honest protocol as well as the simulator require only elementary local operations and classical communication.

Proof. In the following, we will drop the space–time labels corresponding to the messages to avoid unnecessary annotations and it is easy to see that there exist space–time labels for each message involved such that the construction presented below is satisfied. We define the honest protocol $\Pi_{\mathcal{CF}^{\text{uf}} \to \mathcal{CF}^{1/2}} = \{\Pi_A', \Pi_B'\}$ as follows.

1. Receive the coin flip outcome from the corresponding interface of the unfair coin flipping resource $\mathcal{CF}^{\text{uf}}$ at the inner interface.
2. If this outcome has a bit value (say c), output c at the outer interface. If this outcome is an abort ($\perp$), then output $c_u = 0$ or $c_u = 1$ each with probability $p = 1/2$ at the outer interface.

$\Pi_{\mathcal{CF}^{\text{uf}} \to \mathcal{CF}^{1/2}}$ perfectly constructs a $1/2$-biased coin flipping resource for the following simulators (the same for Sim_A and Sim_B).

1. Receive the output bit c' from the biased coin flipping resource on the inner interface and output the same bit at the outer interface.
2. Upon receiving the additional input of $\perp$ or $\overline{\perp}$ at the outer interface, forward $b' = c'$ to the resource at the inner interface if this input is not an abort ($\overline{\perp}$) and forward $b' = \bar{c}' = c' \oplus 1$ to the resource if the input at the outer interface is an abort ($\perp$).

One can easily verify that the real and ideal systems are identical, for convenience, we have drawn this in figure C2. □

C.2. Abort channel

In section 2.3.3, a $\mathcal{CD}$ is defined such that once Alice inputs her message at P (respectively, P', if she is dishonest), Bob is guaranteed to receive it at Q (or Q' if he is dishonest). In this section we consider a version of a channel with delay in which Alice may additionally abort, and prevent Bob from getting her message. We call this an abort channel, and write $\mathcal{CD}^{\perp}$.

Definition 12 (Abort channel, $\mathcal{CD}^{\perp}$). An abort channel $\mathcal{CD}^{\perp} = (CD, CD_A^{\perp}, CD_B)$ between a sender Alice and a receiver Bob is a tuple of resources characterized by five space–time locations, $P \prec P' \prec R \prec Q' \prec Q$. CD and CD_B are defined identically to a standard $\mathcal{CD}$ (definition 5). $CD_A^{\perp}$ is defined as follows.

$CD_A^{\perp}$: Dishonest Alice inputs (a, P'). She may also input $(\perp, R)$. If she input $(\perp, R)$, Bob does not receive anything. Otherwise, Bob receives (a, Q).

Nearly the same protocol as used in theorem 3 can be used to construct an unfair coin flip from an abort channel.

Lemma 11 (Construction $\mathcal{CD}^{\perp} \to \mathcal{CF}^{\text{uf}}$). *Given a classical abort channel* $\mathcal{CD}^{\perp}$, *there exists a classical protocol* $\Pi_{\mathcal{CD}^{\perp} \to CF^{\text{uf}}} = \{\Pi_A, \Pi_B\}$ *that perfectly constructs an unfair coin flipping resource* $\mathcal{CF}^{\text{uf}}$.

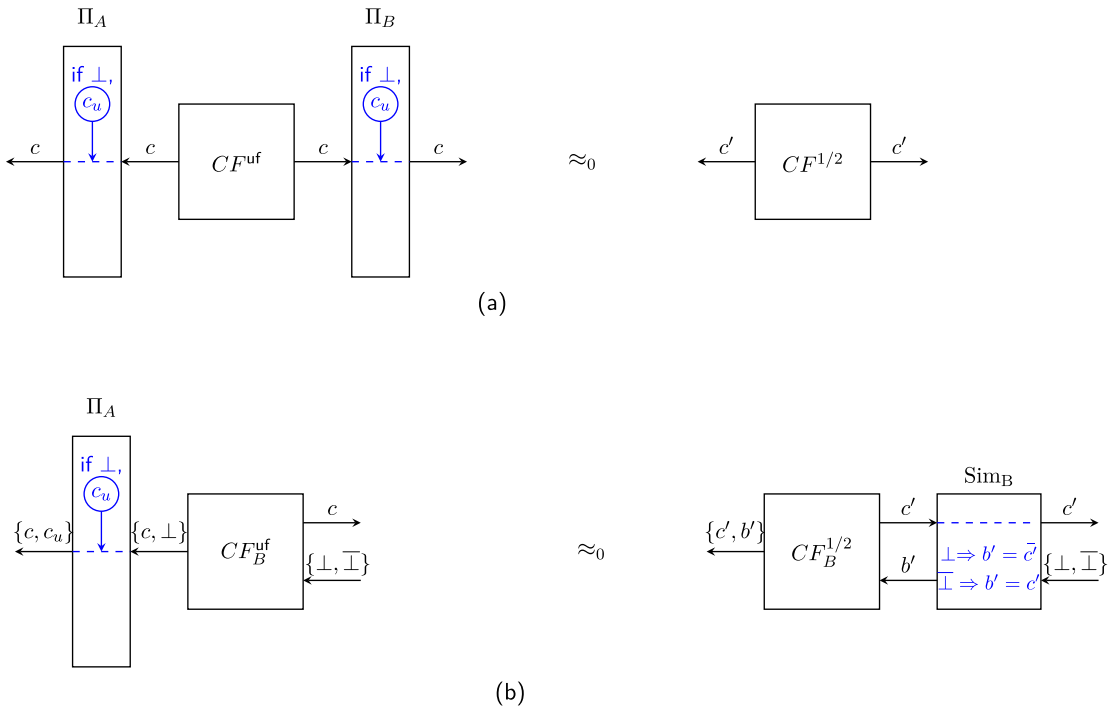


Figure C2. (a) When both parties are honest, the outcomes of the unfair resource CF^{uf} are never equal to $\perp$ and the protocols Π_A and Π_B simply forward the bit c received at the inner interface to their outer interface. This is a perfect construction since the honest resources CF^{uf} and $CF^{1/2}$ are the same. (b) The simulator Sim_B for dishonest Bob simply forwards c' received at its inner interface to its outer interface and sets $b' = c'$ if it receives $\overline{\perp}$ at the outer interface and $b' = \bar{c}'$ otherwise. Now the protocol Π_A may also receive the abort input $\perp$ from the unfair CF resource, in which case it forwards the uniformly random bit c_u which equals either 0 or 1 each with probability $1/2$ and simply forwards the input c from the unfair CF resource otherwise. The construction is perfect because the probability distribution of inputs and outputs from the real system is the same as the input and output probability distribution of the ideal system and hence the two are perfectly indistinguishable. More specifically, whenever a dishonest player does not abort, the outputs at both interfaces will be equal to an independently generated, uniformly random bit (labelled as c for the real system and c' for the ideal system. If the dishonest player aborts, the two outputs will be equal to an independently generated, uniformly random bit (c or c') with a probability of $1/2$ and they will be uniformly random but completely uncorrelated (c_u and c for the real system and b' and c' for the ideal system) with a probability of $1/2$. The argument for dishonest Alice is identical. Constructibility of a $1/2$-biased CF resource from an unfair CF resource.

The constructed and ideal resources are indistinguishable for any possible distinguisher (including quantum and non-signalling distinguishers). The honest protocol as well as the simulator require only elementary local operations and classical communication.

Proof. The protocol is the same as the one used to construct $\mathcal{CF}^0$ from $\mathcal{CD}$, except that if Bob does not receive anything from the channel, he outputs $\perp$ instead of picking a uniform a himself. The simulator σ_A has to be changed in the same way: if it does not receive an input (a, A') or if it recives (a, A'), but later gets an abort $\perp$ (which is now allowed by $\mathcal{CD}^{\perp}$), it notifies the resource $\mathcal{CF}_A^{\perp}$ to abort and output $\perp$ at Bob's interface. Drawing up a figure similar to figure B1, one can see that here too we have perfect security. □

It then follows from theorem 4 that an abort channel cannot be constructed without any setup assumptions either.

Corollary 12 (Impossibility of $\mathcal{CD}^{\perp}$). *It is impossible to construct $\mathcal{CD}^{\perp}$, with $\epsilon < \frac{1}{12}$, between two mutually distrusting parties solely through the exchange of messages through any classical, quantum or relativistic protocol.*

The distinguisher required to distinguish the real form ideal systems has the same complexity and memory requirements as the distinguisher used in theorem 4 composed with the protocols used in lemmas 10 and 11. In particular, if these are efficient, classical and have bounded or noisy memory, then so does the distinguisher.

Proof. Lemma 11 constructs $\mathcal{CF}^{\text{uf}}$ from $\mathcal{CD}^{\perp}$, and lemma 10 constructs $\mathcal{CF}^{1/2}$ from $\mathcal{CF}^{\text{uf}}$. Thus, the impossiblity of constructing $\mathcal{CF}^{p}$ from theorem 4 immediately implies the impossibility of constructing $\mathcal{CD}^{\perp}$. □

Finally, we can show that theorem 7 also holds for abort channels.

Lemma 13 (Impossibility of extending $\mathcal{CD}^{\perp}$). *Given* n *abort channels with delay $\mathcal{CD}_1^{\perp}$, …, $\mathcal{CD}_n^{\perp}$ between two parties, it is impossible to construct with $\epsilon \leqslant \frac{1}{8}$ a channel $\mathcal{CD}'^{\perp}$ between the two parties with a trusted region that is larger than the trusted region of all of the individual channels used.*

This holds for all protocols Π_A, Π_B in $\mathbb{C}$, which includes inefficient and non-signalling systems. The distinguisher needed to distinguish the real from ideal system has the same complexity requirements as the protocol Π_A, Π_B. In particular, if it is efficient or classical, then so is the distinguisher. Furthermore, if the channels constructed and used are classical, then the distinguisher also has the same quantum memory requirements as the protocol Π_A, Π_B.

The proof of lemma 13 is identical to the proof of theorem 7 found in appendix B.3, because the distinguisher used runs the honest protocol Pi_A, Pi_B, and $\mathcal{CD}$ and $\mathcal{CD}^{\perp}$ only differ on the adversarial interface (a dishonest Alice can provoke an abort). So we omit it.

ORCID iDs

Lídia del Rio https://orcid.org/0000-0002-2445-2701

References

[1] Yin J *et al* 2017 Satellite-based entanglement distribution over 1200 kilometers *Science* **356** 1140–4
[2] Ren J-G *et al* 2017 Ground-to-satellite quantum teleportation *Nature* **549** 70
[3] Liao S-K *et al* 2017 Satellite-to-ground quantum key distribution *Nature* **549** 43
[4] Maurer U and Renner R 2011 Abstract cryptography *2nd Symp. Innovations in Computer Science, ICS 2011* ed B Chazelle (Tsinghua: Tsinghua University Press) pp 1–21
[5] Canetti R 2001 Universally composable security: a new paradigm for cryptographic protocols *Proc. 42nd IEEE Symp. on Foundations of Computer Science, FOCS '01* (Piscataway, NJ: IEEE) p 136
[6] Kent A 1999 Unconditionally secure bit commitment *Phys. Rev. Lett.* **83** 1447–50
[7] Kent A 2012 Unconditionally secure bit commitment by transmitting measurement outcomes *Phys. Rev. Lett.* **109** 130501
[8] Kaniewski J, Tomamichel M, Hanggi E and Wehner S 2013 Secure bit commitment from relativistic constraints *IEEE Trans. Inf. Theory* **59** 4687–99
[9] Lunghi T *et al* 2015 Practical relativistic bit commitment *Phys. Rev. Lett.* **115** 030502
[10] Unruh D 2010 Universally composable quantum multi-party computation *Advances in Cryptology—EUROCRYPT 2010* (*Lecture Notes in Computer Science* vol 6110) (Berlin: Springer) pp 486–505
[11] Kashefi E and Pappa A 2017 Multiparty delegated quantum computing *Cryptography* **1** 12
[12] Blum M 1983 Coin flipping by telephone a protocol for solving impossible problems *ACM SIGACT News* **15** 23–7
[13] Kilian J 1988 Founding crytpography on oblivious transfer *Proc. 20th annual ACM Symp. on Theory of Computing—STOC '88* (New York: ACM) pp 20–31
[14] Hallgren S, Smith A and Song F 2011 Classical cryptographic protocols in a quantum world *Int. J. Quantum Inf.* **13** 1550028
[15] Kaniewski J 2015 Relativistic quantum cryptography *PhD Thesis* National University of Singapore
[16] Canetti R and Fischlin M 2001 Universally composable commitments *Advances in Cryptology—CRYPTO 2001: 21st Annual Int. Cryptology Conf. Proc. (Santa Barbara, CA, 19–23, August 2001)* (Berlin: Springer) pp 19–40
[17] Mayers D 1997 Unconditionally secure quantum bit commitment is impossible *Phys. Rev. Lett.* **78** 3414–7
[18] Lo H-K and Chau H F 1997 Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78** 3410–3
[19] Lo H-K and Chau H 1998 Why quantum bit commitment and ideal quantum coin tossing are impossible *Physica* D **120** 177–87
[20] Unruh D 2011 Concurrent composition in the bounded quantum storage model *Advances in Cryptology—EUROCRYPT 2011* (*Lecture Notes in Computer Science*) (Berlin: Springer) pp 467–86
[21] Unruh D 2013 Everlasting multi-party computation *Advances in Cryptology—CRYPTO 2013* ed R Canetti and J A Garay (Berlin: Springer) pp 380–97
[22] Portmann C, Matt C, Maurer U, Renner R and Tackmann B 2017 Causal boxes: quantum information-processing systems closed under composition *IEEE Trans. Inf. Theory* **63** 1
[23] Demay G and Maurer U 2013 Unfair coin tossing *2013 IEEE Int. Symp. on Information Theory* (Piscataway, NJ: IEEE) pp 1556–60
[24] Chailloux A and Kerenidis I 2013 Optimal quantum strong coin flipping *Proc. 54th Symp. on Foundations of Computer Science, FOCS '13* (Piscataway, NJ: IEEE) pp 527–33
[25] Damgård I B, Fehr S, Salvail L and Schaffner C 2008 Cryptography in the bounded-quantum-storage model *SIAM J. Comput.* **37** 1865–90
[26] Chakraborty K, Chailloux A and Leverrier A 2015 Arbitrarily long relativistic bit commitment *Phys. Rev. Lett.* **115** 250501
[27] Portmann C and Renner R 2014 Cryptographic security of quantum key distribution arXiv:1409.3525
[28] Broadbent A, Fitzsimons J and Kashefi E 2009 Universal blind quantum computation *2009 50th Annual IEEE Symp. on Foundations of Computer Science* (Piscataway, NJ: IEEE) pp 517–26
[29] Dunjko V, Fitzsimons J F, Portmann C and Renner R 2014 *Composable Security of Delegated Quantum Computation* (Berlin: Springer) pp 406–25
[30] Dunjko V and Kashefi E 2016 Blind quantum computing with two almost identical states arXiv:1604.01586
[31] Chiribella G, D'Ariano G M, Perinotti P and Valiron B 2013 Quantum computations without definite causal structure *Phys. Rev.* A **88** 022318
[32] Procopio L M *et al* 2015 Experimental superposition of orders of quantum gates *Nat. Commun.* **6** 7913
[33] Rubino G *et al* 2017 Experimental verification of an indefinite causal order *Sci. Adv.* **3** e1602589
[34] Colnaghi T, D'Ariano G M, Perinotti P and Facchini S 2012 Quantum computation with programmable connections between gates *Phys. Lett.* A **376** 2940–3

[35] Araújo M, Costa F and Brukner Č 2014 Computational advantage from quantum-controlled ordering of gates *Phys. Rev. Lett.* **113** 250402
[36] Oreshkov O, Costa F and Brukner Č 2012 Quantum correlations with no causal order *Nat. Commun.* **3** 1092
[37] Zych M, Costa F, Pikovski I and Brukner C 2017 Bell's theorem for temporal order arXiv:1708.00248
[38] Hardy L 2005 Probability theories with dynamic causal structure: a new framework for quantum gravity arXiv:gr-qc/0509120
[39] Chiribella G, D'Ariano G M and Perinotti P 2009 Theoretical framework for quantum networks *Phys. Rev.* A **80** 022339
[40] Gutoski G 2010 On a measure of distance for quantum strategies *J. Math. Phys.* **53** 032202
[41] Hardy L 2012 The operator tensor formulation of quantum theory *Phil. Trans. R. Soc.* A **370** 3385–417