On the composable security of weak coin flipping

Jiawei Wu (吴家为)[1], Yanglin Hu (胡杨林)[1], Akshay Bansal[2,3], and Marco Tomamichel[1,4]

[1]Centre for Quantum Technologies, National University of Singapore, Singapore
[2]Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA
[3]Virginia Tech Center for Quantum Information Science and Engineering, Blacksburg, VA, USA
[4]Department of Electrical and Computer Engineering, National University of Singapore, Singapore

Weak coin flipping is a cryptographic primitive in which two mutually distrustful parties generate a shared random bit to agree on a winner via remote communication. While a stand-alone secure weak coin flipping protocol can be constructed from noiseless quantum communication channels, its composability remains unexplored. In this work, we demonstrate that no weak coin flipping protocol can be abstracted as a simple black-box resource with composable security. Despite this, we also establish the overall stand-alone security of quantum weak coin flipping protocols under composition in sequential order.

1 Introduction

Motivation and background

Cryptographic systems or protocols are expected to guarantee security even when composed with multiple other cryptographic systems. To illustrate this, consider a cryptographic protocol designed to perform secure communication between two parties while leaking at most the length of the communicated message. One possible way to construct such a scheme is to first use a system that generates and distributes secret keys amongst the users and then use another system that pads the key with the intended message to be sent to the receiver (the so-called one-time pad). While it is relatively straightforward to see that a buggy implementation that compromises the security of key distribution or one-time pad would result in overall insecure communication, it is at times difficult to formally argue that the final composition results in a secure communication channel when both the constituent systems (key distribution and one-time pad) are assumed secure in isolation. Indeed, it might seem natural to use small accessible information of the distributed key as the security criterion for key distribution. However, the fact that key distribution using this criterion is secure in isolation does not imply that the final communication protocol is secure [1], due to the data locking effect [2]. We thus say that composability fails for this security criterion.

Several frameworks have been proposed that are intended to analyze compositions of cryptographic systems, starting with Canetti's seminal Universally Composable (UC)

Jiawei Wu (吴家为): constchar0212@gmail.com
Yanglin Hu (胡杨林): yanglin.hu@u.nus.edu
Akshay Bansal: akshaybansal14@gmail.com
Marco Tomamichel: marco.tomamichel@nus.edu.sg, https://marcotom.info/

security framework [3, 4]. Since then, several extensions and variants have emerged (see, e.g., [5, 6, 7, 8]). We focus here on the model of Abstract Cryptography (AC) by Maurer and Renner [9, 10]. In contrast to the previous frameworks, the latter is a top-down axiomatic approach and is intended to provide better insights via abstraction of a given complex cryptographic system and is thus most suitable for our purposes. The security in the AC framework is built on simulation-based security. Here, for a given system to be deemed secure, it suffices to ensure that all adversarial attacks on the system can be simulated on an ideal system. Therefore, to prove the security of any multi-party protocol in the AC framework, one needs to show the existence of such a simulator simulating all possible adversary attacks.

The cryptographic setting we consider in this work is a two-party primitive called weak coin flipping (WCF). Informally speaking, in WCF two mutually distrustful parties, say Alice and Bob, need to agree on a binary outcome even though the two parties have opposite preferences. The protocol is deemed secure if it produces a fair coin toss in case both parties are honest and a dishonest party can at most bias the honest party's outcome towards their preference. The WCF task is fundamentally different from the other commonly studied tasks such as strong coin flipping (SCF), bit commitment (BC), oblivious transfer, or more generally, secure function evaluation. While the latter protocols are shown to be insecure with an unbounded adversary [11, 12, 13, 14, 15], it is possible to construct weak coin flipping protocols with quantum communication that exhibit almost perfect security with arbitrarily small bias [16]. The explicit protocols which are shown to have an arbitrarily small bias are developed in [17, 18, 19]. The security notion employed in these results, known as information-theoretic security, allows an adversary to enjoy unlimited resources (i.e., the adversary has no restrictions on its computational power or use of memory, etc.). It is well-studied for a range of different cryptographic tasks and, in most cases, is stronger than other commonly studied security definitions such as computational [20, 21, 22], bounded storage [23, 24, 25] or even game-based [26, 27], where an adversary can perform attacks in only some prescribed ways.

Previously, it was shown that WCF enjoys information-theoretic stand-alone security, i.e., it is secure as a single protocol instance in isolation [16, 17, 18, 19]. While WCF itself is of limited interest, it is a powerful tool in constructing optimal protocols for several other primitives such as bit commitment [28] and strong coin flipping [29]. However, such constructions would require more than stand-alone security, and it is still unclear if WCF protocols have composable security when combined with other cryptographic protocols.

Contributions

Our main contributions encompass two negative theorems and one positive theorem. In Theorem 5, we demonstrate the impossibility of constructing a typical WCF resource (see Definition 4) analogous to the widely-used SCF resource [30] from noiseless communication channels in the AC framework. Generally speaking, a resource is the abstraction of certain cryptographic functionality (see Section 2.1). This WCF resource generates a random bit for both parties, allowing the cheating party to learn the bit in advance and bias it towards their preferred choice. It was shown that the widely-used SCF resource cannot be achieved in the AC framework [31], but the result for the similar WCF resource remains unknown until this work. We state Theorem 5 here informally.

Theorem 1 (Informal)**.** *The typical WCF resource in Definition 4 with composable security cannot be constructed from noiseless communication channels in the AC framework.*

To prove Theorem 5, we show that WCF protocols using noiseless communication

channels are vulnerable to the man-in-the-middle attack when composed in parallel. As a result, the typical WCF resource cannot be constructed by any WCF protocol from noiseless communication channels in the AC framework.

While Theorem 5 shows the impossibility of the typical WCF resource in the AC framework, we can still define an alternative WCF resource at the cost of increasing the interaction complexity. Nevertheless, such an alternative WCF resource that can be constructed from noiseless communication channels must be extremely complicated in terms of its interaction complexity, as is shown in Theorem 6. Replacing an actual protocol with an ideal resource intends to simplify the analysis; therefore, it is meaningless to study such an alternative WCF resource. Here is the informal statement of Theorem 6.

Theorem 2 (Informal)**.** *Any WCF resource with composable security constructed from noiseless communication channels in the AC framework must have high interaction complexity.*

The proof of Theorem 6 consists of two steps. First, we show that an alternative WCF resource with composable security constructed from noiseless communication channels implies a WCF protocol with the same interaction complexity as the alternative WCF resource. Then, together with the exponential lower bound on the interaction complexity of WCF protocols [32], we conclude that a WCF resource with a low interaction complexity cannot exist.

Next, we extend the classical version of the composition theorem for sequentially ordered protocols [33, Theorem 7.4.3] to the quantum case. We find a sufficient condition called global security where WCF and other modules can be composed into a larger system with stand-alone security. A composition between WCF and other components is globally secure if there is no correlation between the outcomes of WCF and other components. We thus show in Theorem 10 that global security holds when WCF and all other components are composed in a strict causal order. That is, there is no other component running concurrently with WCF. The constructions for optimal SCF and optimal BC exactly satisfy global security.

Theorem 3 (Informal)**.** *A primitive constructed from WCF with stand-alone security under strictly ordered sequential composition maintains its stand-alone security.*

The idea to prove Theorem 10 is by contradiction. Assume that there is some correlation between outcomes of WCF with stand-alone security and other components under ordered sequential composition. Using the information carried from previous components to WCF, we can construct an attack breaking the stand-alone security of WCF. This contradicts our assumption and thus proves Theorem 10.

Related work

Causality in the composable framework. Some early works [34, 35] developed the paradigm that only allows for sequential-order composition, where protocols are executed one after another. Canetti [3] relaxed sequential composition to modular composition in the UC framework, where the former is a special case of the latter. The AC framework [9, 10] takes a top-down approach. Only the connection of abstract systems is considered at the top level, and the execution order is left at the lower level specification. Under the AC framework, the causal box model [36] provides the causal order specification that allows for a quantum superposition of different message orders.

Concerning concurrent composition. Literature [24, 25] addresses the difficulty of concurrent parallel composition in the UC framework and the bounded-storage model. The

composability of BC was discussed in [37]. They define the weak binding security of BC in a stand-alone rather than composable manner and propose a counterexample where the string commitment constructed from multiple instances of BC is insecure. In a previous model of general cryptographic protocols [33, Section 7.3], concurrent calls to an oracle (resource) are also forbidden. This restriction primarily stems from the formulation of syntax in that model, rather than an explicit security concern. Recent work by Batra et al. [38] provides device-independent protocols for oblivious transfer and bit commitment proven secure under sequential composition, where all queries to the ideal functionality must be performed sequentially, but their concurrent composable security remains unknown.

Coin flipping within the AC framework. To study the composability of SCF, Demay and Maurer [30] propose an SCF resource and prove that it can be constructed from a BC resource. However, this resource is shown to be impossible to construct from noiseless communication channels, even in a relativistic setting [31].

2 Preliminaries

2.1 The abstract cryptography framework

The building blocks of the framework are resources, converters (protocols), and distinguishers. Resources are interactive systems that abstract cryptographic functionalities, and converters transform one resource into another. Distinguishers distinguish resources from each other. The framework can describe multiparty functionalities, but in this work, we only focus on two-party ones.

- A *resource*, denoted by R, has one interface accessible to each party. Each party can send inputs, receive outputs, perform operations and give instructions via the corresponding interface. In two-party cryptography, it is necessary to consider three different behaviors R, R_A and R_B of a resource, in which R, R_A and R_B correspond to the case where both are honest, where only Alice is dishonest, and where only Bob is dishonest, respectively. We use $\mathcal{R} = (R, R_A, R_B)$ to compactly denote a resource.

- A *converter*, denoted by α, is a cryptographic system with an inner interface that connects to a resource and an outer interface that connects to a player. The set of all converters is denoted by Σ. Each party can instruct the converter on the outer interface to execute specific tasks on the inner interface. A converter α can convert one resource R into another resource S by connecting its inner interface to one interface of the resource R. The interfaces of the resource S consist of the unconnected interface of the resource R and the outer interface of the converter α. We denote the connection between the converter α and the left-side (right-side) interface of the resource R by αR ($R\alpha$).

- A *protocol* $\pi = (\pi_A, \pi_B)$ consists of Alice's converter π_A and Bob's converter π_B. By connecting each converter to the corresponding interface of a resource R, the protocol π can transform R into the required resource S, provided that $S = \pi_A R \pi_B$. For example, suppose R is a binary symmetric channel resource and (π_A,π_B) is an encoder-decoder pair corresponding to a proper error-correcting code. Then one can construct a noiseless channel resource as $S = \pi_A R \pi_B$.

- A *distinguisher*, denoted by $\mathcal{D}$, is an agent who can access both interfaces of a resource. Given one of two resources R and S uniformly at random, a distinguisher

distinguishes whether the resource is R or S by interacting with it on both interfaces. The distinguishing advantage of the above task is defined as

$$d(R,S) = \sup_{\mathcal{D}} |\Pr[\mathcal{D}(R)=0] - \Pr[\mathcal{D}(S)=0]|. \tag{1}$$

The distinguishing advantage is a pseudo metric between two resources, satisfying the symmetry and triangle inequality properties. If $d(R,S) \leq \delta$, we also write $R \approx_\delta S$.

With these building blocks, we define composable security for two-party functionalities.

Definition 1 (Composable security)**.** *A protocol $\pi = (\pi_A, \pi_B)$ constructs resource $\mathcal{S} = (S, S_A, S_B)$ out of resource $\mathcal{R} = (R, R_A, R_B)$ with distinguishing advantage δ if the following conditions are satisfied:*

1. *Correctness*

$$S \approx_\delta \pi_A R \pi_B; \tag{2}$$

2. *Security against dishonest Bob*

$$\exists \sigma_B \in \Sigma, S_B \sigma_B \approx_\delta \pi_A R_B; \tag{3}$$

3. *Security against dishonest Alice*

$$\exists \sigma_A \in \Sigma, \sigma_A S_A \approx_\delta R_A \pi_B. \tag{4}$$

This construction is denoted by $\mathcal{R} \xrightarrow{\pi,\delta} \mathcal{S}$. Alternatively, we say that $\mathcal{S}$ is an abstraction of π based on $\mathcal{R}$, or that $\mathcal{S}$ abstracts π based on $\mathcal{R}$.

In Definition 1, σ_A and σ_B are called simulators. These simulators enforce a critical security property: any cheating strategy against the real resource $\mathcal{R}$ can be translated via the simulators into a corresponding cheating strategy against the ideal resource $\mathcal{S}$. For instance, if dishonest Bob deviates from π_B and follows π'_B instead, then, we have $S_B \sigma_B \pi'_B \approx_\delta \pi_A R_B \pi'_B$ by Equation (3), which means Bob's strategy π'_B in the real world (interacting with $\pi_A R_B$) is simulated by the $\sigma_B \pi'_B$ in the ideal world (interacting with S_B). For a detailed description of simulators and the related security notions in cryptography, we refer to the tutorial [39].

When $\mathcal{R}$ is a noiseless communication channel, the conditions can be simplified as

$$S \approx_\delta \pi_A \pi_B, \tag{5}$$

$$\exists \sigma_B \in \Sigma, S_B \sigma_B \approx_\delta \pi_A, \tag{6}$$

$$\exists \sigma_A \in \Sigma, \sigma_A S_A \approx_\delta \pi_B. \tag{7}$$

2.2 The quantum comb model

A quantum comb [40, 41] is a general quantum information processing system with internal memory that processes incoming messages sequentially. An example of a quantum comb is shown in Figure 1. At the lower level specification of the AC framework where the execution order is taken into account, building blocks are commonly modeled as quantum combs. A protocol which can be modeled within the quantum comb model (QCM) is called a QCM protocol. All existing WCF protocols can be classified as QCM protocols.

The interaction complexity of a QCM protocol π, denoted by $\mathsf{Intcom}(\pi)$, is defined as the communication rounds it requires. As an example, for a protocol π modeled by Figure 1, $\mathsf{Intcom}(\pi) = n$. For resources S_A and S_B, their interaction complexity refers to the communication rounds at the adversary's side. For example, the interaction complexity of WCF resource S_A in Figure 3(b) is the number of rounds on the left side, which is 1.

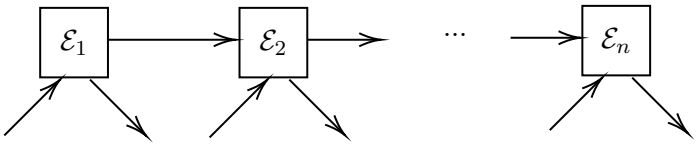

Figure 1: An example of quantum comb. The lines represent quantum registers, and $\mathcal{E}_i$ is a quantum operation. Each quantum operation interacts with the environment through an input-output pair, resembling the teeth of a comb.

2.3 The causal box model

The causal box model [36] is a more general specification of building blocks in the AC framework. The causal box model describes the causal structure of the messages exchanged by these building blocks. The quantum comb model can be treated as a special case of the causal box model.

In the causal box model, the abstract blocks are modeled as causal boxes. A causal box is an information processing system with input and output wires. Each message on a wire is described by a quantum state on space $\mathcal{H} \otimes l^2(\mathcal{T})$, where $\mathcal{T}$ is a partially ordered set (poset) that defines the message ordering, and $l^2(\mathcal{T})$ is the set of all functions $\mathcal{T} \to \mathbb{C}$ with bounded L^2-norm. Note that $\mathcal{T}$ is not necessarily interpreted as time, as time is totally ordered. In general, a wire may carry multiple messages. Therefore, the wire space is defined as the Fock space of the message space,

$$\mathcal{F}_{\mathcal{H}}^{\mathcal{T}} := \bigoplus_{n=0}^{\infty} \vee^n \left(\mathcal{H} \otimes l^2(\mathcal{T}) \right), \tag{8}$$

where $\vee^n \mathcal{H}$ denotes the symmetric subspace of $\mathcal{H}^{\otimes n}$. Here, $\mathcal{F}_{\mathcal{H}}^{\mathcal{T}}$ is also a Hilbert space. For convenience, we use the shorthand notation $\mathcal{F}_A^{\mathcal{T}}$ for $\mathcal{F}_{\mathcal{H}_A}^{\mathcal{T}}$. With this definition, wires can be merged or split, i.e., for $\mathcal{H}_A = \mathcal{H}_{A_1} \oplus \mathcal{H}_{A_2}$,

$$\mathcal{F}_A^{\mathcal{T}} = \mathcal{F}_{A_1}^{\mathcal{T}} \otimes \mathcal{F}_{A_2}^{\mathcal{T}}. \tag{9}$$

Formally, a causal box is defined as a completely positive and trace-preserving (CPTP) map that transforms the input wires to the output wires. This map should further respect the causality condition, i.e., the output message at $t' \in \mathcal{T}$ only depends on the input messages at $t \in \mathcal{T}$ where $t \preceq t'$. A precise definition can be found in Appendix A.

The composition of causal boxes consists of parallel composition and loops. The parallel composition of causal boxes Φ and Ψ, denoted by $\Phi \| \Psi$, is defined as the map $\Phi \otimes \Psi$. By Equation (9), the input and output spaces of $\Phi \otimes \Psi$ remain valid wires. A loop connects segments with the same dimension of the input and output wires. An interface labeled by x for a causal box Φ is denoted by $\mathsf{int}_x(\Phi)$, which consists of a set of wires, possibly including both input and output wires. For example, the inner and outer interfaces of a converter α are denoted by $\mathsf{int}_{in}(\alpha)$ and $\mathsf{int}_{out}(\alpha)$, respectively. Two interfaces $\mathsf{int}_a(\Phi)$ and $\mathsf{int}_b(\Psi)$ are compatible if there exists a bijection $P : \mathsf{int}_a(\Phi) \leftrightarrow \mathsf{int}_b(\Psi)$ such that each input wire of $\mathsf{int}_a(\Phi)$ corresponds to an output wire of $\mathsf{int}_b(\Psi)$ with the same dimension and vice versa.

2.4 Weak coin flipping

Here, we formulate WCF protocols with causal boxes.

Definition 2 (Weak coin flipping protocol)**.** *A weak coin flipping protocol using noiseless communication channels is a pair of converters $\pi = (\pi_A, \pi_B)$ with compatible inner interfaces, where π_A (π_B) has one output wire on the outer interface and only outputs a single classical bit at t_a (t_b). The poset $\mathcal{T}$ of the protocol is bounded both from above and below, i.e., $\exists t_0, t_a, t_b \in \mathcal{T}$, such that $\forall t \in \mathcal{T}$, it holds that $t_0 \preceq t$, $t \preceq t_a$ and $t \preceq t_b$.*

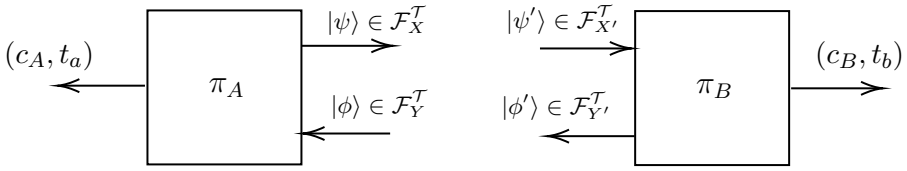

Figure 2: A general model for a coin flipping protocol using noiseless communication channels. The message spaces X, Y and X', Y' are of the same dimension, respectively.

In a WCF protocol, we say Alice wins if $c_B = 0$, while Bob wins if $c_A = 1$. In this case, an honest Bob only needs to prevent a cheating Alice from biasing c_B towards 0 and an honest Alice only needs to prevent a cheating Bob from biasing c_A towards 1.

Definition 3 (Stand-alone security of WCF)**.** *Let $z \in [0, \frac{1}{2}]$ and $\epsilon \leq z$. A coin flipping protocol $\pi = (\pi_A, \pi_B)$ is a z-unbalanced ϵ-biased WCF protocol (with stand-alone security), denoted by* $\mathrm{WCF}(z, \epsilon)$*, if the following conditions are satisfied:*

(S1) *The composition $\pi_A \pi_B$ by connecting the inner interface of (π_A, π_B) outputs (c_A, c_B) with a probability of*

$$\Pr[c_A = c_B = 0] = z, \quad \Pr[c_A = c_B = 1] = 1 - z. \tag{10}$$

(S2) *For any converter α compatible with the inner interface of π_B, the composition $\alpha\pi_B$ outputs $c_B = 0$ with a probability of*

$$\Pr[c_B = 0] \leq z + \epsilon. \tag{11}$$

(S3) *For any converter β compatible with inner interface of π_A, the composition $\pi_A\beta$ outputs $c_A = 1$ with a probability of*

$$\Pr[c_A = 1] \leq 1 - z + \epsilon. \tag{12}$$

We call a protocol balanced if $z = \frac{1}{2}$ and unbiased if $\epsilon = 0$.

3 Weak coin flipping is not universally composably secure

This section shows that WCF cannot be universally composably secure in the AC framework. The result contains two parts. First, we consider a specific WCF resource derived from a simple but widely adapted SCF resource [30] and show that this specific WCF resource cannot be constructed from a noiseless communication channel. Nevertheless, this result does not exclude the existence of other more complicated resources that can be constructed with, say, the protocol in [18]. Then our second result shows that, for any WCF protocol with enough stand-alone security, one cannot abstract it into a useful black-box resource, where usefulness means that the resource captures the full functionality of WCF while maintains a low interaction complexity.

3.1 Impossibility for a specific resource

We consider a reasonable and simple WCF resource in Figure 3 which is largely motivated from the strong coin flipping resource described in [30, Section III][1]. In the WCF task, a dishonest party wants to force only one of the two outcomes. To reflect this idea, we model the possible malicious operation as follows: (1) a cheating Alice (Bob) intercepts the random bit c' (c'') which ought to be the honest output in advance and (2) based on c' (c''), Alice (Bob) sends b' and p' (b'' and p'') to the resource to either resign by setting $p' = 1$ ($p'' = 1$) or replace c' with b with probability $\frac{\epsilon}{1-z}$ ($\frac{\epsilon}{z}$) by setting $p' = 0$ ($p'' = 0$). This establishes Definition 4 as a tuple of ideal WCF resources that allows for a maximum bias of ϵ for different scenarios.

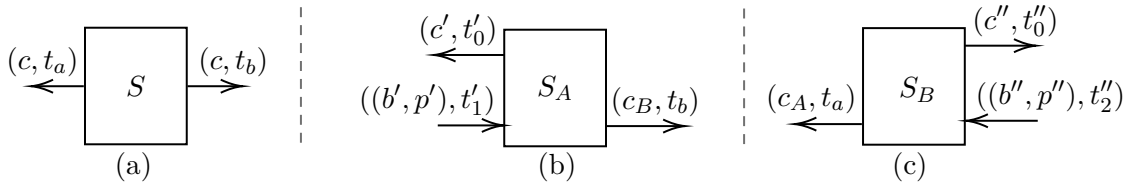

Figure 3: (a), (b) and (c) respectively show the components S, S_A, S_B of the WCF resource $\mathcal{S}$. Every message is assigned an element of the order set to indicate the causal order.

Definition 4 (z-unbalanced ϵ-biased WCF resource)**.** *Let $z \in [0, \frac{1}{2}]$ and $\epsilon \in [0, z]$. A z-unbalanced ϵ-biased WCF resource is characterized by a tuple $\mathcal{S} = (S, S_A, S_B)$, as is shown in Figure 3.*

1. *S describes the case when both Alice and Bob are honest. In this case, both parties obtains a random bit c according to the probabilities*

$$\Pr[c = 0] = z, \quad \Pr[c = 1] = 1 - z. \tag{13}$$

2. *S_A describes the case when Alice is dishonest and Bob is honest. S_A outputs a random bit c' subject to the probability distribution $(z, 1-z)$ at t'_0 and receives two bits b', p' at t'_1 at the left interface. Then it outputs a bit c_B at t_b at the right interface. If $p' = 1$, then $c_B = 1$, else $c_B = b'$ with probability $\frac{\epsilon}{1-z}$ and $c_B = c'$ with probability $1 - \frac{\epsilon}{1-z}$. The causality condition is $t'_0 \prec t'_1 \prec t_b$.*

3. *S_B describes the case when Alice is honest and Bob is dishonest. S_B outputs a random bit c'' subject to the probability distribution $(z, 1-z)$ at t''_0 and receives two bits b'', p'' controlled by Bob at t''_1 at the right interface. Then it outputs a bit c_A at t_a at the left interface. If $p'' = 1$, then $c_A = 0$, else $c_A = b''$ with probability $\frac{\epsilon}{z}$ and $c_A = c''$ with probability $1 - \frac{\epsilon}{z}$. The causality condition is $t''_0 \prec t''_1 \prec t_a$.*

To elaborate on the functionality when one party is malicious, consider an example where cheating Alice tries to bias the output c_B of S_A towards 0. For this purpose, she

[1] Although the resource had origins in Blum's protocol [42] that constructs an *unfair* coin flip (where a party is allowed to abort on observing the outcome), it serves as an abstraction for a large family of SCF protocols. When using a similar protocol here, it is equivalent to a *biased* coin flip if the honest party declares themselves the winner (locally) whenever the dishonest party aborts [30]. Therefore, it is unnecessary to consider the case where players abort.

needs to set $p' = 0$ regardless of the value of c'. Then the probability of her successfully forcing $c_B = 0$ is

$$\Pr[c_B = 0] = \Pr[c' = 0] \cdot \Pr[c_B = 0|c' = 0] + \Pr[c' = 1] \cdot \Pr[c_B = 0|c' = 1].$$

As $p' = 0$, the optimal strategy for Alice is to set $b' = 0$ since c_B is either c' or b'. If $c' = 0$, which happens with probability $\Pr[c' = 0] = z$, then $c_B = 0$ for certain, i.e., $\Pr[c_B = 0|c' = 0] = 1$. If $c' = 1$, which happens with probability $\Pr[c' = 1] = 1 - z$, Alice's conditional winning probability equals the probability that c_B takes the value of b', i.e., $\Pr[c_B = 0|c' = 1] = \frac{\epsilon}{1-z}$. We thus have

$$\Pr[c_B = 0] = \Pr[c' = 0] \cdot 1 + \Pr[c' = 1] \cdot \frac{\epsilon}{1 - z} = z + \epsilon. \tag{14}$$

Similar arguments also hold for cheating Bob.

The following theorem indicates that the resource in Definition 4 cannot be constructed from noiseless communication channel.

Theorem 5. *For $z \in [0, \frac{1}{2}]$ and $\epsilon \in [0, z]$, there does not exist a protocol $\pi = (\pi_A, \pi_B)$ which can construct an z-unbalanced ϵ-biased WCF resource $\mathcal{S} = (S, S_A, S_B)$ with a distinguishing advantage $\delta < \frac{1}{3}(z(1 - z) - \epsilon + \epsilon \min\{2\epsilon, z\})$.*

Proof. Suppose that there exists a protocol $\pi = (\pi_A, \pi_B)$ that constructs an ideal z-unbalanced ϵ-biased WCF resource $\mathcal{S} = (S, S_A, S_B)$ with a distinguishing advantage δ (without loss of generality, we assume $z \in [0, \frac{1}{2}]$). Combining the security conditions for Alice (6) and Bob (7) using triangle inequality, we obtain

$$\exists \sigma \in \Sigma, S_B \sigma S_A \approx_{2\delta} \pi_A \pi_B, \tag{15}$$

where $\sigma = \sigma_B \sigma_A$. Once again, combining the previous equation with the correctness condition (5) using triangle inequality, we get

$$\exists \sigma \in \Sigma, S_B \sigma S_A \approx_{3\delta} S, \tag{16}$$

or equivalently,

$$\exists \sigma \in \Sigma, d(S_B \sigma S_A, S) \leq 3\delta. \tag{17}$$

This relation is illustrated in Figure 4.

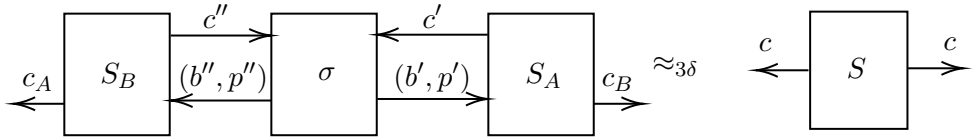

Figure 4: Illustration for Inequality (17).

We next establish a constant lower bound on such δ (constant in terms of z) by deriving a lower bound on the distinguishing advantage $d(S_B \sigma S_A, S)$ for any σ, i.e., $\min_\sigma d(S_B \sigma S_A, S)$. As the two systems $S_B \sigma S_A$ and S in Figure 4 do not need any external input, $d(S_B \sigma S_A, S)$ is simply the total variation distance between their output distributions, denoted by $P_{c_A c_B}$ and P_{cc} respectively, i.e.,

$$d(S_B \sigma S_A, S) = \frac{1}{2} \| P_{c_A c_B} - P_{cc} \|_1, \tag{18}$$

with $P_{cc}(0,0)=z, P_{cc}(1,1)=1-z$.

The best choice of causal order for σ is $t'_0 \prec t'_1, t'_0 \prec t''_1, t''_0 \prec t'_1, t''_0 \prec t''_1$ since it can maximize the use of information of c', c''. Then, the minimum distinguishing advantage can be bounded as follows:

$$\begin{aligned}
\min_{\sigma} d(S_B \sigma S_A, S) &= \min_{\sigma} \frac{1}{2} \big(\Pr[c_A=0, c_B=1] + \Pr[c_A=1, c_B=0] \\
&\qquad + \big|\Pr[c_A=0, c_B=0] - z\big| + \big|\Pr[c_A=1, c_B=1] - 1 + z\big|\big) \\
&\geq \min_{\sigma} \big(\Pr[c_A=0, c_B=1] + \Pr[c_A=1, c_B=0]\big) \\
&= \min_{\sigma} \Pr[c_A \neq c_B] \\
&\geq \min_{\sigma} \Pr[c'=1, c''=0] \cdot \Pr[c_A \neq c_B | c'=1, c''=0] \\
&\quad + \min_{\sigma} \Pr[c'=0, c''=1] \cdot \Pr[c_A \neq c_B | c'=0, c''=1] \\
&\quad + \min_{\sigma} \Pr[c'=c''] \cdot \Pr[c_A \neq c_B | c'=c''].
\end{aligned} \tag{19}$$

In the previous equation, the optimal distribution on (b', p', b'', p'') determines the optimal σ for each received value c', c''. The optimal distributions for different choices of c' and c'' are discussed next.

1. If $c'=c''=0$ or $c'=c''=1$, then the box σ outputs $p'=0, b'=c', p''=0, b''=c''$ to keep $c_A=c''=c'=c_B$, implying that $\min_\sigma \Pr[c_A \neq c_B | c'=c''] = 0$.

2. If $c'=0, c''=1$, then the box σ outputs $p'=1, p''=0$ to force the outcome $c_A=c_B=1$, implying that $\min_\sigma \Pr[c_A \neq c_B | c'=0, c''=1] = 0$.

3. If $c'=1, c''=0$, then we can assume the box σ outputs $p'=p''=0$ because setting $p'=1$ ($p''=1$) has the same effect as setting $p'=0, b'=c'$ ($p''=0, b''=c''$). Consider the event $c_A \neq c_B$ conditioned on different cases of (b', b''):

$$\begin{aligned}
&\Pr[c_A \neq c_B | c'=1, c''=0, b'=0, b''=0] = 1 - \frac{\epsilon}{1-z}; \\
&\Pr[c_A \neq c_B | c'=1, c''=0, b'=1, b''=0] = 1; \\
&\Pr[c_A \neq c_B | c'=1, c''=0, b'=0, b''=1] = 1 - \frac{\epsilon(1-2\epsilon)}{z(1-z)}; \\
&\Pr[c_A \neq c_B | c'=1, c''=0, b'=1, b''=1] = 1 - \frac{\epsilon}{z}.
\end{aligned} \tag{20}$$

All possible cheating strategies are in the convex hull of the above four cases, then we have

$$\min_{\sigma} \Pr[c_A \neq c_B | c'=1, c''=0] \tag{21}$$

$$= \min_{P_{b',b''}} \sum_{i',i'' \in \{0,1\}} P_{b',b''}(i',i'') \cdot \Pr[c_A \neq c_B | c'=1, c''=0, b'=i', b''=i''] \tag{22}$$

$$= \min_{i',i'' \in \{0,1\}} \Pr[c_A \neq c_B | c'=1, c''=0, b'=i', b''=i''] \tag{23}$$

$$= \begin{cases} 1 - \frac{\epsilon(1-2\epsilon)}{z(1-z)}, & \text{if } 0 \leq \epsilon < z/2 \\ 1 - \frac{\epsilon}{z}, & \text{if } z/2 < \epsilon \leq z \end{cases}. \tag{24}$$

where the conditional probabilities $\Pr[c_A \neq c_B | c'=1, c''=0, b'=i', b''=i'']$ are given in Equation (20), and Equation (24) holds because $0 \leq \epsilon \leq z \leq 1/2$.

By the above discussion, Equation (19) continues as

$$\min_{\sigma} d(S_B \sigma S_A, S) \geq \min_{\sigma} \Pr[c' = 1, c'' = 0] \cdot \Pr[c_A \neq c_B | c' = 1, c'' = 0] \tag{25}$$

$$= z(1-z) - \epsilon + \epsilon \min\{2\epsilon, z\}, \tag{26}$$

where Equation (25) follows from Equation (19) and the implications of Item 1 and Item 2. Equation (26) simply follows from Equation (24). Finally, combining Equation (17) and Equation (26), we have

$$\delta \geq \frac{1}{3} \left(z(1-z) - \epsilon + \epsilon \min\{2\epsilon, z\} \right), \tag{27}$$

which implies that π cannot construct $\mathcal{S}$ with a vanishing distinguishing advantage. □

Setting $\epsilon = 0, z = \frac{1}{2}$, we conclude that there does not exist a protocol π that constructs an ideal balanced unbiased WCF resource $\mathcal{S}$ with a distinguishing advantage $\delta < \frac{1}{12}$.

3.2 Impossibility for a general resource

Composable security is defined by requiring that an actual protocol emulates an ideal resource within a certain accuracy. As established in Theorem 5, no actual protocol can approximate the ideal WCF resource defined in Definition 4. However, this impossibility result pertains only to this specific ideal WCF resource. By redefining the ideal WCF resource, potentially introducing additional structure, a protocol that securely constructs this modified ideal resource may still exist at the cost of a more complicated and less useful ideal WCF resource.

To address this possibility, it is crucial to determine what properties a WCF resource must possess to be useful in general. For a WCF resource $\mathcal{S} = (S, S_A, S_B)$, we propose the following conditions:

- **Fully expressing**. A resource $\mathcal{S}$ for WCF(z, ϵ) is fully expressing if
  1. S outputs the same value c at each side subject to distribution: $\Pr[c = 0] = z, \Pr[c = 1] = 1 - z$.
  2. For any converter α, the composition αS_A outputs bit 0 at the right interface with probability at most $z + \epsilon$.
  3. For any converter β, the composition $S_B \beta$ outputs bit 1 at the left interface with probability at most $1 - z + \epsilon$.
- **Simple**. Resource simplicity refers to abstraction of non-essential details of a protocol, thereby reducing its interaction complexity. This simplification facilitates the analysis of the resource in a more general context. Here we take the interaction complexity $\mathsf{Intcom}(S_A)$, $\mathsf{Intcom}(S_B)$ (defined in Section 2.2) to quantify it. Although the idea of a simple resource is rather subjective, we state a resource to be simple if its net interaction complexity $(\mathsf{Intcom}(S_A) + \mathsf{Intcom}(S_B))$ is of $\mathcal{O}(1)$.

Next, we will show that a fully expressing and simple WCF resource cannot be constructed from noiseless communication channels. Specifically, Theorem 6 states that, if a fully expressing resource for WCF(z, ϵ) with small ϵ can be constructed from noiseless communication channels, then its interaction complexity cannot be small.

Theorem 6. *Let π be a QCM* WCF$(\frac{1}{2},\epsilon)$ *protocol, and π constructs a fully expressing resource $\mathcal{S}=(S,S_A,S_B)$. Then the interaction complexity of $\mathcal{S}$ satisfies*

$$\min\{\mathsf{Intcom}(S_A),\mathsf{Intcom}(S_B)\}\geq\exp\left(\Omega(1/\sqrt{\epsilon})\right). \tag{28}$$

To prove Theorem 6, we need a proposition rewritten from [32, Theorem 8.2].

Proposition 7. *If π is a QCM* WCF$(\frac{1}{2},\epsilon)$ *protocol, then*

$$\mathsf{Intcom}(\pi)\geq\exp\left(\Omega(1/\sqrt{\epsilon})\right). \tag{29}$$

Proof of Theorem 6. Without loss of generality, we can assume $\mathsf{Intcom}(S_B)\leq\mathsf{Intcom}(S_A)$. Since $\mathcal{C}\xrightarrow{\pi}\mathcal{S}$, there exist converters σ_A,σ_B such that $\pi_A\pi_B\approx S$, $\pi_A\approx S_B\sigma_B$, and $\pi_B\approx\sigma_A S_A$. Construct a new protocol $\pi'=(\pi'_A,\pi'_B)$ with $\pi'_A=S_B,\pi'_B=\sigma_B\sigma_A S_A$. Because resource $\mathcal{S}$ is fully expressing, we conclude that π' is also a WCF$(\frac{1}{2},\epsilon)$ protocol. By Proposition 7,

$$\mathsf{Intcom}(S_B)=\mathsf{Intcom}(\pi')\geq\exp\left(\Omega(1/\sqrt{\epsilon})\right). \tag{30}$$

□

Some parts of the argument in the above proof are of more general interest. That is, if there exists a resource $\mathcal{S}$ that abstracts a two-party protocol π, it implies the existence of another protocol π' with the same interaction complexity as the resource $\mathcal{S}$. Furthermore, if the resource reduces the interaction complexity of π, then π' is a better protocol than π in terms of interaction complexity. An example is delegated quantum computation (DQC), where the client aims to delegate computation to the server while maintaining privacy. The S_A (against dishonest client) of DQC resource [43] abstracting the protocol in [44, 45] has no interaction on either side. This implies the existence of a simple DQC protocol with no interaction, wherein the client performs all the computation herself, ensuring both correctness and blindness.

4 Security of weak coin flipping under composition

Section 3 highlights the difficulties when formulating the security of WCF in the AC framework. Fortunately, despite these difficulties, there is a prospect of attaining positive outcomes regarding the composability of such protocols. This section starts with the limitation of the stand-alone security definition (Definition 3) in the context of composition. Specifically, for the construction of unbalanced WCF from a balanced one, we propose a condition (Inequality (34)) which, while implicit in [29], is essential in the security proof of the unbalanced WCF protocol depicted there. Subsequently, we introduce global security as an extension of the stand-alone definition to encompass possible interdependency between the outputs of the WCF protocol and other components in a larger system. Furthermore, we establish the condition under which global security is maintained.

4.1 Stand-alone security is not sufficient

For a cryptographic task, some security definitions seem fine from a stand-alone viewpoint, but may present some loopholes when composed with other protocols. For example, the accessible information criteria for quantum key distribution falls short of providing composable security due to the data-locking effect [2, 1]. A similar problem occurs in WCF. In particular, a WCF protocol $\pi=(\pi_1,\pi_2)$ (where π_1 and π_2 are used instead of π_A and

π_B to avoid confusion in subsequent protocol description) may find its stand-alone security insufficient for upper-level tasks.

To illustrate, consider an attacking strategy for an unbalanced WCF protocol $\mu = (\mu_A, \mu_B)$ constructed from two instances of balanced WCF protocol $\pi = (\pi_1, \pi_2)$. The protocol μ aims to model the scenario where Alice and Bob are concurrently running two instances of WCF with an undetermined execution order. Assume the protocol π follows the quantum comb model [41, 40] with $n+1$ (assume that n is odd without loss of generality) rounds of communication, where Alice and Bob send messages alternately. Then, π_1 and π_2 can be characterized by the ordered set $\mathcal{T}_\pi$ shown in Figure 5b, where the subset $\{t_i\}_{i=0}^n$ is totally ordered. The comb model further requires that

(**R1**) Messages are sent by π_1 and accepted by π_2 only at t_i where i is even.

(**R2**) Messages are sent by π_2 and accepted by π_1 only at t_i where i is odd.

The above conditions allow us to consider the wires in the two directions separately–one within the even subset of $\mathcal{T}_\pi$ and the other within the odd subset of $\mathcal{T}_\pi$.

The protocol μ is constructed by connecting two independent instances of π with the converter $\eta = (\eta_A, \eta_B)$, as shown in Figure 5a. The converter η_A accepts a classical bit c_A at position t_n from π_1 and a classical bit c'_A at position t'_b from π'_2 and outputs c''_A at position t_A, where $c''_A = c_A \wedge c'_A$.

We demonstrate that the stand-alone security of μ can be compromised even if that of π is maintained. As per [29, Lemma 4], if π is a WCF$(\frac{1}{2}, \epsilon)$ protocol and $\epsilon < 1/6$, μ is expected to be a WCF$(\frac{3}{4}, \frac{3}{2}\epsilon)$ protocol. However, it fails to be a WCF$(\frac{3}{4}, \frac{3}{2}\epsilon)$ protocol, as there exists a strategy for dishonest Bob to win the game with probability $\frac{1}{2}$. Before elaborating on this strategy, we introduce the delay box, denoted by Θ_f. This box essentially transforms a message at position t to a future position t' according to some delay function f. For a rigorous definition of delay box, see Appendix A.3.

For simplicity, denote $\theta_{f_1}, \theta_{f_2}$ as θ_1, θ_2. Consider the parallel composition of delay boxes $\theta = \theta_1 \| \theta_2$ depicted in Figure 6. The delay functions are defined as

$$f_1 : \{t_i \in \mathcal{T}_\pi \mid i \text{ is even}\} \to \mathcal{T}_{\theta_1}, t_i \mapsto t'_i, \tag{31}$$

$$f_2 : \{t'_i \in \mathcal{T}'_\pi \mid i \text{ is odd}\} \to \mathcal{T}_{\theta_2}, t'_i \mapsto t_i. \tag{32}$$

Proposition 8 shows that Figure 6a emulates a WCF protocol between Alice and herself. See Appendix B.1 for the proof.

Proposition 8. *The box $(\pi_1 \| \pi'_2)\theta$ has the same output distribution as $\pi_1 \pi_2$.*

Since $\pi = (\pi_1, \pi_2)$ is a balanced WCF protocol, the distribution of the final output c''_A is $P_{c''_A} = (1/2, 1/2)$, which contradicts our expectation that μ is a WCF$(\frac{3}{4}, \frac{3}{2}\epsilon)$ protocol.

This example suggests that a stronger criterion is necessary to guarantee the safe composition of WCF protocols. To achieve a WCF$(\frac{3}{4}, \frac{3}{2}\epsilon)$ protocol, it is essential that for any box connected to the inner interface of $\pi_1 \| \pi'_2$, the output satisfies

$$\forall x \in \{0,1\}, \Pr[c'_A = 1 | c_A = x] \leq \frac{1}{2} + \epsilon. \tag{33}$$

More generally, to construct an unbalanced WCF protocol WCF(z, ϵ') for arbitrary $z \in [0, \frac{1}{2}]$ with n instances of protocol π, the following condition is needed:

$$\forall i \in [n], \forall x_1^{i-1} \in \{0,1\}^{i-1}, \Pr[c_{A,i} = 1 | c_{A,1} = x_1, \ldots, c_{A,i-1} = x_{i-1}] \leq \frac{1}{2} + \epsilon, \tag{34}$$

where $x_1^i = x_1 x_2 \ldots x_i$ and the result of the i-th instance is denoted by $c_{A,i}$. Notably, inequality (34) is an implicit but crucial condition for the security of unbalanced WCF protocol introduced in [29].

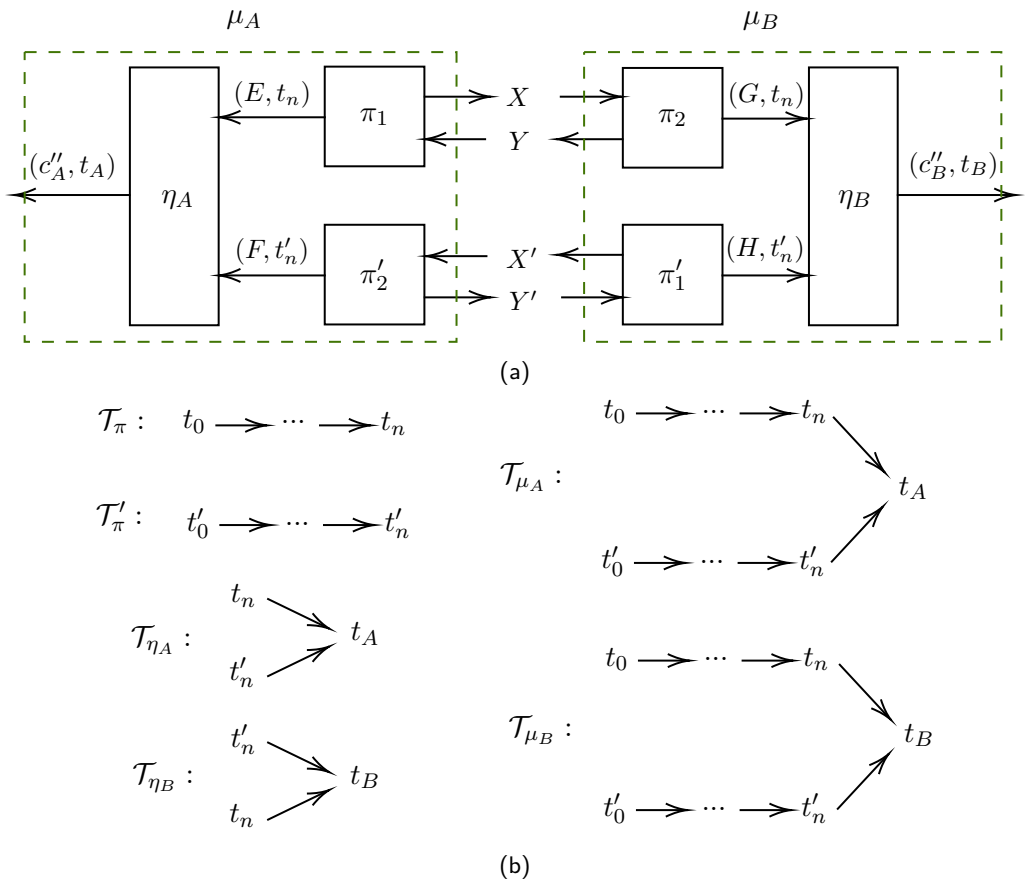

Figure 5: (a) The protocol $\mu = (\mu_A, \mu_B)$ is constructed from protocol π, π' and η. $\eta = (\eta_A, \eta_B)$ is a pair of converters and the two instances $\pi' = (\pi'_1, \pi'_2)$ and $\pi = (\pi_1, \pi_2)$ are the same except the ordered sets $\mathcal{T}'_\pi, \mathcal{T}_\pi$ are independent. (b) This figure shows the Hasse diagram of the posets $\mathcal{T}_\pi, \mathcal{T}'_\pi, \mathcal{T}_{\eta_A}, \mathcal{T}_{\eta_B}, \mathcal{T}_{\mu_A}, \mathcal{T}_{\mu_B}$. The Hasse diagram depicts the order relation with directed edge and omits the transitive and reflexive connections for simplicity. The poset $\mathcal{T}_{\mu_A}$ is obtained by union of $\mathcal{T}_\pi, \mathcal{T}'_\pi, \mathcal{T}_{\eta_A}$, which is defined in Definition 17. The poset of $\mathcal{T}_{\mu_b}$ is obtained similarly.

4.2 Global security

What is the sufficient condition for Inequality (34) to hold? More broadly speaking, what is the safe way to compose WCF protocols? Despite negative results discussed in Section 3 on the possibility of abstracting WCF as a resource, there are still certain secure ways of composition, e.g., those satisfying Inequality (34). To explore this, we generalize Inequality (34), introduce the concept of global secrecy and specify the sufficient condition for it.

Definition 9 (Global security of WCF in a larger system)**.** *Let π be a* WCF(z, ϵ) *protocol and η be a protocol that only outputs classical messages $K_A, K'_A, K_B, K'_B \in \mathbb{N}$ at its outer interface, where K_A, K_B are output before C_A, C_B and K'_A, K'_B are output after C_A, C_B. For a new protocol $\xi = (\xi_A, \xi_B)$ with $\xi_A = \pi_A \| \eta_A, \xi_B = \pi_B \| \eta_B$ (denoted by $\xi = \pi \| \eta$), the WCF protocol π is said to be globally secure in ξ if:*

1. *For any box α compatible with the inner interface of ξ_A: $\forall k \in \mathbb{N}, \Pr[C_A = 1 | K_A = k] \leq z + \epsilon$,*
2. *For any box β compatible with the inner interface of ξ_B: $\forall k \in \mathbb{N}, \Pr[C_B = 0 | K_B = k] \leq 1 - z + \epsilon$.*

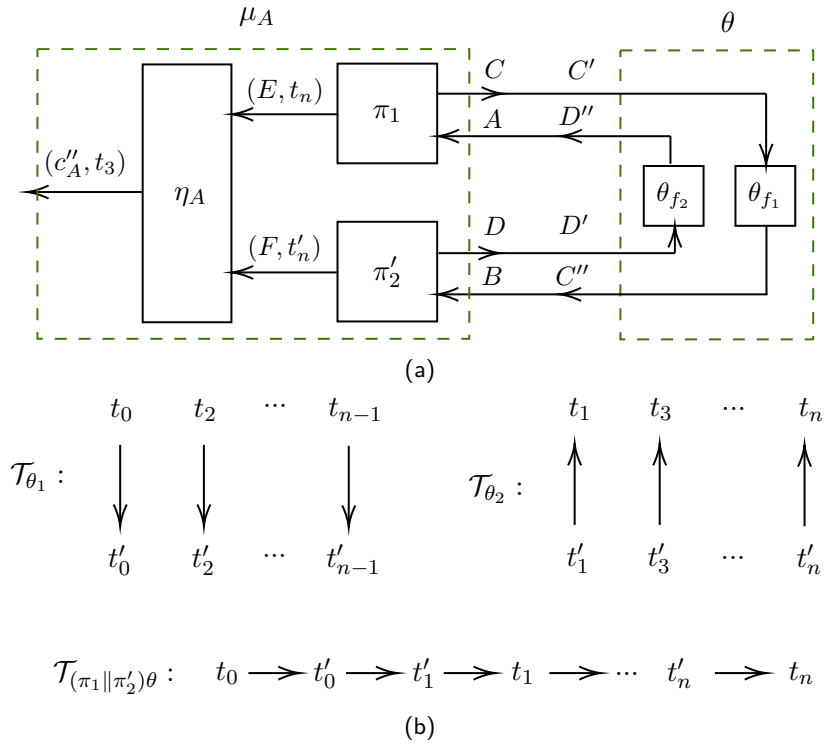

Figure 6: (a) This figure shows the connection of μ_A and delay box θ. The box $\theta = \theta_1 \| \theta_2$ is a parallel composition of two delay boxes. (b) This figure shows the Hasse diagram of the ordered sets $\mathcal{T}_{\theta_1}$, $\mathcal{T}_{\theta_2}$ and $\mathcal{T}_{(\pi_1\|\pi'_2)\theta}$.

The global security defined above is a property of the whole composed system $\pi\|\eta$ rather than the protocol η alone. For some protocols η and η', a protocol π may be globally secure in $\pi\|\eta$ but not in $\pi\|\eta'$.

Notably, global security in this definition is much weaker than the universal composability in the AC framework. It is not within any composable framework and only applies to the scenario where the system composed with WCF in parallel takes no input from the outer interface. This assumption is even stricter than the non-interactive assumption in the bounded storage model [24]. Therefore, global security of all components in a larger system only ensures the stand-alone security of the larger system.

The following theorem formulates the intuition that the WCF protocol is not affected by other boxes as long as we forbid any other interaction when the WCF protocol is active.

Theorem 10. *Let π be a $\mathrm{WCF}(z, \epsilon)$ protocol and η be any protocol with only classical output at the outer interface. $\xi = \pi\|\eta$ is their parallel composition with the ordered set $\mathcal{T}$. Then π is globally secure in the protocol if there exists a partition $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ of $\mathcal{T}$ such that*

(C1) *$\forall t_1 \in \mathcal{T}_1, t_2 \in \mathcal{T}_2, t_3 \in \mathcal{T}_3$, $t_1 \prec t_2 \prec t_3$;*

(C2) *η only accepts input and produces output on set $\mathcal{T}_1 \cup \mathcal{T}_3$, while π only accepts input and produces output on set $\mathcal{T}_2$.*

The proof of Theorem 10 is in Appendix B.2. The proof idea is by contradiction. If the adversary can break the global security of the composed protocol, then the adversary can also break the stand-alone security of the WCF protocol, which contradicts the fact and thus completes the proof. Theorem 10 establishes the sufficient condition that the WCF protocols can be composed while maintaining the overall stand-alone security.

For more complicated functionalities, it is usually easy to construct asymmetric imperfect protocols in which one party can cheat more than the other party. Unbalanced WCF protocols make it possible for two parties to fairly choose one of these asymmetric imperfect protocols at random. This results in a less asymmetric imperfect protocol. Therefore, unbalanced WCF protocols play a key role in constructing optimal protocols of more complicated functionalities such as SCF and BC [29, 28]. An unbalanced WCF(z, ϵ') protocol can be constructed from balanced WCF$(\frac{1}{2}, \epsilon)$ protocols where $z = 0.b_1b_2 \dots b_n$ is in binary representation, as is shown in Figure 7.

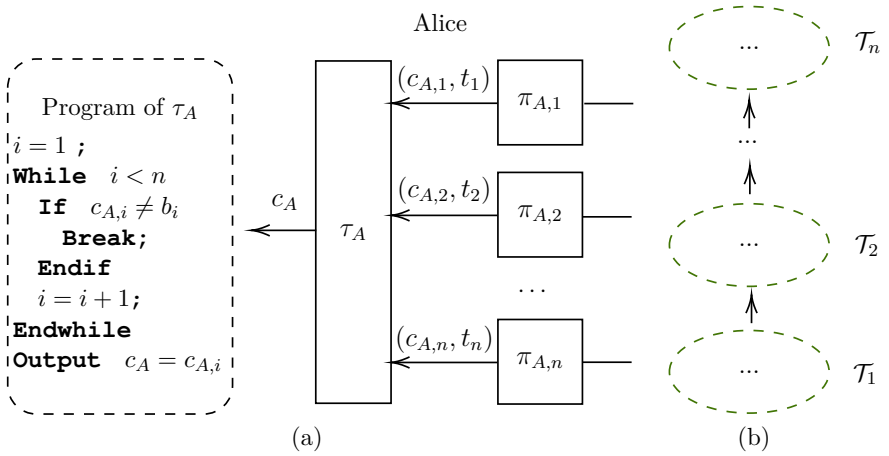

Figure 7: (a) This figure shows Alice part of the unbalanced WCF protocol $\eta_A = \tau_A(\pi_{A,1} \| \dots \| \pi_{A,n})$ constructed from balanced protocols π. It runs n instances of π_A and processes their result in τ_A. The program of τ_A is presented in the dashed box. Bob's part works similarly. (b) This figure shows the form of the Hasse diagram of η_A, where $\mathcal{T}_i$ is the posets for instance $\pi_{A,i}$. The instances of π_A run in a time-sequential way.

As an example, we apply Theorem 10 to this construction to prove the stand-alone security of the unbalanced WCF protocol in Corollary 11. The idea is to prove the stand-alone security of $\tau_i(\pi_1 \| ... \| \pi_i)$ constructed from $\tau_{i-1}(\pi_1 \| ... \| \pi_{i-1})$ and π_i using Theorem 10 recursively. The detailed proof can be found in Appendix B.3.

Corollary 11. *Let $z \in [0, \frac{1}{2}]$. The unbalanced WCF protocol shown in Figure 7 is a* WCF(z, ϵ') *protocol with $\epsilon' = 2\epsilon + o(\epsilon)$.*

5 Discussion

Our work demonstrates that the standalone security of protocols does not guarantee the security under certain types of composition. In particular, although quantum WCF protocol can be secure in the standalone scenario, it fails to be composably secure in the abstract cryptography framework. Moreover, when we construct new protocols with quantum WCF protocol, it remains secure in sequential composition, but exhibits security loopholes in concurrent composition. Similar security loopholes also arise in other two-party cryptographic tasks, such as bit commitment [25, 37]. For these tasks, though we have hoped for simple and good abstractions for actual protocols in the abstract framework, our work suggests that such abstraction does not exist, which makes security analysis of such protocols notably challenging.

6 Acknowledgement

We thank Christopher Portmann and Vilasini Venkatesh for useful discussions. This research was initiated while AB was hosted at CQT. This research is supported by the National Research Foundation, Singapore and A*STAR under its CQT Bridging Grant and its Quantum Engineering Programme (NRF2021-QEP2-01-P06). AB acknowledges the partial support provided by Commonwealth Cyber Initiative (CCI-SWVA) under the 2023 Cyber Innovation Scholars Program.

References

[1] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. "Small accessible quantum information does not imply security". Physical Review Letters **98**, 140502 (2007).

[2] David P. DiVincenzo, Michał Horodecki, Debbie W. Leung, John A. Smolin, and Barbara M. Terhal. "Locking classical correlations in quantum states". Physical Review Letters **92**, 067902 (2004).

[3] Ran Canetti. "Security and Composition of Multiparty Cryptographic Protocols". Journal of Cryptology **13**, 143–202 (2000).

[4] Ran Canetti. "Universally composable security: A new paradigm for cryptographic protocols". In Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science. Pages 136–145. (2001).

[5] Ran Canetti, Yevgeniy Dodis, Rafael Pass, and Shabsi Walfish. "Universally composable security with global setup". In Theory of Cryptography. Pages 61–85. Springer Berlin Heidelberg (2007).

[6] Dominique Unruh. "Universally composable quantum multi-party computation". In Advances in Cryptology – EUROCRYPT 2010. Pages 486–505. Springer Berlin Heidelberg (2010).

[7] Ran Canetti and Jonathan Herzog. "Universally composable symbolic security analysis". Journal of Cryptology **24**, 83–147 (2011).

[8] Ran Canetti, Asaf Cohen, and Yehuda Lindell. "A simpler variant of universally composable security for standard multiparty computation". In Advances in Cryptology – CRYPTO 2015. Pages 3–22. Springer Berlin Heidelberg (2015).

[9] Ueli Maurer and Renato Renner. "Abstract cryptography". In The Second Symposium on Innovations in Computer Science, ICS 2011. Pages 1–21. Tsinghua University Press (2011). url: https://crypto.ethz.ch/publications/files/MauRen11.pdf.

[10] Ueli Maurer. "Constructive Cryptography – A New Paradigm for Security Definitions and Proofs". In Theory of Security and Applications. Pages 33–56. Lecture Notes in Computer Science. Springer (2012).

[11] Hoi-Kwong Lo. "Insecurity of quantum secure computations". Physical Review A **56**, 1154–1162 (1997).

[12] Hoi-Kwong Lo and H. F. Chau. "Is quantum bit commitment really possible?". Physical Review Letters **78**, 3410–3413 (1997).

[13] Dominic Mayers. "Unconditionally Secure Quantum Bit Commitment is Impossible". Physical Review Letters **78**, 3414–3417 (1997).

[14] Hoi-Kwong Lo and H.F. Chau. "Why quantum bit commitment and ideal quantum coin tossing are impossible". Physica D: Nonlinear Phenomena **120**, 177–187 (1998).

[15] Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Rohrig. "Multiparty quantum coin flipping". In Proceedings of the 19th Annual IEEE Conference on Computational Complexity. Pages 250–259. (2004).

[16] Carlos Mochon. "Quantum weak coin flipping with arbitrarily small bias" (2007). arXiv:0711.4114.

[17] Atul Singh Arora, Jérémie Roland, and Stephan Weis. "Quantum weak coin flipping". In Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing. Pages 205–216. (2019).

[18] Atul Singh Arora, Jérémie Roland, and Chrysoula Vlachou. "Analytic quantum weak coin flipping protocols with arbitrarily small bias". In Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA). Pages 919–938. (2021).

[19] Atul Singh Arora, Jérémie Roland, Chrysoula Vlachou, and Stephan Weis. "Solutions to quantum weak coin flipping". Cryptology ePrint Archive, Paper 2022/1101 (2022).

[20] Daniel J Bernstein, Johannes Buchmann, and Erik Dahmen. "Post-Quantum Cryptography". Springer Berlin Heidelberg. (2008).

[21] Ivan Damgård and Carolin Lunemann. "Quantum-secure coin-flipping and applications". In Advances in Cryptology – ASIACRYPT 2009. Pages 52–69. Springer Berlin Heidelberg (2009).

[22] Urmila Mahadev. "Classical homomorphic encryption for quantum circuits". In Proceedings of the 59th Annual Symposium on Foundations of Computer Science. Pages 332–338. (2018).

[23] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. "Cryptography in the bounded-quantum-storage model". SIAM Journal on Computing **37**, 1865–1890 (2008).

[24] Stephanie Wehner and Jürg Wullschleger. "Composable Security in the Bounded-Quantum-Storage Model". In Automata, Languages and Programming. Pages 604–615. Lecture Notes in Computer Science. Springer (2008).

[25] Dominique Unruh. "Concurrent composition in the bounded quantum storage model". In Advances in Cryptology – EUROCRYPT 2011. Pages 467–486. Springer Berlin Heidelberg (2011).

[26] Dan Boneh and Victor Shoup. "A Graduate Course in Applied Cryptography". Online. (2023). url: `https://toc.cryptobook.us/`.

[27] David Nowak. "A framework for game-based security proofs". In Information and Communications Security. Pages 319–333. Springer Berlin Heidelberg (2007).

[28] André Chailloux and Iordanis Kerenidis. "Optimal Bounds for Quantum Bit Commitment". In Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science. Pages 354–362. (2011).

[29] André Chailloux and Iordanis Kerenidis. "Optimal Quantum Strong Coin Flipping". In Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science. Pages 527–533. (2009).

[30] Grégory Demay and Ueli Maurer. "Unfair coin tossing". In Proceedings of the IEEE International Symposium on Information Theory. Pages 1556–1560. (2013).

[31] V Vilasini, Christopher Portmann, and Lídia del Rio. "Composable security in relativistic quantum cryptography". New Journal of Physics **21**, 043057 (2019).

[32] Carl A. Miller. "The impossibility of efficient Quantum weak coin flipping". In Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing. Pages 916–929. (2020).

[33] Oded Goldreich. "Foundations of Cryptography". Volume 2. Cambridge University Press. (2004).

[34] Silvio Micali and Phillip Rogaway. "Secure Computation". In Advances in Cryptology — CRYPTO '91. Pages 392–404. Springer Berlin Heidelberg (1992).

[35] Donald Beaver. "Foundations of Secure Interactive Computing". In Advances in Cryptology — CRYPTO '91. Pages 377–391. Springer Berlin Heidelberg (1992).

[36] Christopher Portmann, Christian Matt, Ueli Maurer, Renato Renner, and Björn Tackmann. "Causal Boxes: Quantum Information-Processing Systems Closed Under Composition". IEEE Transactions on Information Theory **63**, 3277–3305 (2017).

[37] Jędrzej Kaniewski, Marco Tomamichel, Esther Hänggi, and Stephanie Wehner. "Secure bit commitment from relativistic constraints". IEEE Transactions on Information Theory **59**, 4687–4699 (2013).

[38] Rishabh Batra, Sayantan Chakraborty, Rahul Jain, and Upendra Kapshikar. "Robust and composable device-independent quantum protocols for oblivious transfer and bit commitment" (2024). arXiv:2404.11283.

[39] Yehuda Lindell. "How to simulate it – a tutorial on the simulation proof technique". Pages 277–346. Springer International Publishing. (2017).

[40] Gus Gutoski and John Watrous. "Toward a general theory of quantum games". In Proceedings of the 39th Annual ACM Symposium on Theory of Computing. Pages 565–574. (2007).

[41] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. "Theoretical framework for quantum networks". Physical Review A **80**, 022339 (2009).

[42] Manuel Blum. "Coin flipping by telephone a protocol for solving impossible problems". SIGACT News **15**, 23–27 (1983).

[43] Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann, and Renato Renner. "Composable Security of Delegated Quantum Computation". In Advances in Cryptology – ASIACRYPT 2014. Pages 406–425. Springer Berlin Heidelberg (2014).

[44] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. "Universal Blind Quantum Computation". In Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science. Pages 517–526. (2009).

[45] Joseph F. Fitzsimons. "Private quantum computation: An introduction to blind quantum computing and related protocols". npj Quantum Information **3**, 1–11 (2017).

A Causal box model

In this appendix, we introduce necessary concepts related to the causal box model. Part of this section is from [36].

A.1 Causal box

Let $\mathcal{T}$ be a partially ordered set (poset). That is, $\mathcal{T}$ is a set equipped with a binary relation $\preceq$ that is reflexive, antisymmetric and transitive. For $x, y \in \mathcal{T}$, $x \prec y$ if $x \preceq y$ and $x \neq y$. Denote $\mathcal{T}^{\preceq t} = \{x \in \mathcal{T} \mid x \preceq t\}$.

Definition 12 (Cuts)**.** *A subset $\mathcal{C}$ of poset $\mathcal{T}$ is a cut if it takes the form*

$$\mathcal{C} = \bigcup_{t \in \mathcal{C}} \mathcal{T}^{\preceq t}. \tag{35}$$

A cut is bounded if $\exists t \in \mathcal{T}, \mathcal{C} \subseteq \mathcal{T}^{\preceq t}$. The set of all cuts of $\mathcal{T}$ is denoted by $\mathfrak{C}(\mathcal{T})$. The set of all bounded cuts of $\mathcal{T}$ is denoted by $\bar{\mathfrak{C}}(\mathcal{T})$.

Lemma 13 (An equivalent condition for cut)**.** *A subset $\mathcal{C}$ of a poset $\mathcal{T}$ is a cut if and only if $t \in \mathcal{C} \Rightarrow \forall x \preceq t, x \in \mathcal{C}$.*

Proof. If $\mathcal{C}$ is a cut, for $t \in \mathcal{C}$ and $x \preceq t$, we have $x \in \mathcal{T}^{\preceq t}$, thus $x \in \mathcal{C}$. If $\forall t \in \mathcal{C}, \forall x \preceq t, x \in \mathcal{C}$, then $\forall x \in \mathcal{T}^{\preceq t}, x \in \mathcal{T}$. We have $\forall t \in \mathcal{C}, \mathcal{T}^{\preceq t} \subseteq \mathcal{C}$, thus $\mathcal{C} = \bigcup_{t \in \mathcal{C}} \mathcal{T}^{\preceq t}$. □

Definition 14 (Causality function)**.** *A function $\chi : \mathfrak{C}(\mathcal{T}) \to \mathfrak{C}(\mathcal{T})$ is a causality function if:*

$$\forall \mathcal{C}, \mathcal{D} \in \mathfrak{C}(\mathcal{T}), \quad \chi(\mathcal{C} \cup \mathcal{D}) = \chi(\mathcal{C}) \cup \chi(\mathcal{D}), \tag{36}$$

$$\forall \mathcal{C}, \mathcal{D} \in \mathfrak{C}(\mathcal{T}), \quad \mathcal{C} \subseteq \mathcal{D} \implies \chi(\mathcal{C}) \subseteq \chi(\mathcal{D}), \tag{37}$$

$$\forall \mathcal{C} \in \bar{\mathfrak{C}}(\mathcal{T}) \setminus \{\emptyset\}, \quad \chi(\mathcal{C}) \subsetneq \mathcal{C}, \tag{38}$$

$$\forall \mathcal{C} \in \bar{\mathfrak{C}}(\mathcal{T}), \forall t \in \mathcal{C}, \exists n \in \mathbb{N}, \quad t \notin \chi^n(\mathcal{C}), \tag{39}$$

Using cuts and causality function, we can formally define the causal box.

Definition 15 (Causal box)**.** *A causal box is a system with input wire X and output wire Y, defined as a set of CPTP maps:*

$$\Phi := \{\Phi^{\mathcal{C}} : \mathfrak{T}(\mathcal{F}_X^{\mathcal{T}}) \to \mathfrak{T}(\mathcal{F}_Y^{\mathcal{C}})\}_{\mathcal{C} \in \bar{\mathfrak{C}}(\mathcal{T})}, \tag{40}$$

where $\mathfrak{T}(\mathcal{H})$ denotes the set of all trace class operators on the Hilbert space $\mathcal{H}$. These maps must be mutually consistent

$$\forall \mathcal{C}, \mathcal{D} \in \bar{\mathfrak{C}}(\mathcal{T}), \mathcal{C} \subseteq \mathcal{D} : \Phi^{\mathcal{C}} = \mathrm{tr}_{\mathcal{D} \setminus \mathcal{C}} \circ \Phi^{\mathcal{D}}, \tag{41}$$

and respect causality, i.e., there exists a causality function $\chi : \mathfrak{C}(\mathcal{T}) \to \mathfrak{C}(\mathcal{T})$ such that

$$\Phi^{\mathcal{C}} = \Phi^{\mathcal{C}} \circ \mathrm{tr}_{\mathcal{T} \setminus \chi(\mathcal{C})}. \tag{42}$$

Alternatively, the causal box Φ can be described in Choi-Jamiołkowski (CJ) representation. To be precise, the Choi operator $R_\Phi^{\mathcal{C}}$ for the CPTP map $\Phi^{\mathcal{C}}$ is a sesquilinear semi-definite form on $\mathcal{F}_Y^{\mathcal{C}} \otimes \mathcal{F}_X^{\chi(\mathcal{C})}$ such that

$$R_\Phi^{\mathcal{C}}(\psi_Y \otimes \psi_X, \varphi_Y \otimes \varphi_X) = \langle \psi_Y | \Phi^{\mathcal{C}} \left(|\bar{\psi}_X\rangle\langle\bar{\varphi}_X| \right) |\varphi_Y\rangle. \tag{43}$$

where $|\overline{\psi}\rangle = \sum_i |i\rangle\langle\psi|i\rangle$ for a fixed basis $\{|i\rangle\}_i$.

A.2 Connection of causal boxes

Causal boxes can be connected by parallel composition and loop.

Definition 16 (Parallel composition of causal boxes)**.** *Let* $\Phi = \{\Phi^{\mathcal{C}}\}_{\mathcal{C}\in\bar{\mathfrak{C}}(\mathcal{T})}$ *and* $\Psi = \{\Psi^{\mathcal{C}}\}_{\mathcal{C}\in\bar{\mathfrak{C}}(\mathcal{T})}$ *be two causal boxes. The parallel composition of them, denoted by* $\Phi\|\Psi$ *is defined as*

$$\Gamma \coloneqq \left\{\Phi^{\mathcal{C}} \otimes \Psi^{\mathcal{C}}\right\}. \tag{44}$$

The above definition of parallel composition implicitly requires the causal boxes Φ and Ψ share the same partially ordered set $\mathcal{T}$. However, a general causal box may not contain the information of the causal structure of some other causal box. Then, a predefined common poset $\mathcal{T}$ may not exist. In this case, to make the composition possible, we propose a more general version of parallel composition. Before that, we introduce the union of posets that might have intersection.

A poset $\mathcal{T}$ can be treated as a tuple of a set and a partial order relation $\mathcal{T} = (\mathfrak{S}, \preceq)$. We define the union of two posets as follows.

Definition 17 (Union of partial orders)**.** *Let* $\mathcal{T}_1 = (\mathfrak{S}_1, \preceq_1)$ *and* $\mathcal{T}_2 = (\mathfrak{S}_2, \preceq_2)$ *be two compatible posets. Let the relation on the set* $\mathfrak{S} = \mathfrak{S}_1 \cup \mathfrak{S}_2$ *be* $\preceq = \preceq_1 \sqcup \preceq_2$*. Then* $x \preceq y$ *if and only if there exists a sequence* $\{a_i\}_{i=0}^{n} \subseteq \mathfrak{S}_1 \sqcup \mathfrak{S}_2$ *such that* $a_1 = x$*,* $a_n = y$ *and* $\forall i \in [n]$ *either* $a_{i-1} \preceq_1 a_i$ *or* $a_{i-1} \preceq_2 a_i$*. The union of posets, denoted by* $\mathcal{T}_1 \sqcup \mathcal{T}_2$*, is then defined as*

$$\mathcal{T}_1 \sqcup \mathcal{T}_2 \coloneqq (\mathfrak{S}_1 \cup \mathfrak{S}_2, \preceq_1 \sqcup \preceq_2) = (\mathfrak{S}, \preceq) \tag{45}$$

In the above definition, $\mathcal{T}_1$ and $\mathcal{T}_2$ are said to be compatible if $\preceq_1 \sqcup \preceq_2$ is still a partial order.

After introducing the union of posets, we are ready to define the parallel composition of two causal boxes with compatible posets.

Definition 18 (Parallel composition of causal boxes with arbitrary compatible ordered sets)**.** $\Phi = \{\Phi^{\mathcal{C}}\}_{\mathcal{C}\in\bar{\mathfrak{C}}(\mathcal{T}_1)}$ *and* $\Psi = \{\Psi^{\mathcal{C}}\}_{\mathcal{C}\in\bar{\mathfrak{C}}(\mathcal{T}_2)}$ *are causal boxes defined on compatible partially ordered set* $\mathcal{T}_1$ *and* $\mathcal{T}_2$ *respectively, which can have* arbitrary intersection*.* Φ *has input wire* X_1 *and output wire* Y_1*.* Ψ *has input wire* X_2 *and output wire* Y_2*. The parallel composition of* Φ *and* Ψ*, denoted by* $\Gamma = \Phi\|\Psi$*, is defined on the new poset* $\mathcal{T} = \mathcal{T}_1 \sqcup \mathcal{T}_2$ *as*

$$\Gamma \coloneqq \{\Gamma^{\mathcal{C}}\}_{\mathcal{C}\in\bar{\mathfrak{C}}(\mathcal{T})}, \tag{46}$$

$$\Gamma^{\mathcal{C}} \coloneqq \Phi^{\mathcal{C}_1} \otimes \Psi^{\mathcal{C}_2} \circ \mathrm{tr}_{\mathcal{F}_{X_1}^{\mathcal{T}\setminus\mathcal{T}_1} \otimes \mathcal{F}_{X_2}^{\mathcal{T}\setminus\mathcal{T}_2}}, \tag{47}$$

where $\mathcal{C}_1 = \mathcal{T}_1 \cap \mathcal{C}, \mathcal{C}_2 = \mathcal{T}_2 \cap \mathcal{C}$*.*

Lemma 19, 20 and 21 suggest that Definition 18 is well-defined.

Lemma 19. *For compatible posets* $\mathcal{T}_1$ *and* $\mathcal{T}_2$*, if* $\mathcal{C}$ *is a cut in* $\mathcal{T}_1 \sqcup \mathcal{T}_2$*, then* $\mathcal{C}_1 = \mathcal{C} \cap \mathcal{T}_1$ *and* $\mathcal{C}_2 = \mathcal{C} \cap \mathcal{T}_2$ *are cuts in* $\mathcal{T}_1$ *and* $\mathcal{T}_2$ *respectively.*

Proof. Notice that

$$\mathcal{C}_1 = \mathcal{C} \cap \mathcal{T}_1 = \bigcup_{t\in\mathcal{C}} (\mathcal{T}^{\preceq t} \cap \mathcal{T}_1). \tag{48}$$

Assume $t' \in \mathcal{T}^{\preceq t} \cap \mathcal{T}_1$, then by Definition 17, $\forall x \in \mathcal{T}_1, x \preceq_1 t' \Rightarrow x \preceq t \Rightarrow x \in \mathcal{T}^{\preceq t} \cap \mathcal{T}_1$. According to Lemma 13, $\mathcal{T}^{\preceq t} \cap \mathcal{T}_1$ is a cut in $\mathcal{T}_1$. As the union of cuts, $\mathcal{C}_1$ is also a cut. The same argument follows for $\mathcal{C}_2$. □

Lemma 20 (Existence of causality function)**.** *Let $\Gamma = \Phi \| \Psi$ with the poset $\mathcal{T} = \mathcal{T}_1 \sqcup \mathcal{T}_2$ be the parallel composition of causal boxes Φ and Ψ with compatible posets $\mathcal{T}_1$ and $\mathcal{T}_2$. There exists a causality function χ on $\mathfrak{C}(\mathcal{T})$ such that:*

$$\Gamma^{\mathcal{C}} = \Gamma^{\mathcal{C}} \circ \mathrm{tr}_{\mathcal{F}_{X_1 \oplus X_2}^{\chi(\mathcal{C})}} \tag{49}$$

Proof. Assume χ_1 and χ_2 are causality functions for Φ and Ψ, respectively. Construct the function $\chi : \mathfrak{C}(\mathcal{T}) \to \mathfrak{C}(\mathcal{T})$ as $\chi(\mathcal{C}) = \chi_1(\mathcal{C} \cap \mathcal{T}_1) \cup \chi_2(\mathcal{C} \cap \mathcal{T}_2)$, then it is easy to verify the conditions in Definition 14. □

Lemma 21 (Associativity)**.** *For boxes Φ, Ψ, Θ with compatible posets $\mathcal{T}_\Phi, \mathcal{T}_\Psi, \mathcal{T}_\Theta$, we have*

$$(\Phi \| \Psi) \| \Theta = \Phi \| (\Psi \| \Theta). \tag{50}$$

Proof. This lemma follows directly from Definition 18. □

Definition 22 (Loop)**.** *Let $\Phi = \{\Phi^{\mathcal{C}} : \mathfrak{T}(\mathcal{F}_{AB}^{\mathcal{T}}) \to \mathfrak{T}(\mathcal{F}_{CD}^{\mathcal{C}})\}_{\mathcal{C} \in \bar{\mathfrak{C}}(\mathcal{T})}$ be a causal box such that $\dim \mathcal{H}_B = \dim \mathcal{H}_C$ is its CJ representation. Let $\{|k_C\rangle\}$ and $\{|l_C\rangle\}$ be any orthonormal bases of $\mathcal{F}_C^{\mathcal{C}}$ and $\{|k_B\rangle\}$ and $\{|l_B\rangle\}$ be corresponding bases of $\mathcal{F}_B^{\mathcal{C}}$. The new box by looping from wire B to wire C, denoted by $\Psi = \Phi^{C \hookrightarrow B}$, is a set of maps $\{\Psi^{\mathcal{C}} : \mathfrak{T}(\mathcal{F}_A^{\mathcal{T}}) \to \mathfrak{T}(\mathcal{F}_D^{\mathcal{C}})\}$ with CJ representation*

$$R_\Psi^{\mathcal{C}}(\psi_D \otimes \psi_A, \varphi_D \otimes \varphi_A) \tag{51}$$

$$= \sum_{k,l} R_\Phi^{\mathcal{C}}(k_C \otimes \psi_D \otimes \psi_A \otimes \bar{k}_B, l_C \otimes \varphi_D \otimes \varphi_A \otimes \bar{l}_B), \tag{52}$$

where the conjugate $|\overline{\psi}\rangle = \sum_i |i_B\rangle\langle\psi|i_B\rangle$ is taken with respect to the base $|i_B\rangle$ of $\mathcal{F}_B^{\mathcal{T}}$ on which the CJ representation is defined.

Note that, to define a loop, it is necessary to specify two bases for each of the connected wire. With different bases for the wires, the result of the loop can be different.

A.3 Delay box

Definition 23 (Delay function)**.** *Let $\mathcal{T}$ be a poset and $\mathcal{G} = \{t \in \mathcal{T} \mid \exists t' \in \mathcal{T}, t \prec t'\}$ is a subset of $\mathcal{T}$. A function $f : \mathcal{G} \to \mathcal{T}$ is a delay function on $\mathcal{T}$ if for any $t \in \mathcal{G}$, $t \prec f(t)$.*

Proposition 24. *If $\mathcal{T}$ is a finite set, a delay function f on $\mathcal{T}$ induces a causality function*

$$\chi_f(\mathcal{C}) = \bigcup_{t : f(t) \in \mathcal{C}} \mathcal{T}^{\preceq t}. \tag{53}$$

It is easy to verify χ_f is a causality function by definition.

Definition 25 (Delay box)**.** *A delay box derived from a delay function $f : \mathcal{G} \to \mathcal{T}$ with input wire X and output wire X' is denoted by $\Theta_f = \{\Theta_f^{\mathcal{C}} : \mathfrak{T}(\mathcal{F}_X^{\chi_f(\mathcal{C})}) \to \mathfrak{T}(\mathcal{F}_X^{\mathcal{C}})\}_{\mathcal{C} \in \bar{\mathfrak{C}}(\mathcal{T})}$. $\mathcal{H}_X$ and $\mathcal{H}_{X'}$ are of the same dimension. $\Theta_f^{\mathcal{C}}$ is defined as the following isometry:*

$$U_f^{\mathcal{C}} = \bigoplus_{n=0}^{\infty} \left(\sum_{i \in I} |i\rangle_{X'}\langle i|_X \otimes \sum_{t \in \chi_f(\mathcal{C})} |f(t)\rangle\langle t| \right)^{\otimes n}, \tag{54}$$

for some bases $\{|i\rangle_X\}_{i \in I}$ and $\{|i\rangle_{X'}\}_{i \in I}$ of spaces $\mathcal{H}_X$ and $\mathcal{H}_{X'}$.

θ_1 is a delay box from input wire C' to output wire C'' and is derived from f_1 defined in Equation (31). Then, $U_{f_1}^{\mathcal{C}}$ is an isometry between $\mathcal{F}_{C'}^{\chi_{f_1}(\mathcal{C})}$ and $\mathcal{F}_{C''}^{\mathcal{C} \cap \mathcal{T}_{\pi'}}$.

B Proofs

B.1 Proof of Proposition 8

Proposition. *The box $(\pi_1\|\pi_2')\theta$ has the same output distribution as $\pi_1\pi_2$.*

Proposition 8 implies that two parties running π_1 and π_2' with an adversary running θ is equivalent to two parties running π_1 and π_2' between themselves. To achieve this, the adversary performs the man-in-the-middle attack, i.e., uses delay boxes to pass messages from π_1 to π_2' and pass responses from π_2' to π_1 subsequently. To be precise, notice that the boxes π_1 and π_2' work on two independent posets, i.e., the top part and bottom part in Figure 8b, respectively. The delay boxes θ_1 and θ_2 are the bridges that connect the two corresponding wire spaces. Then the key point is to find proper wire space isomorphisms for the wire connections such that π_2' together with the delay boxes is a perfect emulation of π_2.

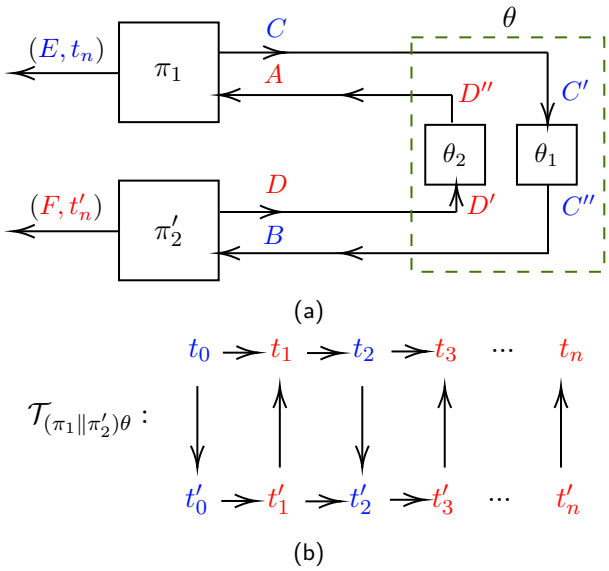

Figure 8: (a) This figure shows the connected box $(\pi_1\|\pi_2')\theta$. The wire with a blue notation indicates that the messages on this wire only stay in sets $\mathcal{T}_\pi^{\text{even}}$ and $\mathcal{T}_{\pi'}^{\text{even}}$, while the red notation corresponds to the sets $\mathcal{T}_\pi^{\text{odd}}$ and $\mathcal{T}_{\pi'}^{\text{odd}}$. (b) This figure explains the partition of the totally ordered set $\mathcal{T}_{(\pi_1\|\pi_2')\theta}$ with a non-standard Hasse diagram. Specifically, The blue elements at the top form the set $\mathcal{T}_\pi^{\text{even}}$; The blue elements at the bottom form the set $\mathcal{T}_{\pi'}^{\text{even}}$; The red elements at the top form the set $\mathcal{T}_\pi^{\text{odd}}$; The red elements at the bottom form the set $\mathcal{T}_{\pi'}^{\text{odd}}$.

Define the sets

$$\mathcal{T}_\pi^{\text{even}} := \{t_i \in \mathcal{T}_\pi \mid i \text{ is even}\}, \qquad \mathcal{T}_\pi^{\text{odd}} := \{t_i \in \mathcal{T}_\pi \mid i \text{ is odd}\}, \tag{55}$$

$$\mathcal{T}_{\pi'}^{\text{even}} := \{t_i \in \mathcal{T}_{\pi'} \mid i \text{ is even}\}, \qquad \mathcal{T}_{\pi'}^{\text{odd}} := \{t_i \in \mathcal{T}_{\pi'} \mid i \text{ is odd}\}. \tag{56}$$

Because the protocol π is restricted to the comb model, the wires B, C, C', C'', E are only effective on the set $\mathcal{T}_\pi^{\text{even}}$ and $\mathcal{T}_{\pi'}^{\text{even}}$. Similarly, the wires A, D, D', D'', F are only effective on the set $\mathcal{T}_\pi^{\text{odd}}$ and $\mathcal{T}_{\pi'}^{\text{odd}}$. By saying wire X is only effective on $\mathcal{T}'$, we mean the state on this wire is always in the space $\mathcal{F}_X^{\mathcal{T}'}$.

For convenience, where the cut $\mathcal{C}$ is obvious, denote for $X = B, C, C', C'', E$

$$\hat{X} = \mathcal{F}_X^{\mathcal{C}\cap\mathcal{T}_\pi^{\text{even}}}, \tag{57}$$

$$\tilde{X} = \mathcal{F}_X^{\mathcal{C}\cap\mathcal{T}_{\pi'}^{\text{even}}}, \tag{58}$$

where $\mathcal{T}_\pi$ is the poset for $\pi = (\pi_1, \pi_2)$ and $\mathcal{T}_{\pi'}$ is the partial order for $\pi' = (\pi_2', \pi_1')$. Denote the wire space of $X = A, D, D', D'', F$ by

$$\hat{X} = \mathcal{F}_X^{\mathcal{C}\cap\mathcal{T}_\pi^{\text{odd}}}, \tag{59}$$

$$\tilde{X} = \mathcal{F}_X^{\mathcal{C}\cap\mathcal{T}_{\pi'}^{\text{odd}}}. \tag{60}$$

For any wire X, we call the isomorphism between $\hat{X}$ and $\tilde{X}$, obtained by substituting t_i with t_i', the natural isomorphism.

For $\mathcal{C} \in \mathfrak{C}(\mathcal{T}_\pi)$, $\{|i\rangle_{\hat{A}}\}$ is an orthonormal base of space $\mathcal{F}_A^{\chi_\pi(\mathcal{C})}$, The Choi-Jamiołkowski (CJ) representation of the box π_1 is a sesquilinear form $R_{\pi_1}^{\mathcal{C}}$ satisfying

$$R_{\pi_1}^{\mathcal{C}}(\psi_{\hat{C}} \otimes \psi_{\hat{E}} \otimes \psi_{\hat{A}}, \varphi_{\hat{C}} \otimes \varphi_{\hat{E}} \otimes \varphi_{\hat{A}}) = \langle\psi_{\hat{C}}|\langle\psi_{\hat{E}}|\Pi_1^{\mathcal{C}}\left(|\bar{\psi}_{\hat{A}}\rangle\langle\bar{\varphi}_{\hat{A}}|\right)|\varphi_{\hat{E}}\rangle|\varphi_{\hat{C}}\rangle, \tag{61}$$

where $\Pi_1^{\mathcal{C}}$ is the CPTP map for box π_1 on cut $\mathcal{C}$ and the conjugate of $\bar{\psi}_{\hat{A}}, \bar{\varphi}_{\hat{A}}$ is taken on basis $\{|i\rangle_{\hat{A}}\}$. We only care about the effect of $R_{\pi_1}^{\mathcal{C}}$ on space $\hat{A}, \hat{C}, \hat{E}$ because of the conditions (**R1**), (**R2**) required by the comb model.

For $\mathcal{C} \in \mathfrak{C}(\mathcal{T}_{(\pi_1\|\pi_2')\theta})$, assume that the wire B, C are connected with respect to the bases $\{|k_{\hat{C}}\rangle\}, \{|l_{\hat{C}}\rangle\}$ of $\hat{C}$ and the bases $\{|k_{\hat{B}}\rangle\}, \{|l_{\hat{B}}\rangle\}$ of $\hat{B}$. The wire D, A are connected with respect to the orthonormal bases $\{|p_{\hat{D}}\rangle\}$, $\{|q_{\hat{D}}\rangle\}$ of $\hat{D}$ and the orthonormal bases $\{|p_{\hat{A}}\rangle\}$, $\{|q_{\hat{A}}\rangle\}$ of $\hat{A}$. These bases are predefined by the protocol π itself. The CJ representation of $\pi_1\pi_2$ is

$$\begin{aligned} &R_{\pi_1\pi_2}^{\mathcal{C}}(\psi_{\hat{E}} \otimes \psi_{\hat{F}}, \varphi_{\hat{E}} \otimes \varphi_{\hat{F}}) \\ &= \sum_{k,l,p,q} R_{\pi_1}^{\mathcal{C}}(k_{\hat{C}} \otimes \psi_{\hat{E}} \otimes \bar{p}_A, l_{\hat{C}} \otimes \varphi_{\hat{E}} \otimes \bar{q}_{\hat{A}}) R_{\pi_2}^{\mathcal{C}}(p_{\hat{D}} \otimes \psi_{\hat{F}} \otimes \bar{k}_{\hat{B}}, q_{\hat{D}} \otimes \varphi_{\hat{F}} \otimes \bar{l}_{\hat{B}}). \end{aligned} \tag{62}$$

For $\mathcal{C}' \in \mathfrak{C}(\mathcal{T}_{\theta_1})$, $\{|i\rangle_{\hat{C}'}\}$ is a base of space $\mathcal{F}_{C'}^{\chi_{\theta_1}(\mathcal{C}')}$, and $\{|i\rangle_{\tilde{C}''}\}$ is a base of space $\mathcal{F}_{C''}^{f_1(\chi_{\theta_1}(\mathcal{C}'))}$ such that $U_{f_1}|i\rangle_{\hat{C}} = |i\rangle_{\tilde{C}''}$ [2]. The CJ representation of the delay box θ_1 is

$$\begin{aligned} &R_{\theta_1}^{\mathcal{C}'}(\psi_{\hat{C}''} \otimes \psi_{\tilde{C}''} \otimes \alpha_{\hat{C}'}, \varphi_{\hat{C}''} \otimes \varphi_{\tilde{C}''} \otimes \beta_{\hat{C}'}) \\ &= \langle\psi_{\tilde{C}''}|\Theta_1^{\mathcal{C}'}\left(|\bar{\alpha}_{\hat{C}'}\rangle\langle\bar{\beta}_{\hat{C}'}|\right)|\varphi_{\tilde{C}''}\rangle \cdot \langle\psi_{\hat{C}''}|\Omega_{\hat{C}''}\rangle\langle\Omega_{\hat{C}''}|\varphi_{\hat{C}''}\rangle \\ &= \langle\psi_{\tilde{C}''}|\bar{\alpha}_{\tilde{C}''}\rangle\langle\bar{\beta}_{\tilde{C}''}|\varphi_{\tilde{C}''}\rangle \cdot \langle\psi_{\hat{C}''}|\Omega_{\hat{C}''}\rangle\langle\Omega_{\hat{C}''}|\varphi_{\hat{C}''}\rangle, \end{aligned} \tag{63}$$

where $\bar{\alpha}_{\tilde{C}''} \in \mathcal{F}_{C''}^{\mathcal{C}'}$ and $\bar{\alpha}_{\hat{C}'} \in \mathcal{F}_{C'}^{\chi(\mathcal{C}')}$ have the same coefficients in the bases of $\{|i\rangle_{\tilde{C}''}\}$ and $\{|i\rangle_{\hat{C}'}\}$. Since the state in space $\hat{C}''$ is always a vacuum state, we omit the arguments $\psi_{\hat{C}''}, \varphi_{\hat{C}''}$ of $R_{\theta_1^{\mathcal{C}'}}$ and the second term of Equation (63) in the remaining part of the paper.

For all $\mathcal{C} \in \mathfrak{C}(\mathcal{T}_{\pi_1\theta_1})$, wire C and C' are connected with respect to the bases $\{|k_{\hat{C}'}\rangle\}$ and $\{|l_{\hat{C}'}\rangle\}$. Then we have the isomorphisms $|k_{\hat{C}'}\rangle \cong |k_{\hat{C}}\rangle, |l_{\hat{C}'}\rangle \cong |l_{\hat{C}}\rangle$ [3]. the CJ representation of the composition box $\bar{\pi}_1 = \pi_1\theta_1$ is,

[2] This is possible because $\mathcal{F}_{C'}^{\chi_{\theta_1}(\mathcal{C}')} \simeq \mathcal{F}_{C''}^{f_1(\chi_{\theta_1}(\mathcal{C}'))}$.

[3] Since any pair of bases $\{|k_{\hat{C}'}\rangle\}$, $\{|k_{\hat{C}}\rangle\}$ defines a specific isomorphism between $\hat{C}'$ and $\hat{C}$, we use the notation $|k_{\hat{C}'}\rangle \cong |k_{\hat{C}}\rangle$ to denote this isomorphism.

$$
\begin{aligned}
&R^{\mathcal{C}}_{\bar{\pi}_1}(\gamma_{\tilde{C}''}\otimes\psi_{\hat{E}}\otimes\psi_{\hat{A}},\eta_{\tilde{C}''}\otimes\varphi_{\hat{E}}\otimes\varphi_{\hat{A}})\\
&=\sum_{k,l}R^{\mathcal{C}_1}_{\pi_1}(k_{\hat{C}}\otimes\psi_{\hat{E}}\otimes\psi_{\hat{A}},l_{\hat{C}}\otimes\varphi_{\hat{E}}\otimes\varphi_{\hat{A}})R^{\mathcal{C}_2}_{\theta_1}\left(\gamma_{\tilde{C}''}\otimes\bar{k}_{\hat{C}'},\eta_{\tilde{C}''}\otimes\bar{l}_{\hat{C}'}\right) &(64)\\
&=\sum_{k,l}R^{\mathcal{C}_1}_{\pi_1}\left(k_{\hat{C}}\otimes\psi_{\hat{E}}\otimes\psi_{\hat{A}},l_{\hat{C}}\otimes\varphi_{\hat{E}}\otimes\varphi_{\hat{A}}\right)\langle\gamma_{\tilde{C}''}|k_{\tilde{C}''}\rangle\langle l_{\tilde{C}''}|\eta_{\tilde{C}''}\rangle &(65)\\
&=R^{\mathcal{C}_1}_{\pi_1}\left(\sum_k\langle k_{\tilde{C}''}|\gamma_{\tilde{C}''}\rangle k_{\hat{C}}\otimes\psi_{\hat{E}}\otimes\psi_{\hat{A}},\sum_l\langle l_{\tilde{C}''}|\eta_{\tilde{C}''}\rangle l_{\hat{C}}\otimes\varphi_{\hat{E}}\otimes\varphi_{\hat{A}}\right) &(66)\\
&=R^{\mathcal{C}_1}_{\pi_1}\left(\gamma_{\hat{C}}\otimes\psi_{\hat{E}}\otimes\psi_{\hat{A}},\eta_{\hat{C}}\otimes\varphi_{\hat{E}}\otimes\varphi_{\hat{A}}\right), &(67)
\end{aligned}
$$

where $|\gamma_{\hat{C}}\rangle=\left(\sum_k|k_{\hat{C}}\rangle\langle k_{\tilde{C}''}|\right)|\gamma_{\tilde{C}''}\rangle$ and $|\eta_{\hat{C}}\rangle=\left(\sum_l|l_{\hat{C}}\rangle\langle l_{\tilde{C}''}|\right)|\eta_{\tilde{C}''}\rangle$. Equation (64) follows from Definition 18, Equation (65) follows from Equation (63), and Equation (66) follows from the sesquilinearity.

Similarly, for all $\mathcal{C}\in\bar{\mathfrak{C}}(\mathcal{T}_{\pi'_2\theta_2})$, wire D and D' are connected with respect to bases $\{|p_{\tilde{D}'}\rangle\}$ and $\{|q_{\tilde{D}'}\rangle\}$. The CJ representation of the box $\bar{\pi}'_2=\pi'_2\theta_2$ is

$$
\begin{aligned}
&R^{\mathcal{C}}_{\bar{\pi}'_2}\left(\lambda_{\hat{D}''}\otimes\psi_{\tilde{F}}\otimes\psi_{\tilde{B}},\omega_{\hat{D}''}\otimes\varphi_{\tilde{F}}\otimes\varphi_{\tilde{B}}\right) &(68)\\
&=R^{\mathcal{C}_1}_{\pi'_2}\left(\lambda_{\tilde{D}}\otimes\psi_{\hat{F}}\otimes\psi_{\hat{B}},\omega_{\tilde{D}}\otimes\varphi_{\hat{F}}\otimes\varphi_{\hat{B}}\right), &(69)
\end{aligned}
$$

where $|\lambda_{\tilde{D}}\rangle=\left(\sum_p|p_{\tilde{D}}\rangle\langle p_{\hat{D}''}|\right)|\lambda_{\hat{D}''}\rangle$ and $|\omega_{\tilde{D}}\rangle=\left(\sum_q|q_{\tilde{D}}\rangle\langle q_{\hat{D}''}|\right)|\omega_{\hat{D}''}\rangle$.

Notice that, for all $\mathcal{C}\in\bar{\mathfrak{C}}(\mathcal{T}_{(\pi_1\|\pi'_2)})$, we have the isomorphism chain between the wires:

$$
\begin{aligned}
&|k_{\tilde{B}}\rangle\cong|k_{\hat{B}}\rangle\cong|k_{\hat{C}}\rangle\cong|k_{\hat{C}'}\rangle\cong|k_{\tilde{C}''}\rangle,\\
&|l_{\tilde{B}}\rangle\cong|l_{\hat{B}}\rangle\cong|l_{\hat{C}}\rangle\cong|l_{\hat{C}'}\rangle\cong|l_{\tilde{C}''}\rangle,\\
&|p_{\hat{A}}\rangle\cong|p_{\tilde{A}}\rangle\cong|p_{\tilde{D}}\rangle\cong|p_{\tilde{D}'}\rangle\cong|p_{\hat{D}''}\rangle,\\
&|q_{\hat{A}}\rangle\cong|q_{\tilde{A}}\rangle\cong|q_{\tilde{D}}\rangle\cong|q_{\tilde{D}'}\rangle\cong|q_{\hat{D}''}\rangle.
\end{aligned}
\tag{70}
$$

The isomorphisms $\cong$ in the first column are natural isomorphisms. The isomorphisms in the second column are predefined by the connection of $\pi_1\pi_2$. The isomorphisms in the third column can be chosen freely; that is, they are neither predefined nor natural. The isomorphisms in the fourth column follows from the definition of delay boxes θ_1 and θ_2. Therefore, the isomorphisms in the third column induce two pairs of bases for $\tilde{B},\tilde{C}''$ and two pairs of bases for $\hat{A},\hat{D}''$, which are precisely the bases we will use for B,C'' and A,D'' connections.

Then, for $\mathcal{C}=\mathcal{T}_{(\pi_1\|\pi'_2)\theta}$, we choose the bases $\{|k\rangle_{\tilde{C}''}\},\{|l\rangle_{\tilde{C}''}\},\{|k\rangle_{\hat{B}}\},\{|l\rangle_{\hat{B}}\}$ for the connection of C'',B and the bases $\{|p_{\hat{D}''}\rangle\},\{|q_{\hat{D}''}\rangle\},\{|p_{\tilde{A}}\rangle\},\{|q_{\tilde{A}}\rangle\}$ for the connection of D'',A. The CJ representation of the final box $\bar{\pi}_1\bar{\pi}'_2$ is

$$
\begin{aligned}
&R^{\mathcal{T}_{(\pi_1\|\pi_2)\theta}}_{\bar{\pi}_1\bar{\pi}'_2}(\psi_{\hat{E}}\otimes\psi_{\tilde{F}},\varphi_{\hat{E}}\otimes\varphi_{\tilde{F}}) &(71)\\
&=\sum_{k,l,p,q}R^{\mathcal{T}_{\bar{\pi}_1}}_{\bar{\pi}_1}(k_{\tilde{C}''}\otimes\psi_E\otimes\bar{p}_A,l_{\tilde{C}''}\otimes\varphi_{\hat{E}}\otimes\bar{q}_{\hat{A}})R^{\mathcal{T}_{\bar{\pi}'_2}}_{\bar{\pi}'_2}(p_{\hat{D}''}\otimes\psi_{\tilde{F}}\otimes\bar{k}_{\tilde{B}},q_{\hat{D}''}\otimes\varphi_{\tilde{F}}\otimes\bar{l}_{\tilde{B}}) &(72)\\
&=\sum_{k,l,p,q}R^{\mathcal{T}_{\pi}}_{\pi_1}(k_{\hat{C}}\otimes\psi_E\otimes\bar{p}_A,l_{\hat{C}}\otimes\varphi_{\hat{E}}\otimes\bar{q}_{\hat{A}})R^{\mathcal{T}_{\pi'}}_{\pi'_2}(p_{\tilde{D}}\otimes\psi_{\tilde{F}}\otimes\bar{k}_{\tilde{B}},q_{\tilde{D}}\otimes\varphi_{\tilde{F}}\otimes\bar{l}_{\tilde{B}}). &(73)
\end{aligned}
$$

where $\mathcal{C}'_1=\mathcal{C}\cap\mathcal{T}_\pi$ and $\mathcal{C}'_2=\mathcal{C}\cap\mathcal{T}_{\pi'}$. R_{π_2} and $R_{\pi'_2}$ should have the same effect on their

respective wire spaces. Rigorously speaking, for natural isomorphisms

$$\begin{aligned} |p_{\tilde{D}}\rangle \cong |p_{\hat{D}}\rangle, |q_{\tilde{D}}\rangle \cong |q_{\hat{D}}\rangle, \\ |k_{\tilde{B}}\rangle \cong |k_{\hat{B}}\rangle, |l_{\tilde{B}}\rangle \cong |l_{\hat{B}}\rangle, \\ |\psi_{\tilde{F}}\rangle \cong |\psi_{\hat{F}}\rangle, |\varphi_{\tilde{F}}\rangle \cong |\varphi_{\hat{F}}\rangle, \end{aligned} \tag{74}$$

we have

$$R_{\pi_2'}^{\mathcal{T}_{\pi'}}(p_{\tilde{D}} \otimes \psi_{\tilde{F}} \otimes \bar{k}_{\tilde{B}}, q_{\tilde{D}} \otimes \varphi_{\tilde{F}} \otimes \bar{l}_{\tilde{B}}) = R_{\pi_2}^{\mathcal{T}_\pi}(p_{\hat{D}} \otimes \psi_{\hat{F}} \otimes \bar{k}_{\hat{B}}, q_{\hat{D}} \otimes \varphi_{\hat{F}} \otimes \bar{l}_{\hat{B}}). \tag{75}$$

Substituting Equation (75) into Equation (73), we have

$$R_{\bar{\pi}_1\bar{\pi}_2'}^{\mathcal{T}_{(\pi_1\|\pi_2)\theta}}(\psi_{\hat{E}} \otimes \psi_{\tilde{F}}, \varphi_{\hat{E}} \otimes \varphi_{\tilde{F}}) = R_{\pi_1\pi_2}^{\mathcal{T}_\pi}(\psi_{\hat{E}} \otimes \psi_{\hat{F}}, \varphi_{\hat{E}} \otimes \varphi_{\hat{F}}), \tag{76}$$

which concludes the proof.

B.2 Proof of Theorem 10

Theorem. *Let π be a* WCF(z, ϵ) *protocol and η be any protocol with only classical output at the outer interface. $\xi = \pi\|\eta$ is their parallel composition with the ordered set $\mathcal{T}$. Then π is globally secure in the protocol if there exists a partition $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ of $\mathcal{T}$ such that*

(C1) *$\forall t_1 \in \mathcal{T}_1, t_2 \in \mathcal{T}_2, t_3 \in \mathcal{T}_3$, $t_1 \prec t_2 \prec t_3$;*

(C2) *η only accepts input and produces output on set $\mathcal{T}_1 \cup \mathcal{T}_3$, while π only accepts input and produces output on set $\mathcal{T}_2$.*

In this proof, we focus on the first condition in Definition 9, then the second condition follows similarly.

Let α be the adversarial box connected to the parallel composition $\pi_A\|\eta_A$, as shown in Figure 9a. For convenience, c_A, K_A in Definition 9 are relabeled as E, K, respectively. The idea of this proof is by contradiction, explained as follows. Our target is to bound the conditional probability $\Pr[E = 1|K = k]$. Due to condition (**C1**) and (**C2**), the interaction of α divides into three phases (see Figure 9b). Observe that the only way that K can influence E is through the information Q_1 passed from the first phase α_1 to the second phase α_2. If the adversarial box α can bias $\Pr[E = 1|K = k]$ beyond $\frac{1}{2} + \epsilon$, then the information on Q_1 conditioned on $K = k$, together with the box α_2, becomes a successful attacking strategy for π_A alone.

We first simplify the adversarial box and prove this theorem by contradiction. Let $\mathcal{T}$ be the ordered set of $\pi_A\|\eta_A$. Without loss of generality, we can assume the final box $(\pi_A\|\eta_A)\alpha$ is defined on the ordered set $\mathcal{T}$, because any extra element t introduced by α has no effect on $\pi_A\|\eta_A$.

According to the condition (**C**1) and (**C**2), the wire (V_1, W_1), (B, D) and (V_2, W_2) are effective only on $\mathcal{T}_1$, $\mathcal{T}_2$ and $\mathcal{T}_3$, respectively. Let $\{\Phi_\alpha^{\mathcal{C}}\}_{\mathcal{C}\in\bar{\mathfrak{C}}(\mathcal{T})}$ be the set of CPTP maps corresponding to α. Since we are only interested in the final output, we set $\mathcal{C} = \mathcal{T}$. By [36, Lemma 9], the map $\Phi_\alpha^{\mathcal{T}}$ can be decomposed into three maps $\Phi_{\alpha_1}^{\mathcal{T}} : V_1 \mapsto W_1Q_1$, $\Phi_{\alpha_2}^{\mathcal{T}} : BQ_1 \mapsto DQ_2$ and $\Phi_{\alpha_3}^{\mathcal{T}} : V_2Q_2 \mapsto W_2$ that satisfy

$$\Phi_\alpha^{\mathcal{T}} = (\mathrm{id}_{W_1} \otimes \mathrm{id}_D \otimes \Phi_{\alpha_3}^{\mathcal{T}}) \circ (\mathrm{id}_{W_1} \otimes \Phi_{\alpha_2}^{\mathcal{T}} \otimes \mathrm{id}_{V_2}) \circ (\Phi_{\alpha_1}^{\mathcal{T}} \otimes \mathrm{id}_B \otimes \mathrm{id}_{V_2}). \tag{77}$$

Here $\Phi_{\alpha_1}^{\mathcal{T}}$, $\Phi_{\alpha_2}^{\mathcal{T}}$ and $\Phi_{\alpha_3}^{\mathcal{T}}$ can be seen as the map of some boxes α_1, α_2 and α_3, respectively. Similarly, the box η_A is split into η_{A1} and η_{A2}. The decomposition is illustrated in Figure 9b.

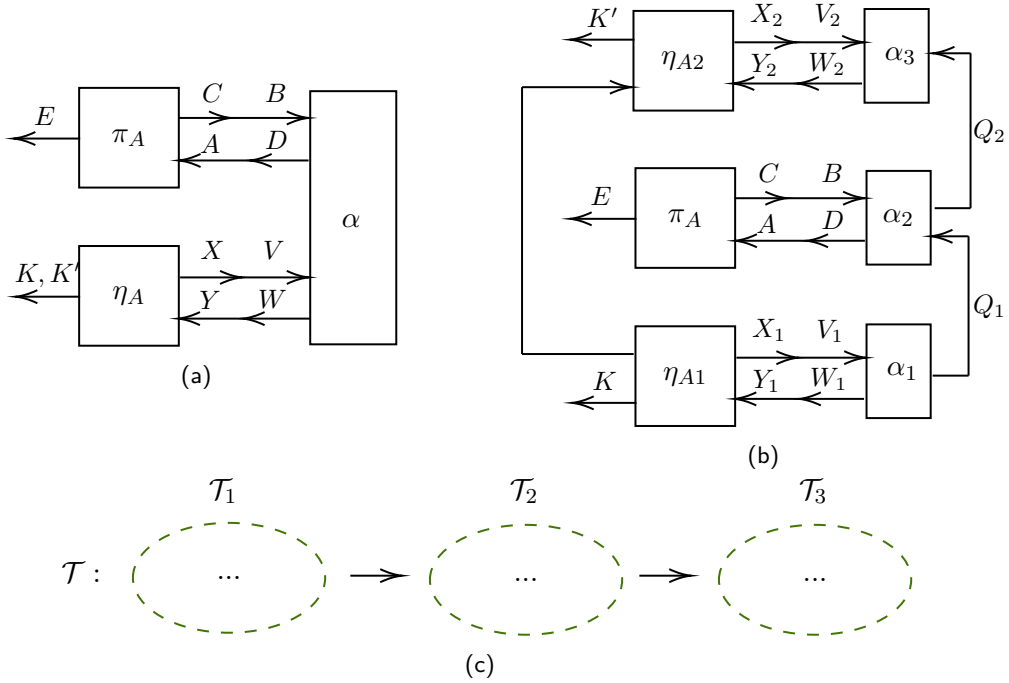

Figure 9: (a) The basic connection of box $(\pi_A \| \eta_A)\alpha$. (b) An equivalent form of the box. The wires X, Y, V, W are split into $(X_1, X_2), (Y_1, Y_2), (V_1, V_2), (W_1, W_2)$, respectively. (c) Causal order of box $(\pi_A \| \eta_A)\alpha$. The sets $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ as a whole are strictly ordered.

Let $\Phi^{\mathcal{T}}_{\eta_A\alpha_1}$ and $\Phi^{\mathcal{T}}_{\pi_A\alpha_2}$ be the map of connected boxes $\eta_A\alpha_1$ and $\pi_A\alpha_2$. Denote $\bar{Q} = \mathcal{F}^{\mathcal{T}}_{Q}$, then the output of $\Phi^{\mathcal{T}}_{\eta_A\alpha_1}$ is a classical-quantum state $\rho_{\bar{Q}K} = \sum_k P_K(k)|k\rangle\langle k| \otimes \rho^k_{\bar{Q}}$. $\Phi^{\mathcal{T}}_{\pi_A\alpha_2}$ is a map from $\mathfrak{T}(\bar{Q})$ to the classical bit E, which can be represented as a binary POVM $\{M_0, M_1\}$. Then the conditional probability is $P_{E|K}(e|k) = \mathrm{tr}(M_e\rho^k_{\bar{Q}})$.

Now we are ready to prove the theorem by contradiction. Assume $\exists k \in \mathbb{N}, \Pr[E = 1|K = k] \geq z + \epsilon$, then $\mathrm{tr}(M_e\rho^k_{\bar{Q}}) \geq z + \epsilon$. Consider a box γ that outputs state $\rho^k_{\bar{Q}}$ and has no input. The box $\pi_A\alpha_2\gamma$ will output $E = 1$ with probability larger than $z + \epsilon$, which contradicts the stand-alone security. Therefore, the first condition in Definition 9 is satisfied.

B.3 Proof of Corollary 11

Corollary. *Let $z \in [0, \frac{1}{2}]$. The unbalanced WCF protocol shown in Figure 7 is a* $\mathrm{WCF}(z, \epsilon')$ *protocol with $\epsilon' = 2\epsilon + o(\epsilon)$.*

The intuition for the proof of Corollary 11 is as follows. The probability of one party ultimately winning is a continuous function of the probabilities of winning in each round. Thus, a small bias in each round necessarily leads to a small overall bias.

Denote the fractional part of z as a binary string b_1^n (with finite precision), that is, $z = 0.b_1b_2\ldots b_n$. Define the sets $I := \{i \in [n] \mid b_i = 0\}$ and $I' := \{i \in [n] \mid b_i = 1\}$. The elements of I and I' form the sequences $(a_1, \ldots, a_{|I|})$ and $(a'_1, \ldots, a'_{|I'|})$, respectively, arranged in ascending order. The ith WCF protocol π_i as well as the other WCF protocols $\pi_1\|\ldots\|\pi_{i-1}$ and $\pi_{i+1}\|\ldots\|\pi_n$ output classical bits and follow strict temporal orders. Therefore, for $i = 2, 3, \ldots, n$ and any bit sequence c_1^{i-1}, we have global security of π_i according

to Theorem 10:

$$\Pr\left[C_{A,i}=1|C_{A,1}^{i-1}=c_1^{i-1}\right]\leq\frac{1}{2}+\epsilon, \tag{78}$$

$$\Pr\left[C_{B,i}=0|C_{B,1}^{i-1}=c_1^{i-1}\right]\leq\frac{1}{2}+\epsilon, \tag{79}$$

where $C_{B(A),1}^{i}=C_{B(A),1}C_{B(A),2}\ldots C_{B(A),i}$.

We first argue that a cheating party needs to maximize the winning probability of each game π_i in order to maximize the final winning probability. At each step π_i, if $b_i=0$, Bob wins the final game with certainty if $C_{A,i}=1$ and wins the final game with a probability smaller than 1 if $C_{A,i}=0$; if $b_i=1$, Bob wins with non-zero probability if $C_{A,i}=0$ while loses with certainty if $C_{A,i}=1$. Therefore, a cheating Bob strives to win at each round of π_i in order to finally win with the highest probability. The similar argument holds for cheating Alice. In conclusion, Bob's winning probability is no larger than the case when

$$\forall i\in[n],\Pr\left[C_{A,i}=1|C_{A,1}^{i-1}=b_1^{i-1}\right]=\frac{1}{2}+\epsilon, \tag{80}$$

and Alice's winning probability is no larger than the case when

$$\forall i\in[n],\Pr\left[C_{B,i}=0|C_{B,1}^{i-1}=b_1^{i-1}\right]=\frac{1}{2}+\epsilon. \tag{81}$$

We will use the above probabilities to compute the upper bound on Alice and Bob's optimal winning probability.

According to the program of τ_A in Figure 7, Bob can win the final game only if the loop breaks at the ath round where $b_a=0$, or equivalently, $a\in I$. Then, his winning probability can be derived as

$$\Pr[\text{Bob wins}]=\sum_{a\in I}\Pr[\text{Loop breaks at } a\text{th round and } C_{A,a}=1] \tag{82}$$

$$=\sum_{i=1}^{|I|}\Pr\left[C_{A,1}^{a_i}=(b_1^{a_i-1},1)\right] \tag{83}$$

$$=\sum_{i=1}^{|I|}\Pr\left[C_{A,a_i}=1|C_{A,1}^{a_i-1}=b_1^{a_i-1}\right]\cdot\prod_{j=1}^{a_i-1}\Pr\left[C_{A,j}=b_j|C_{A,1}^{j-1}=b_1^{j-1}\right] \tag{84}$$

$$=\sum_{i=1}^{|I|}\Pr\left[C_{A,a_i}=1|C_{A,1}^{a_i-1}=b_1^{a_i-1}\right]\cdot\prod_{j\in\{a_k\}_{k=1}^{i-1}}\Pr\left[C_{A,j}=0|C_{A,1}^{j-1}=b_1^{j-1}\right]\cdot$$
$$\prod_{j'\in[a_i-1]\setminus\{a_k\}_{k=1}^{i-1}}\Pr\left[C_{A,j'}=0|C_{A,1}^{j'-1}=b_1^{j'-1}\right] \tag{85}$$

$$\leq\sum_{i=1}^{|I|}\left(\frac{1}{2}+\epsilon\right)^{a_i-i+1}\left(\frac{1}{2}-\epsilon\right)^{i-1}, \tag{86}$$

where $C_{A,1}^{0}=b_1^0$ is defined as a certain event and Inequality (86) follows from Inequal-

ity (78) and (80). Similarly, for cheating Alice, we obtain

$$\Pr[\text{Alice wins}] = \sum_{i=1}^{|I'|} \Pr\left[C_{B,1}^{a'_i} = (b_1^{a'_i-1}, 0)\right] \tag{87}$$

$$= \sum_{i=1}^{|I'|} \Pr\left[C_{B,a'_i} = 0 | C_{B,i}^{a'_i-1} = b_1^{a'_i-1}\right] \prod_{j=1}^{a'_i-1} \Pr\left[C_{B,j} = b_j | C_{B,1}^{j-1} = b_1^{j-1}\right] \tag{88}$$

$$\leq \sum_{i=1}^{|I'|} \left(\frac{1}{2} + \epsilon\right)^{a'_i-i+1} \left(\frac{1}{2} - \epsilon\right)^{i-1}, \tag{89}$$

Then the bias achieved by Bob is

$$\epsilon'_B = |\Pr[\text{Bob wins}] - (1-z)| \tag{90}$$

$$\leq \sum_{i=1}^{|I|} \left(\frac{1}{2} + \epsilon\right)^{a_i-i+1} \left(\frac{1}{2} - \epsilon\right)^{i-1} - \frac{1}{2^{a_i}} \tag{91}$$

$$\leq \sum_{i=1}^{|I|} \frac{2(a_i - 2i + 2)}{2^{a_i}} \epsilon + o(\epsilon). \tag{92}$$

We have omitted the absolute value because the winning probability of a cheating Bob is always larger than that of an honest Bob, $\Pr[\text{Bob wins}] \geq 1 - z$. Note that

$$\sum_{n=i}^{\infty} \frac{n}{2^n} = \frac{i+1}{2^{i-1}}. \tag{93}$$

When $|I| = 1$,

$$\epsilon'_B \leq \frac{2a_1}{2^{a_1}} \epsilon + o(\epsilon) \leq \epsilon + o(\epsilon). \tag{94}$$

When $|I| \geq 2$,

$$\epsilon'_B \leq \frac{2a_1}{2^{a_1}} \epsilon + \frac{1}{2} \sum_{i=2}^{|I|} \frac{(a_i - 2)}{2^{a_i-2}} \epsilon + o(\epsilon) \leq \frac{2a_1}{2^{a_1}} \epsilon + \frac{1}{2} \sum_{i=2}^{\infty} \frac{i-2}{2^{i-2}} \epsilon + o(\epsilon) \leq 2\epsilon + o(\epsilon). \tag{95}$$

In conclusion, for cheating Bob,

$$\epsilon'_B = |\Pr[\text{Bob wins}] - (1-z)| \leq 2\epsilon + o(\epsilon). \tag{96}$$

Similarly, for cheating Alice,

$$\epsilon'_A = |\Pr[\text{Alice wins}] - z| \leq 2\epsilon + o(\epsilon). \tag{97}$$

The final bias is

$$\epsilon' = \max\{\epsilon'_A, \epsilon'_B\} \leq 2\epsilon + o(\epsilon). \tag{98}$$