Physics Letters A 377 (2013) 1076–1087

Contents lists available at SciVerse ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

A short impossibility proof of quantum bit commitment

Giulio Chiribella [c,1], Giacomo Mauro D'Ariano [a,b,*,1], Paolo Perinotti [a,b,1], Dirk Schlingemann [d], Reinhard Werner [e]

[a] QUIT group, Dipartimento di Fisica, via Bassi 6, 27100 Pavia, Italy
[b] INFN Gruppo IV, Sezione di Pavia, via Bassi, 6, 27100 Pavia, Italy
[c] Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, China
[d] ISI Foundation, Quantum Information Theory Unit, Viale S. Severo 65, 10133 Torino, Italy
[e] Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstrasse 2, 30167 Hannover, Germany

ARTICLE INFO

Article history:
Received 11 February 2013
Accepted 25 February 2013
Available online 28 February 2013
Communicated by P.R. Holland

Keywords:
Quantum protocols
Quantum combs
Quantum bit commitment

ABSTRACT

Bit commitment protocols, whose security is based on the laws of quantum mechanics alone, are generally held to be impossible on the basis of a concealment–bindingness tradeoff (Lo and Chau, 1997 [1], Mayers, 1997 [2]). A strengthened and explicit impossibility proof has been given in D'Ariano et al. (2007) [3] in the Heisenberg picture and in a C*-algebraic framework, considering all conceivable protocols in which both classical and quantum information is exchanged. In the present Letter we provide a new impossibility proof in the Schrödinger picture, greatly simplifying the classification of protocols and strategies using the mathematical formulation in terms of quantum combs (Chiribella et al., 2008 [4]), with each single-party strategy represented by a *conditioned comb*. We prove that assuming a stronger notion of concealment—for each classical communication history, not in average—allows Alice's cheat to pass also the worst-case Bob's test. The present approach allows us to restate the concealment–bindingness tradeoff in terms of the continuity of dilations of probabilistic quantum combs with the metric given by the comb discriminability-distance.

1. Introduction

The bit commitment protocol involves two mistrustful parties—Alice and Bob—of which Alice submits to Bob a piece of evidence to be used to confirm a bit value which she will later reveal to Bob, while Bob cannot determine the bit value from the evidence alone. A good bit commitment protocol should be simultaneously *concealing* and *binding*, namely the evidence should be submitted to Bob in such a way that he has (almost) no chance to identify the committed bit value before Alice later decodes it for him, whereas Alice has (almost) no way of changing the value of the committed bit once she has submitted the evidence. In the easiest example to illustrate bit commitment, Alice writes the bit down on a piece of paper, which is then locked in a safe and sent to Bob, whereas Alice keeps the key. At a later time, she will unveil the bit by handing over the key to Bob. However, Bob may be able to open the safe in the meantime, and this scheme is in principle insecure. Yet all bit commitment schemes currently used rely on strongboxes and keys made of computations that are (supposedly) hard to perform (see Ref. [3] for a list of references), and cryptographers have long known that bit commitment (like any other interesting two-party cryptographic primitive) cannot be securely implemented with classical information [5].

Besides having immediate practical applications, bit commitment is also a very powerful cryptographic primitive. Conceived by Blum [6] as a building block for secure coin tossing, it also allows to implement secure oblivious transfer [7–9], which, in turn, is sufficient to establish secure two-party computation [5,10].

It has therefore been a long-time challenge for quantum cryptographers to find *unconditionally secure* quantum bit commitment protocols, in which—very much in parallel to quantum key distribution [11,12]—security is guaranteed by the laws of quantum physics alone.

The first quantum bit commitment protocol appeared in the famous Bennett and Brassard 1984 quantum cryptography paper [11], in a version for implementing coin tossing. However, they also proved that Alice can cheat using EPR correlations, by which she can unveil either bit at the opening stage by measuring in the appropriate basis a particle entangled with the one encoding the bit, whereas Bob has no way to detect the attack. Subsequent

* Corresponding author at: QUIT group, Dipartimento di Fisica, via Bassi 6, 27100 Pavia, Italy.
E-mail addresses: gchiribella@mail.tsinghua.edu.cn (G. Chiribella), dariano@unipv.it (G.M. D'Ariano), paolo.perinotti@unipv.it (P. Perinotti), d.schlingemann@tu-bs.de (D. Schlingemann), Reinhard.Werner@itp.uni-hannover.de (R. Werner).
1 http://www.quantummechanics.it.

0375-9601/$ – see front matter
http://dx.doi.org/10.1016/j.physleta.2013.02.045

proposals for bit commitment schemes tried to evade this type of attack, *e.g.* in the protocol of Ref. [13] which for a while was generally accepted to be unconditionally secure.

In 1996 Lo and Chau [1], and Mayers [2] realized that all previously proposed bit commitment protocols were vulnerable to a generalized version of the EPR attack that renders the [11] proposal insecure, a result that they slightly extended to cover quantum bit commitment protocols in general. Their basic argument is the following. At the end of the commitment phase, Bob will hold one out of two quantum states ϱ_k as proof of Alice's commitment to the bit value $k \in \{0, 1\}$. Alice holds its purification ψ_k, which she will later pass on to Bob to unveil. For the protocol to be concealing, the two states ϱ_k should be (almost) indistinguishable, $\varrho_0 \approx \varrho_1$. But Uhlmann's theorem [14] then implies the existence of a unitary transformation U that (nearly) rotates the purification of ϱ_0 into the purification of ϱ_1. Since U is localized on the purifying system only, which is entirely under Alice's control, Lo–Chau–Mayers argue that Alice can switch at will between the two states, and is not in any way bound to her commitment. As a consequence, any concealing bit commitment protocol is argued to be necessarily non-binding (these results still hold true when both parties are restricted by superselection rules [15]). So while the proposed quantum bit commitment protocols offer good practical security on the grounds that Alice's EPR attack is hard to perform with current technology, none of them is unconditionally secure.

Starting from 2000 the Lo–Chau–Mayers no-go theorem [1,2] has been continually challenged by Yuen and others [16–18], arguing that the impossibility proof or Ref. [1] does not exhaust all conceivable quantum bit commitment protocols, whereas it is still unclear if Mayer's framework [2] is complete. Spekkens and Rudolph [19] extended the no-go theorem with quantitative bounds (which can be saturated) on the degree of concealment and bindingness that can be achieved simultaneously in any bit commitment protocol. This impossibility proof is complete for all protocols that do not use classical communication, whence involving strategies that can be completely purified.[2] The protocols that have been claimed to circumvent the no-go theorem [16] strengthen Bob's position with the help of 'secret parameters' or 'anonymous states', so that Alice lacks some information needed to cheat successfully: while Uhlmann's theorem would still imply the existence of a unitary cheating transformation as described above, this transformation might be unknown to Alice.

The above attempts to build up a secure quantum bit commitment protocol have motivated the thorough analysis of Ref. [3], which provided a strengthened and explicit impossibility proof exhausting all conceivable protocols in which not only quantum information, but also classical information (*i.e.* publicly known) is exchanged between the two parties, including the possibility of protocol aborts and resets. The proof [3] encompasses protocols even with unbounded number of communication rounds (it is only required that the expected number of rounds is finite), and with quantum systems on infinite-dimensional Hilbert spaces. However, the considerable length of the proof in Ref. [3] makes it still hard to follow (see *e.g.* comments in Ref. [17]), lacking a synthetic intuition of the impossibility proof.

The debate can be only settled with an appropriate formulation of the problem, which is sufficiently powerful to include all possible protocols in a single simple mathematical object, thus leaving no shadow of doubt on the completeness of the protocol classification. Once the mathematical formulation of all protocols is settled,

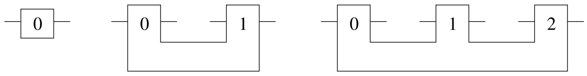

Fig. 1. Illustration of the diagrammatic representation of quantum combs. For a quantum comb each line entering or exiting a comb tooth represents a quantum system, while for a conditioned comb it represents a hybrid quantum–classical system. A quantum operation (the box on the left corner) is a special case of quantum comb with a single tooth.

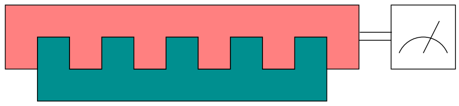

Fig. 2. A two-party protocol in which classical and quantum information are exchanged assigns the set of allowed conditioned combs, along with the pertaining input–output structure. A conditioned comb is a collection of quantum combs labeled by histories of classical communication, each quantum comb representing a specific sequence of single-party moves for a particular classical history. Each tooth of a comb corresponds to a single turn of the protocol, the last one representing the last turn in the commitment phase. For histories ending in a successful commitment, at the opening Bob performs a joint measurement on all the systems available to him. Combining Bob's comb before the opening with this final measurement yields a special case of quantum comb—the so-called *quantum tester*—whose output is the committed bit value. In this framework, Alice's comb plays the role of a "state" encoding the bit value, whereas Bob's tester plays the role of a "POVM" for binary discrimination. Such binary discrimination—prescribed by the protocol at its end—should not be confused with Bob's attempts to discriminate Alice's strategies before the opening, whose outcomes can be included in the classical information history.

then the impossibility statement becomes just a mathematical theorem. In this Letter we will first see that the appropriate notion to describe all individual strategies in a purely quantum protocol is the *quantum comb*. The quantum comb generalizes the notion of quantum operation of Kraus [20], and has been originally introduced in Ref. [4] to describe quantum *circuit boards*, where inputs and outputs are not just quantum states, but quantum operations themselves. Since quantum combs are in one-to-one correspondence with sequences of quantum operations [4,21], a quantum comb is suited to represent the sequence of moves performed by a party in a multi-round quantum protocol. Indeed, the same mathematical structure of quantum combs has been recognized by Gutoski and Watrous in Ref. [22] as the appropriate formulation of multi-round quantum games. In order to treat protocols that involve both quantum and classical communication, we will then extend this framework by introducing the concept of *conditioned comb*, which describes a computing network that is able to sequentially process both quantum and classical information.

Examples of combs are represented diagrammatically in Fig. 1. For a purely quantum comb, each line entering or exiting a tooth of the comb represents a quantum system. For a conditioned comb, each line represents a hybrid quantum–classical system, accounting also for classical information exchanged at each step. In a two-party protocol, a comb represents a single-party strategy, with each tooth of the comb representing the move performed by the party at some turn. Subsequent turns are represented by subsequent teeth, from left to right. The output of the multi-round protocol is given by two combs interlaced as in Fig. 2—the upper Bob's, the lower Alice's. The exchange of quantum–classical systems can be mathematically described in a C*-algebraic representation of a deterministic comb, or, equivalently, by treating the conditioned comb as a collection of (purely quantum) probabilistic combs, each of them being labeled by a particular history of classical communication. In this Letter, we will choose the second point of view, which avoids using the C*-algebraic framework, with the need, however, of considering collections of probabilistic quantum

[2] Notice that here the term *strategy* simply refers to a choice of parameters and actions that are allowed by the protocol (honest strategy) or not (dishonest strategy). This terminology is quite standard in cryptography literature, and should not be interpreted in a game-theoretical fashion.

combs, accounting for the classical information coming from measurements.

A protocol assigns the set of allowed strategies, *i.e.* the set of allowed conditioned combs, along with the pertaining input–output structure regulating the exchange of quantum and classical information. As already mentioned, a conditioned comb is a collection of probabilistic quantum combs, each of them representing the sequence of single-party moves associated to a particular history of classical communication. In a general protocol, some histories will lead to a successful commitment, while some other will possibly lead to an *abortion*, in which the two parties irrevocably give up, excluding any further communication (if the protocol is restarted, then the concatenation of the two sequences can be regarded as part of a new longer protocol with possible *resets*). Accordingly, we will consider histories from the beginning to the end of the commitment (which can be either successful or not), *i.e.* excluding the opening. Each tooth of a comb corresponds to a single turn of the protocol, and, in the case of successful commitment, the last tooth represents the last turn before the opening.

For histories that end in a successful commitment, in the opening Alice will send to Bob a classical message along with a set of ancillae prescribed by the protocol, and, Bob will perform a suitable joint measurement on all quantum systems available to him, as in Fig. 2. The combination of Bob's comb (up to the opening) with the final measurement at the opening is itself a special case of quantum comb—the so-called *quantum tester*—whose output is the committed bit value. In this framework, Alice's comb plays the role of a "state" encoding the bit value, whereas Bob's tester plays the role of a "POVM" for binary discrimination. Such binary discrimination—prescribed by the protocol at its end—should not be confused with Bob's attempts to discriminate Alice's strategies before the opening, whose outcomes can be included in the classical information history. We will see that the fact that the protocol has many rounds actually can help Bob in discriminating between different Alice's strategies. Thus, the probability of Bob cheating—which in a protocol with a single Bob–Alice–Bob round would be represented by the CB-norm distance between channels—here is replaced by the *comb distance* [23], which is larger than the CB-norm, since Bob can exploit the memory structure of Alice's strategy.

In the following we will consider the concealment–bindingness tradeoff for any possible history of classical information exchanged within the protocol. This will allow us to restate the tradeoff in terms of a mathematical theorem assessing the continuity of dilations of probabilistic quantum combs with the norm given defined in terms of the comb discriminability-distance. The dilation theorem shows that any probabilistic combs can be dilated to a single contraction V (*i.e.* $V^\dagger V \leqslant I$), upon introducing some additional ancillae. As a consequence, the impossibility proof will run essentially as follows. At the end of the commitment phase (which is located just before the last teeth of both parties) Bob sees one out of two possible Alice's strategies that are (almost) indistinguishable. Instead, at the opening, the two dilated strategies of Alice corresponding to the two values of the committed bit are (almost) perfectly discriminable. As a consequence of indistinguishability up to the commitment phase, Alice can choose between the two strategies by performing a unitary transformation on the ancilla in the last tooth of her comb. Therefore, one has (almost) perfect opening, and, at the same time, Alice can cheat perfectly. The concealment–bindingness tradeoff is thus reduced to the continuity of the dilation of probabilistic combs in terms of their discriminability-distance. In the present Letter we will restrict to finite-dimensional protocols, with finite-number of rounds. The last assumption does not introduce any practical limitation, since, in the real world one needs to put a bound anyway to the lapse of time needed for the commitment. We will anyway discuss also protocols with unbounded number of rounds in the concluding section.

Before starting the main sections of the Letter, we want to compare the present approach with that of the previous impossibility proof in Ref. [28]. Ref. [28] treats the strategies as the preparation of a quantum register, and classical and quantum communications are described in the Heisenberg picture in the field framework of C^*-algebras. In the present approach the C^*-algebraic framework is avoided, by treating classical histories as labels for sequences of quantum operations in the Schrödinger picture, and strategies are identified with conditioned quantum combs, which provide a direct mathematical formulation of the causal structure of the strategy. At this level the two approaches are fully equivalent. There are, however, conceptual differences, for which the two approaches are not equivalent. The most relevant difference is the notion of security, which in the present treatment is taken at the strongest level, *i.e.* worst-case over all classical histories, whereas in Ref. [28] security was defined in average. The present notion of security is cryptographically the strongest and indeed the true practical one, corresponding to a priceless commitment bit, as already stressed in Refs. [16,17]. Another important difference between the present approach and that of Ref. [28] is a more general impossibility proof, in which one can restrict the set of possible Bob's operations, even though he can always purify (*i.e.* the set is a convex set closed under dilations). This makes the impossibility proof more general, including the case of a Bob constrained by a checking Alice.

The Letter is organized as follows. In Section 2 we review the definition and the main features of a quantum protocol for bit commitment, giving its mathematical formulation in terms of quantum combs, and defining what a successful bit commitment protocol would have to achieve. The analysis will be based solely on the principles of quantum mechanics, including classical physics, but not including relativistic constraints, which are known to facilitate secure bit commitment [24,25]. In Section 3 we will briefly recall the prerequisites about quantum combs, including the notion of quantum tester, the comb distance, and we provide the generalized Stinespring dilation theorem for probabilistic combs, along with a continuity theorem for the comb distance. In Section 4 we review the quantum bit commitment protocol, and present its mathematical formulation in terms of quantum combs, restating the impossibility theorem by means of a continuity theorem for the generalized Stinespring dilation of probabilistic combs versus their comb distance. Section 6 concludes the Letter with some comments and a summary of the main results.

2. What is a protocol

A protocol regulates the exchange of messages between Alice and Bob, such that at every stage it is clear what type of message is expected from the participants, although, of course, their content is not fixed. The expected message types can be either classical or quantum or a combination thereof, with the number of distinguishable classical signals and the dimension of the Hilbert spaces fixed. The number of classical states and the dimension of the Hilbert spaces can depend on classical information generated previously.

2.1. Phases of the protocol

In any commitment scheme, we can distinguish two main phases. The first is the *commitment phase*, in which Alice and Bob exchange classical and quantum messages in order to commit the bit. Eventually, this phase can end either with a successful commitment, or with an abort, in which the two party irrevocably give up the purpose of committing the bit (of course, in a well-designed

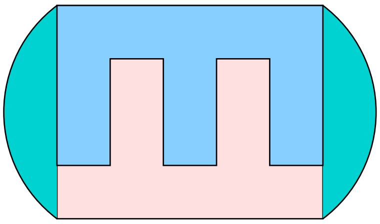

Fig. 3. The bit commitment protocol is two-party only, and trusted third parties are not allowed. Here in figure trusted rounded portions represent examples of third parties, *e.g.* the left one could be a trusted joint state, and the right one a trusted joint measurement. Another example of third party could be a third comb interlaced with Alice's and Bob's.

protocol, the probability of abort should be vanishingly small). If no abort took place, the bit value is considered to be committed to Bob but, supposedly, concealed from him. Since bit commitment is a two-party protocol and trusted third parties are not allowed, the starting state necessarily has to be originated by one of the two parties (see also Fig. 3). Moreover, since we can always include in the protocol null steps (in which no information, classical or quantum, is exchanged), without loss of generality, we can restrict our attention to protocols that are started by Bob.

The second phase is the *opening phase*. In the case of abort during the commitment, this is just a null step, whereas, in the case of successful commitment, at the opening Alice will send to Bob some classical or quantum information in order to reveal the bit value. Taking both Alice's message and his own (classical and quantum) records, Bob will then perform a suitable *verification measurement*. His measurement will result in either a successful readout of the committed bit, or in a failure, *e.g.* due to the detection of an attempted cheat. Again, in a well-designed protocol the probability of failure should be vanishingly small.

2.2. Conditions on successful protocols

In the following we will denote by a_0 and a_1 two honest strategies corresponding to the two bit values 0 and 1, respectively. We call a protocol *ε-concealing*, if, conditioned by any history of classical communication, Bob cannot distinguish between the strategies a_0 and a_1 (up to an error ε) before Alice opens the commitment. In general, of course, the probability of a given history of classical communication depends on whether Alice chooses a_0 or a_1. Since this dependence can be exploited by Bob to infer the bit value, we must require that, no matter what strategy b Bob uses, the conditioned probability of a_0 given history s never differs from the probability of a_1 given history s by more than ε. Note that this requirement must by satisfied even by histories that end up in an abort, otherwise, by the sole fact that the protocol aborted Bob could reliably infer the value of the bit.

We say that an Alice's strategy $a^\sharp$ is *δ-close* to a if, conditioned by any history of classical communication, Bob cannot distinguish a from $a^\sharp$ (up to an error δ) at any time, including the opening phase. Given two honest strategies a_0 and a_1, a *δ-cheating* is a pair of strategies $a_0^\sharp$ and $a_1^\sharp$, with the properties that (i) $a_i^\sharp$ is δ-close to a_i for $i = 0, 1$ and (ii) Alice can turn $a_0^\sharp$ into $a_1^\sharp$ with a local operation on her ancillae after the end of the commitment phase. In other words, the strategies $a_0^\sharp$ and $a_1^\sharp$ are the same throughout the commitment phase, and differ only by a local operation carried out before the opening. If no δ-cheating strategy exists for Alice, we call the protocol δ-binding.

3. Prerequisites on quantum combs

Here we briefly summarize the formalism of quantum combs and few related results.

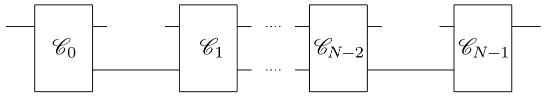

Fig. 4. N-comb: sequential network of N quantum operations with memory. The network contains input and output systems (free wires in the diagram), as well as internal memories (wires connecting the boxes).

3.1. Choi–Jamiołkowski operators and link product

A quantum operation (trace non-increasing CP-map) $\mathscr{C}$ from states on $\mathcal{H}_i$ to states on $\mathcal{H}_j$ is described by its Choi–Jamiołkowski operator

$$C = (\mathscr{C} \otimes \mathscr{I}_i)\big(|I_i\rangle\rangle\langle\langle I_i|\big) \in \mathsf{Lin}(\mathcal{H}_j \otimes \mathcal{H}_i), \tag{1}$$

where $\mathscr{I}_i$ is the identity map on $\mathcal{H}_i$, and $|I_i\rangle\rangle \in \mathcal{H}_i^{\otimes 2}$ is the maximally entangled vector $|I_i\rangle\rangle = \sum_n |n\rangle|n\rangle$. By Choi's theorem, the map $\mathscr{C}$ is CP if and only if the Choi–Jamiołkowski operator is positive (semidefinite). In general, we will often exploit the one-to-one correspondence between bipartite states in $|F\rangle\rangle \in \mathcal{H}_j \otimes \mathcal{H}_i$ and operators F from $\mathcal{H}_i$ to $\mathcal{H}_j$ given by

$$|F\rangle\rangle = (F \otimes I_i)|I_i\rangle\rangle, \tag{2}$$

and the useful relation

$$(F \otimes I_i)|I_i\rangle\rangle = \big(I_j \otimes F^\tau\big)|I_j\rangle\rangle, \tag{3}$$

F^τ denoting the transpose of F with respect to the orthonormal basis $\{|n\rangle\}$. If $\mathscr{C}$ is a quantum operation from $\mathcal{H}_i$ to $\mathcal{H}_j$ and $\mathscr{D}$ is a quantum operation from $\mathcal{H}_j$ to $\mathcal{H}_k$, the Choi–Jamiołkowski operator of the quantum operation $\mathscr{D}\mathscr{C}$, from $\mathcal{H}_i$ to $\mathcal{H}_k$, resulting from the connection of $\mathscr{C}$ and $\mathscr{D}$ is given by the *link product* [4]

$$D * C := \mathrm{Tr}_j\big[(D \otimes I_i)\big(I_k \otimes C^{\tau_j}\big)\big], \tag{4}$$

Tr_j and τ_j denoting partial trace and partial transpose on $\mathcal{H}_j$, respectively. A quantum operation $\mathscr{C}$ is trace-preserving (*i.e.* it is a channel) if and only if it satisfies the normalization condition

$$I_j * C \equiv \mathrm{Tr}_j[C] = I_i. \tag{5}$$

Viewing quantum states as a special kind of channels (with one-dimensional input space), Eq. (4) yields

$$\mathscr{C}(\rho) = C * \rho = \mathrm{Tr}_i\big[C\big(I_j \otimes \rho^\tau\big)\big]. \tag{6}$$

3.2. Quantum combs

A quantum comb describes a sequential network of N quantum operations with memory $(\mathscr{C}_k)_{k=0}^{N-1}$, with $N-1$ open slots in which variable quantum operations can be inserted, as in Fig. 4. The comb is in one-to-one correspondence with the Choi–Jamiołkowski operator R of the network, which can be computed as the link product of the Choi–Jamiołkowski operators $(C_k)_{k=0}^{N-1}$:

$$R := C_{N-1} * \cdots * C_0. \tag{7}$$

Labeling the input (output) spaces of $\mathscr{C}_k$ as $\mathcal{H}_{2k}$ ($\mathcal{H}_{2k+1}$), we have that R is a non-negative operator on $\bigotimes_{j=0}^{2N-1} \mathcal{H}_j$.

For networks of channels the operator R has to satisfy the recursive normalization condition [4,22]

$$\mathrm{Tr}_{2k-1}\big[R^{(k)}\big] = I_{2k-2} \otimes R^{(k-1)}, \quad k = 1, \ldots, N, \tag{8}$$

where $R^{(N)} := R$, $R^{(k)} \in \mathsf{Lin}(\bigotimes_{j=0}^{2k-1} \mathcal{H}_j)$, and $R^{(0)} = 1$. Moreover, one has the characterization [4,21]

Theorem 1. *Any positive operator R satisfying Eq. (8) is the Choi–Jamiołkowski operator of a network of N channels. Any positive operator R' such that $R' \leqslant R$ is the Choi–Jamiołkowski operator of a network of N quantum operations.*

We call a quantum comb R satisfying Eq. (8) *deterministic*, and a comb $R' \leqslant R$ *probabilistic*.

3.3. Dilation of quantum combs

By the Stinespring–Kraus–Ozawa theorem [26,20,27], any quantum operation $\mathscr{C}$ from states on $\mathcal{H}_i$ to $\mathcal{H}_j$ can be dilated to an isometric map followed by a post-selection on an ancilla

$$\mathscr{C}(\rho) = \mathrm{Tr}_A\big[(I \otimes P_A) V \rho V^\dagger\big] = \mathrm{Tr}_A\big[K \rho K^\dagger\big], \quad K = (I \otimes P_A) V, \tag{9}$$

with V isometry from $\mathcal{H}_i$ to $\mathcal{H}_j \otimes \mathcal{H}_A$, and P_A orthogonal projector on the Hilbert space $\mathcal{H}_A$ of the ancilla.

We refer to the single-Kraus map

$$\widetilde{\mathscr{C}}(\rho) := K \rho K^\dagger \tag{10}$$

as to a *dilation* of the quantum operation $\mathscr{C}$. In terms of Choi–Jamiołkowski operators, one has

$$C = \mathrm{Tr}_A[\widetilde{C}] \in \mathsf{Lin}(\mathcal{H}_j \otimes \mathcal{H}_i), \tag{11}$$

where $\widetilde{C} = |K\rangle\rangle\langle\langle K|$ is the Choi–Jamiołkowski operator of the dilation. A (minimal) dilation of the quantum operation $\mathscr{C}$ has ancilla space $\mathcal{H}_A \simeq \mathsf{Supp}(C) \subseteq \mathcal{H}_j \otimes \mathcal{H}_i := \mathcal{H}_{ij}$, and Choi–Jamiołkowski operator

$$\widetilde{C} = \big|C^{\frac{1}{2}}\big\rangle\big\rangle\big\langle\big\langle C^{\frac{1}{2}}\big| \in \mathsf{Lin}(\mathcal{H}_{ij} \otimes \mathcal{H}_A). \tag{12}$$

In particular, when the quantum operation is a quantum channel also its dilation is a channel—$\widetilde{\mathscr{C}}(\rho) = V \rho V^\dagger$, V isometry—with the Choi–Jamiołkowski operator satisfying the normalization condition $\mathrm{Tr}_{A,j}[\widetilde{C}] = I_i$.

Since a quantum comb $R \in \mathsf{Lin}(\mathcal{H})$ with $\mathcal{H} = \bigotimes_{j=0}^{2N-1} \mathcal{H}_j$ represents a sequential network of quantum operations, one can always obtain a dilation of the comb by dilating each quantum operation in the network. A useful dilation of R is given by

$$\widetilde{R} = \big|R^{\frac{1}{2}}\big\rangle\big\rangle\big\langle\big\langle R^{\frac{1}{2}}\big| \in \mathsf{Lin}(\mathcal{H} \otimes \mathcal{H}_A), \tag{13}$$

where $\mathcal{H}_A \simeq \mathsf{Supp}(R)$. The dilation $\widetilde{R}$ has the following interpretation: $\widetilde{R}$ is a quantum comb acting on the Hilbert spaces $(\widetilde{\mathcal{H}}_j)_{j=0}^{2N-1}$, where $\widetilde{\mathcal{H}}_{2N-1} := \mathcal{H}_{2N-1} \otimes \mathcal{H}_A$, and $\widetilde{\mathcal{H}}_k = \mathcal{H}_k$ for $k < 2N-1$. Therefore, it represents a network of quantum operations with memory. Tracing out the ancilla space $\mathcal{H}_A$ in the output $\widetilde{\mathcal{H}}_{2N-1} = \mathcal{H}_{2N-1} \otimes \mathcal{H}_A$ of the last quantum operation $\widetilde{C}_{N-1}$, one then obtains back the original network

$$R = \mathrm{Tr}_A[\widetilde{R}]. \tag{14}$$

For quantum states it is known that the purification is unique up to partial isometries on the ancilla spaces. For quantum combs one has the straightforward extension:

Proposition 1. *If $\widetilde{R}$ and $\widetilde{R}'$ are two dilations of the quantum comb R, i.e. $\widetilde{R}$ and $\widetilde{R}'$ are both non-negative rank-one operators such that*

$$\mathrm{Tr}_A[\widetilde{R}] = \mathrm{Tr}_{A'}\big[\widetilde{R}'\big], \tag{15}$$

then there exists a partial isometry W from A to A' such that

$$\widetilde{R}' = (I \otimes W)\widetilde{R}\big(I \otimes W^\dagger\big), \quad \widetilde{R} = \big(I \otimes W^\dagger\big)\widetilde{R}'(I \otimes W), \tag{16}$$

I denoting the identity on $\mathcal{H} = \bigotimes_{j=0}^{2N-1} \mathcal{H}_j$.

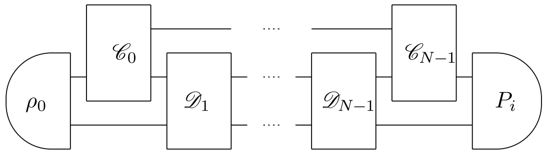

Fig. 5. Testing a network of N quantum operations $(\mathscr{C}_k)_{k=0}^{N-1}$. The tester consists in the preparation of an input state ρ_0, followed by quantum operations $\{\mathscr{D}_1, \ldots, \mathscr{D}_{N-1}\}$, and a final measurement $\{P_i\}$.

For the application to bit commitment it is crucial to note that all dilations of a comb can be obtained by just applying a partial isometry W on the *last output system*. An obvious consequence of the above fact is:

Corollary 1. *If $\widetilde{R}$ and $\widetilde{R}'$ are two dilations of the quantum comb R, then there exist two quantum channels $\mathscr{E}$ from states on $\mathcal{H}_A$ to states on $\mathcal{H}_{A'}$ and $\mathscr{F}$ from states on $\mathcal{H}_{A'}$ to states on $\mathcal{H}_A$ such that*

$$\widetilde{R}' = (\mathscr{I} \otimes \mathscr{E})(\widetilde{R}) = E * \widetilde{R}, \quad \widetilde{R} = (\mathscr{I} \otimes \mathscr{F})\big(\widetilde{R}'\big) = F * \widetilde{R}', \tag{17}$$

$\mathscr{I}$ denoting the identity map on $\mathcal{H} = \bigotimes_{j=0}^{2N-1} \mathcal{H}_j$, E and F being the Choi–Jamiołkowski operators of the channels $\mathscr{E}$ and $\mathscr{F}$, respectively.

This means that one can switch from one dilation to another just by performing some physical transformation on the ancilla in the last output system of the quantum network. As we will see in the following, in a bit commitment protocol this implies that Alice can delay her choice of the bit to the last moment before the opening.

3.4. Quantum testers

A tester represents a quantum network starting with a state preparation and finishing with a measurement. When such a network is connected to a network of N quantum operations as in Fig. 5, the output is a measurement outcome i with probability p_i. In a bit commitment protocol, a dishonest Bob will perform a tester to distinguish Alice's strategies before the opening.

Mathematically, the tester is the collection of Choi–Jamiołkowski operators $\{T_i\}$ given by

$$T_i := P_i * D_{N-1} * \cdots * D_1 * \rho_0, \tag{18}$$

where $(D_k)_{k=1}^{N-1}$ are the Choi–Jamiołkowski operators of the quantum operations $(\mathscr{D}_k)_{k=1}^{N-1}$ in Fig. 5. If the sum over all outcomes $T = \sum_i T_i$ is a deterministic comb, we call the tester as *normalized*.

When the tester is connected to a quantum network R, the probability of the outcome i is

$$p_i = T_i * R = \mathrm{Tr}\big[T_i^\tau R\big], \tag{19}$$

which is nothing but the Born rule, for quantum networks rather than states. Notice that one can include the transpose in the definition of the tester, thus getting the familiar form of the Born rule $p_i = \mathrm{Tr}[T_i R]$. However, here we preferred to write probabilities in terms of the combs R and T_i of the measured and measuring networks, respectively, thus making explicit that the Born rule is nothing but a particular case of link product, the transpose appearing as the signature of the linking of two networks.

For a deterministic comb R and a normalized tester $\{T_i\}$ one has the normalization of the total probability:

$$\sum_i p_i = \sum_i \mathrm{Tr}\big[T_i^\tau R\big] = 1. \tag{20}$$

In general, if one considers sub-normalized testers, one has

$$\sum_i p_i = \sum_i \mathrm{Tr}\big[T_i^\tau R\big] = p \leqslant 1. \tag{21}$$

In the following we will call $T = \sum_i T_i$ *tester operator*.

Proposition 2 *(Decomposition of testers [23]). Let $T = \sum_i T_i$ be the tester operator of the quantum tester $\{T_i\}$. Let $\mathcal{H}_B$ be the ancilla space $\mathcal{H}_B \simeq \mathsf{Supp}(T)$, and $\widetilde{T}$ be the dilation given by*

$$\widetilde{T} = \big|T^{\frac{1}{2}}\big\rangle\!\big\rangle\!\big\langle\!\big\langle T^{\frac{1}{2}}\big| \in \mathsf{Lin}(\mathcal{H} \otimes \mathcal{H}_B). \tag{22}$$

Then, one has the identity

$$\widetilde{T} * R = \big[T^\tau\big]^{\frac{1}{2}} R \big[T^\tau\big]^{\frac{1}{2}}. \tag{23}$$

Moreover, the probabilities of outcomes $p_i = T_i * R$ are given by

$$p_i = P_i * \widetilde{T} * R, \tag{24}$$

where $\{P_i\}$ is the POVM on $\mathcal{H}_B$ defined by

$$P_i = T^{-\frac{1}{2}} T_i T^{-\frac{1}{2}}, \tag{25}$$

$T^{-1/2}$ being the inverse of $T^{1/2}$ on its support.

Proof. Checking Eq. (23) is immediate using Eq. (3)

$$\begin{aligned}\widetilde{T} * R &= \mathrm{Tr}_{\mathcal{H}}\big[\big(R^\tau \otimes I_B\big)\big|T^{\frac{1}{2}}\big\rangle\!\big\rangle\!\big\langle\!\big\langle T^{\frac{1}{2}}\big|\big] \\ &= \big[T^\tau\big]^{\frac{1}{2}} R \big[T^\tau\big]^{\frac{1}{2}}.\end{aligned} \tag{26}$$

Regarding Eq. (24), one has $p_i = T_i * R = \mathrm{Tr}[T_i^\tau R] = \mathrm{Tr}[[T^\tau]^{\frac{1}{2}} P_i^\tau [T^\tau]^{\frac{1}{2}} R] = \mathrm{Tr}[P_i^\tau(\widetilde{T} * R)] = P_i * \widetilde{T} * R$. $\square$

The interpretation of the above result is the following realization scheme for the tester $\{T_i\}$:

- realize the quantum network $\widetilde{T}$ and connect it with the measured network R;
- conditionally on the given history of classical information corresponding to $\widetilde{T}$, perform the POVM $\{P_i\}$ on the ancilla state $\rho = \widetilde{T} * R$.

3.5. Discriminability of combs

Proposition 2 reduces any measurement on quantum network R to a measurement on a suitable (sub-normalized) state $\rho = \widetilde{T} * R$, which is obtained by connecting the input comb R with a suitable comb $\widetilde{T}$ corresponding to the dilation of Eq. (22). In particular, it reduces the discrimination of two networks R_0 and R_1 to the discrimination of two output states

$$\rho_T^{(i)} = \widetilde{T} * R_i = \big[T^\tau\big]^{\frac{1}{2}} R_i \big[T^\tau\big]^{\frac{1}{2}}, \quad i = 0, 1. \tag{27}$$

This allows for the definition of an operational distance between networks [23], whose meaning is directly related to statistical discriminability

$$\begin{aligned}\|R_1 - R_0\|_{\mathrm{op}} &:= \sup_T \big\|\rho_T^{(1)} - \rho_T^{(0)}\big\|_1 \\ &= \sup_T \big\|\widetilde{T} * (R_1 - R_0)\big\|_1 \\ &= \sup_T \big\|\big[T^\tau\big]^{\frac{1}{2}}(R_1 - R_0)\big[T^\tau\big]^{\frac{1}{2}}\big\|_1,\end{aligned} \tag{28}$$

where the supremum is taken over the set of all tester operators $T = \sum_i T_i$, and $\|A\|_1 = \mathrm{Tr}\,|A|$. Remarkably, the above norm can be strictly greater than the CB-norm of the difference $\mathscr{R}_1 - \mathscr{R}_0$ of the two multipartite channels [23]. This means that a sequential scheme such as that in Fig. 5 can achieve a strictly better discrimination than a parallel scheme where a multipartite entangled state is fed in the unknown channel.

In the case in which the tester T and the combs R_i are probabilistic (namely correspond to networks of quantum operations) the states $\rho_T^{(i)} = \widetilde{T} * R_i$ are generally sub-normalized, *i.e.* $\mathrm{Tr}[\rho_T^{(i)}] \leqslant 1$. In this case, the sole fact that the sequences of quantum operations represented by T and R_i took place helps in discriminating between R_0 and R_1. To be concrete, consider the scenario in which R_0 and R_1 have flat prior probabilities $\pi_0 = \pi_1 = 1/2$. The probability that the sequence of operations represented by T and R_i takes place is then given by $p(T, R_i) = \mathrm{Tr}[\rho_T^{(i)}]/2$. Since this probability depends on i, upon knowing that the sequence of quantum operations T took place the initial flat prior must be updated to

$$\pi_i' = p(R_i|T) = \frac{p(T, R_i)}{p(T)} = \frac{\mathrm{Tr}[\rho_T^{(i)}]}{\mathrm{Tr}[\rho_T^{(0)} + \rho_T^{(1)}]}. \tag{29}$$

The discrimination is now between the two conditional states $\bar{\rho}_T^{(i)} := \frac{\rho_T^{(i)}}{\mathrm{Tr}[\rho_T^{(i)}]}$ with prior probability π_i', $i = 0, 1$. Therefore, the maximum success probability is given by

$$\begin{aligned}p_{succ} &= \frac{1}{2}\big(1 + \big\|\pi_0' \bar{\rho}_T^{(0)} - \pi_1' \bar{\rho}_T^{(1)}\big\|_1\big) \\ &= \frac{1}{2}\left(1 + \frac{\|\rho_T^{(0)} - \rho_T^{(1)}\|_1}{\mathrm{Tr}[\rho_T^{(0)} + \rho_T^{(1)}]}\right).\end{aligned} \tag{30}$$

We will conveniently introduce the comb conditional "distance"

$$\begin{aligned}d(R_1, R_0) &:= \sup_T{}' \frac{\|\rho_T^{(1)} - \rho_T^{(0)}\|_1}{\mathrm{Tr}[\rho_T^{(1)} + \rho_T^{(0)}]} \\ &= \sup_T{}' \frac{\|\widetilde{T} * (R_1 - R_0)\|_1}{\mathrm{Tr}[\widetilde{T} * (R_1 + R_0)]} \\ &= \sup_T{}' \frac{\|[T^\tau]^{\frac{1}{2}}(R_1 - R_0)[T^\tau]^{\frac{1}{2}}\|_1}{\mathrm{Tr}[T^\tau(R_1 + R_0)]},\end{aligned} \tag{31}$$

where $\sup'$ (and consistently $\inf'$) denotes the supremum (infimum) restricted to the tester operators T such that $\mathrm{Tr}[T^\tau(R_0 + R_1)] > 0$. Here we use the expression "distance" in quotation marks because the quantity $d(R_1, R_0)$ does not satisfy all the mathematical properties of a distance: for example, it can be zero even if R_1 and R_0 do not coincide.

3.5.1. Discriminability with a restricted set of testers

The comb distance quantifies the performances of the best scheme among all possible sequential schemes one can use to discriminate between two quantum networks. However, in a bit commitment protocol the set of schemes that Bob can actually use for discrimination may be limited by several factors. For example, Alice could perform random checks during the commitment phase in order to force Bob to use a quantum network that is close to the one prescribed by the honest strategy. We will therefore define optimal conditional discrimination between R_0 and R_1 relatively to a restricted convex set T of tester operators that can actually occur in the protocol, thus introducing the conditional "distance"

$$\begin{aligned}d(R_1, R_0)|_{\mathsf{T}} &:= \sup_{T \in \mathsf{T}}{}' \frac{\|\rho_T^{(1)} - \rho_T^{(0)}\|_1}{\mathrm{Tr}[\rho_T^{(1)} + \rho_T^{(0)}]} \\ &= \sup_{T \in \mathsf{T}}{}' \frac{\|[T^\tau]^{\frac{1}{2}}(R_1 - R_0)[T^\tau]^{\frac{1}{2}}\|_1}{\mathrm{Tr}[T^\tau(R_1 + R_0)]}.\end{aligned} \tag{32}$$

Lemma 1. *The conditional "distance" in Eq. (32) is monotone under the application of a channel on the output spaces, namely*

$$d\big((\mathscr{C}\otimes\mathscr{I}_{in})R_1,(\mathscr{C}\otimes\mathscr{I}_{in})R_0\big)\big|_{\mathsf{T}}\leqslant d(R_1,R_0)|_{\mathsf{T}}. \tag{33}$$

Proof. Use monotonicity of trace-distance and the fact that the map $\mathscr{C}$ is trace-preserving. □

3.6. Continuity of dilation

We now prove that if two quantum combs R_0 and R_1 are close to each other then there exist two dilations $\widetilde{R}_0$ and $\widetilde{R}_1$ that are close with respect to the conditional "distance". Such continuity theorem replaces Stinespring's continuity theorem [28] used in the previous (C*-algebraic) impossibility proof of Ref. [3].

Lemma 2 *(Continuity of dilation). Let $R_0,R_1\in\mathsf{Lin}(\mathcal{H})$ be two quantum combs, $\widetilde{R}_i=|R_i^{\frac12}\rangle\rangle\langle\langle R_i^{\frac12}|\in\mathsf{Lin}(\mathcal{H}\otimes\mathcal{H}_A)$, $\mathcal{H}_A\simeq\mathcal{H}$ be two dilations, and $\mathsf{T}\subseteq\mathsf{Lin}(\mathcal{H})$ be an arbitrary convex set of tester operators T. The following bound holds*

$$\inf_{\mathcal{P}} d\big(\widetilde{R}_1,(\mathcal{I}\otimes\mathcal{P})(\widetilde{R}_0)\big)\big|_{\mathsf{T}\otimes I}\leqslant 2\sqrt{d(R_0,R_1)|_{\mathsf{T}}} \tag{34}$$

where $\mathsf{T}\otimes I=\{T\otimes I\mid T\in\mathsf{T}\}$ and the infimum is taken over the set of random unitary channels $\mathcal{P}(\rho)=\sum_k p_kU_k\rho U_k^\dagger$ acting on the ancilla $\mathcal{H}_A$.

Proof. If we define

$$\widetilde{\Delta}_{U_k}:=\frac{\widetilde{R}_1-(I\otimes U_k)\widetilde{R}_0(I\otimes U_k^\dagger)}{\mathrm{Tr}[(\widetilde{R}_0+\widetilde{R}_1)*T]}, \tag{35}$$

we have

$$\inf_{\mathcal{P}} d\big(\widetilde{R}_1,(\mathcal{I}\otimes\mathcal{P})(\widetilde{R}_0)\big)\big|_{\mathsf{T}\otimes I}=\inf_{\mathcal{P}}\sup_{T\in\mathsf{T}}{}'\bigg\|\sum_k p_k\widetilde{T}*\widetilde{\Delta}_{U_k}\bigg\|_1. \tag{36}$$

Using the triangular inequality for the trace-norm

$$\bigg\|\sum_k p_k\widetilde{T}*\widetilde{\Delta}_{U_k}\bigg\|_1\leqslant\sum_k p_k\|\widetilde{T}*\widetilde{\Delta}_{U_k}\|_1. \tag{37}$$

Moreover, exploiting Eq. (23) we can write

$$\|\widetilde{T}*\widetilde{\Delta}_{U_k}\|_1=\big\|\Psi^{(1)}_{T,I}-\Psi^{(0)}_{T,U_k}\big\|_1, \tag{38}$$

where $\Psi^{(0)}_{T,I}$ and $\Psi^{(1)}_{T,U_k}$ are defined by

$$\Psi^{(i)}_{T,C}:=\big|\Psi^{(i)}_{T,C}\big\rangle\big\rangle\big\langle\big\langle\Psi^{(i)}_{T,C}\big|,$$

$$\big|\Psi^{(i)}_{T,C}\big\rangle\big\rangle:=\frac{([T^\tau]^{\frac12}\otimes C)|R_i^{\frac12}\rangle\rangle}{\sqrt{\mathrm{Tr}[(R_0+R_1)T^\tau]}}, \tag{39}$$

for $C\in\mathsf{Lin}(\mathcal{H}_A)$ any contraction. Using the bound

$$\begin{aligned}&\big\||\psi\rangle\langle\psi|-|\varphi\rangle\langle\varphi|\big\|_1^2\\&\quad=\big(\|\psi\|^2+\|\varphi\|^2\big)^2-4\big|\langle\psi|\varphi\rangle\big|^2\\&\quad\leqslant\big(\|\psi\|+\|\varphi\|\big)^2\big(\|\psi\|^2+\|\varphi\|^2-2\big|\langle\psi|\varphi\rangle\big|\big),\end{aligned} \tag{40}$$

which for $\|\psi\|^2+\|\varphi\|^2=1$ becomes

$$\big\||\psi\rangle\langle\psi|-|\varphi\rangle\langle\varphi|\big\|_1^2\leqslant 2\big(1-2\big|\langle\psi|\varphi\rangle\big|\big), \tag{41}$$

we obtain

$$\|\widetilde{T}*\widetilde{\Delta}_{U_k}\|_1\leqslant 2\big(1-2\big|\big\langle\big\langle\Psi^{(1)}_{T,I}\big|\Psi^{(0)}_{T,U_k}\big\rangle\big\rangle\big|\big)^{\frac12}. \tag{42}$$

Then, by Jensen's inequality we have the following bound

$$\begin{aligned}&2\inf_{\mathcal{P}}\sup_{T\in\mathsf{T}}{}'\sum_k p_k\big(1-2\big|\big\langle\big\langle\Psi^{(1)}_{T,I}\big|\Psi^{(0)}_{T,U_k}\big\rangle\big\rangle\big|\big)^{\frac12}\\&\quad\leqslant 2\inf_{\mathcal{P}}\sup_{T\in\mathsf{T}}{}'\bigg(1-2\sum_k p_k\big|\big\langle\big\langle\Psi^{(1)}_{T,I}\big|\Psi^{(0)}_{T,U_k}\big\rangle\big\rangle\big|\bigg)^{\frac12}\\&\quad\leqslant 2\inf_{\mathcal{P}}\sup_{T\in\mathsf{T}}{}'\bigg(1-2\bigg|\sum_k p_k\big\langle\big\langle\Psi^{(1)}_{T,I}\big|\Psi^{(0)}_{T,U_k}\big\rangle\big\rangle\bigg|\bigg)^{\frac12}\\&\quad=2\inf_{\mathcal{P}}\sup_{T\in\mathsf{T}}{}'\big(1-2\big|\big\langle\big\langle\Psi^{(1)}_{T,I}\big|\Psi^{(0)}_{T,C}\big\rangle\big\rangle\big|\big)^{\frac12}\\&\quad\leqslant 2\inf_{\mathcal{P}}\sup_{T\in\mathsf{T}}{}'\big(1-2\,\mathrm{Re}\big\langle\big\langle\Psi^{(1)}_{T,I}\big|\Psi^{(0)}_{T,C}\big\rangle\big\rangle\big)^{\frac12},\end{aligned} \tag{43}$$

where C is the contraction $C=\sum_k p_kU_k$. Let us define by C the convex set of all contractions $C=\sum_k p_kU_k$, and define the following function on $\mathsf{C}\times\mathsf{T}$

$$f(C,T):=\mathrm{Re}\big\langle\big\langle\Psi^{(1)}_{T,I}\big|\Psi^{(0)}_{T,C}\big\rangle\big\rangle. \tag{44}$$

In Appendix A we use Sion's minimax theorem of Ref. [29] to prove the identity

$$\inf_{T\in\mathsf{T}}{}'\sup_{C\in\mathsf{C}}f(C,T)=\sup_{C\in\mathsf{C}}\inf_{T\in\mathsf{T}}{}'f(C,T). \tag{45}$$

The chain of inequalities proved until now gives

$$\begin{aligned}\inf_{\mathcal{P}} d\big(\widetilde{R}_1,(\mathcal{I}\otimes\mathcal{P})(\widetilde{R}_0)\big)\big|_{\mathsf{T}}&\leqslant 2\Big(1-2\sup_C\inf_{T\in\mathsf{T}}{}'f(C,T)\Big)^{\frac12}\\&\leqslant 2\Big(1-2\inf_{T\in\mathsf{T}}{}'\sup_C f(C,T)\Big)^{\frac12} \qquad (46)\\&\leqslant 2\Big(1-2\inf_{T\in\mathsf{T}}{}'\sup_U f(U,T)\Big)^{\frac12}, \qquad (47)\end{aligned}$$

where we substituted the supremum over contractions $C=\sum_k p_kU_k$ with the supremum over unitaries U, since the function $f(T,C)$ is linear in C. Moreover, we have

$$\begin{aligned}\sup_U f(T,U)&=\sup_U\mathrm{Re}\big\langle\big\langle\Psi^{(0)}_{T,I}\big|I\otimes U\big|\Psi^{(1)}_{T,I}\big\rangle\big\rangle\\&=\sup_U\big\langle\big\langle\Psi^{(0)}_{T,I}\big|I\otimes U\big|\Psi^{(1)}_{T,I}\big\rangle\big\rangle=\frac{F(\rho_T^{(1)},\rho_T^{(0)})}{\mathrm{Tr}[\rho_T^{(1)}+\rho_T^{(0)}]},\end{aligned} \tag{48}$$

where $\rho_T^{(i)}$, $i=0,1$, denote the unnormalized states $\rho_T^{(i)}:=[T^\tau]^{\frac12}R_i[T^\tau]^{\frac12}$ and $F(\rho,\sigma)=\sup_U\mathrm{Tr}[\rho^{\frac12}U\sigma^{\frac12}]$ is the Uhlmann fidelity. Finally, we can use the Bures–Alberti–Uhlmann bound

$$\mathrm{Tr}[\rho+\sigma]-2F(\rho,\sigma)\leqslant\|\rho-\sigma\|_1 \tag{49}$$

to obtain

$$\inf_{\mathcal{P}} d\big(\widetilde{R}_1,(\mathcal{I}\otimes\mathcal{P})(\widetilde{R}_0)\big)\big|_{\mathsf{T}} \qquad (50)$$

$$\leqslant 2\sup_{T\in\mathsf{T}}{}'\bigg(1-2\frac{F(\rho_T^{(1)},\rho_T^{(0)})}{\mathrm{Tr}[\rho_T^{(0)}+\rho_T^{(1)}]}\bigg)^{\frac12}$$

$$\leqslant 2\sup_{T\in\mathsf{T}}{}'\frac{\|\rho_T^{(1)}-\rho_T^{(0)}\|_1^{\frac12}}{\mathrm{Tr}[\rho_T^{(0)}+\rho_T^{(1)}]}=2\sqrt{d(R_1,R_0)|_{\mathsf{T}}}.\quad\square \tag{51}$$

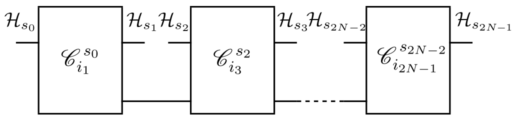

Fig. 6. Conditioned comb: sequence of quantum operations depending on previously exchanged classical information. Here i_{2k-1} is the outcome of the k-th quantum operation, and $s_l = i_0 i_1 \dots i_l$ is the history of classical information available at step l.

3.7. Conditioned quantum combs

A general two-party protocol entails the exchange of both quantum systems and of classical information, which is in principle openly known. Therefore, the strategy of a party will result in a sequence of quantum operations $\mathscr{C}^{s_{2k-2}}_{i_{2k-1}}$, $k = 1, 2, \dots, N$, as in Fig. 6. Here the index i_{2k-1} denotes the outcome of the quantum operation, and the string s_l represents the full history of classical information exchanged before the occurrence of the operation, namely $s_l = i_0 i_1 \dots i_l$, with i_{2k-2} representing the input classical information at step k. For example, if the comb in Fig. 6 represents Alice's strategy in a two-party protocol with Alice's and Bob's combs interlaced as in Fig. 2, it describes the following situation: Alice receives from Bob the classical information $i_0 \equiv s_0$ along with a quantum system with the Hilbert space $\mathcal{H}_{s_0}$. Then she performs the instrument $\mathscr{I}^{s_0} = \{\mathscr{C}^{s_0}_j\}$ obtaining the outcome $j = i_1$. Then she sends to Bob the outcome along with a quantum system with the Hilbert space $\mathcal{H}_{s_1}$ with $s_1 = i_0 i_1$. The normalization of the instrument is

$$\sum_{i_1} \mathrm{Tr}_{\mathcal{H}_{s_1}} \left[\mathscr{C}^{s_0}_{i_1}(\rho)\right] = \mathrm{Tr}[\rho], \quad \forall s_0, \forall \rho \in \mathsf{Lin}(\mathcal{H}_{s_0}), \tag{52}$$

which, in terms of Choi–Jamiołkowski operators reads

$$\sum_{i_1} \mathrm{Tr}_{\mathcal{H}_{s_1}} \left[C^{s_0}_{i_1}\right] = I_{s_0}, \quad \forall s_0. \tag{53}$$

At the next step Alice receives from Bob the classical information i_2 along with a quantum system with the Hilbert space $\mathcal{H}_{s_2}$, which depends on $s_2 = i_0 i_1 i_2$. Then she performs the instrument $\mathscr{I}^{s_2} = \{\mathscr{C}^{s_2}_j\}$ obtaining the outcome $j = i_3$, and so on. By linking the Choi–Jamiołkowski operators of all quantum operations, one obtains a family of probabilistic combs $\{R_{s_{2N-1}}\}$ satisfying the normalization conditions

$$\sum_{i_{2k-1}} \mathrm{Tr}_{\mathcal{H}_{s_{2k-1}}} \left[R^{(k)}_{s_{2k-2} i_{2k-1}}\right] = I_{s_{2k-2}} \otimes R^{(k-1)}_{s_{2k-3}}, \tag{54}$$

where $R^{(N)}_{s_{2N-1}} := R_{s_{2N-1}}$, $R^{(k)}_{s_{2k-1}} \in \mathsf{Lin}(\bigotimes_{j=0}^{2k-1} \mathcal{H}_{s_j})$, and $R^{(0)} = 1$. Eq. (54) is the mathematical representation of the most general strategy in a quantum protocol with exchange of classical and quantum information, generalizing the game-theoretical framework introduced by Gutoski and Watrous [22] for protocols involving only exchange of quantum systems. We will call the collection of probabilistic quantum combs satisfying Eq. (54) a *conditioned comb*. This nomenclature reflects the fact that the most general way of conditioning a quantum comb needs to use at each step the information coming from all previous steps.

On the other hand, also the converse statement is true: a collection of positive operators satisfying Eq. (54) can always be realized by a physical scheme as in Fig. 6. This fact is proved in the following proposition.

Theorem 2. *Any conditioned comb is the collection of Choi–Jamiołkowski operators of a network of N conditioned instruments as in Fig. 6.*

Proof. Suppose that a collection of operators $\{R_{s_{2N-1}}\}$ labeled by classical strings $s_{2N-1} = i_0 i_1 \dots i_{2N-1}$ satisfies conditions Eq. (54). Then, we can define the operator

$$R := \sum_{s_{2N-1}} R_{s_{2N-1}} \otimes |s_{2N-1}\rangle\langle s_{2N-1}| \otimes |s_{2N-2}\rangle\langle s_{2N-2}| \otimes \cdots \otimes |s_0\rangle\langle s_0|. \tag{55}$$

Here, R acts on the tensor product $\bigotimes_{j=0}^{2N-1} \mathcal{H}_j$, where the j-th space is $\mathcal{H}_j := (\bigoplus_{s_j} \mathcal{H}_{s_j} \otimes |s_j\rangle)$. With this definition, R is a deterministic comb, *i.e.* an operator satisfying Eq. (8). Therefore, by Proposition 1 R can be realized with a network of N channels $(\mathscr{C}_k)_{k=0}^{N-1}$ as in Fig. 4. Now, if we apply the von Neumann–Lüders measurements $\{I_{s_{2k}} \otimes |s_{2k}\rangle\langle s_{2k}|\}$ on the input space $\mathcal{H}_{2k}$ before channel $\mathscr{C}_k$, followed by $\{I_{s_{2k+1}} \otimes |s_{2k+1}\rangle\langle s_{2k+1}|\}$ on the output space $\mathcal{H}_{2k+1}$ after channel $\mathscr{C}_k$, we obtain the conditioned quantum operations $\{\mathscr{C}^{s_{2k}}_{i_{2k+1}}\}$. Denoting by $C^{s_{2k}}_{i_{2k+1}}$ the Choi–Jamiołkowski operator of the quantum operation $\mathscr{C}^{s_{2k}}_{i2k+1}$ we then have $R_{s_{2N-1}} = C^{s_{2N-2}}_{i_{2N-1}} * C^{s_{2N-4}}_{i_{2N-3}} * \cdots * C^{s_0}_{i_1}$, *i.e.* $R_{s_{2N-1}}$ is the Choi–Jamiołkowski operator of the sequence of quantum operations $(\mathscr{C}^{s_{2k}}_{i_{2k+1}})_{k=0}^{N-1}$, as in Fig. 6. □

As a consequence of the last theorem single-party strategies in a protocol are in one-to-one correspondence with conditioned combs. In the following we will consider dilations of a conditioned comb $\{R_{s_{2N-1}}\}$ defined as the collection $\{\widetilde{R}_{s_{2N-1}}\}$ of dilations $\widetilde{R}_{s_{2N-1}} \in \mathsf{Lin}([\bigotimes_{j=0}^{2N-1} \mathcal{H}_{s_j}] \otimes \mathcal{H}_{A,s_{2N-1}})$ of each comb $R_{s_{2N-1}} \in \mathsf{Lin}(\bigotimes_{j=0}^{2N-1} \mathcal{H}_{s_j})$, where $\mathcal{H}_{A,s_{2N-1}}$ is an ancillary space depending on history. The following theorem guarantees that the dilation of a conditioned comb is still a conditioned comb.

Theorem 3. *For any conditioned comb $\{R_{s_{2N-1}}\}$ the dilation $\{\widetilde{R}_{s_{2N-1}}\}$ defined by $\widetilde{R}_{s_{2N-1}} := |R^{\frac{1}{2}}_{s_{2N-1}}\rangle\rangle\langle\langle R^{\frac{1}{2}}_{s_{2N-1}}|$ is a conditioned comb.*

Proof. Define $\mathcal{H}'_{s_{2N-1}} := \mathcal{H}_{s_{2N-1}} \otimes \mathcal{H}_{A,s_{2N-1}}$ and $\mathcal{H}'_{s_l} = \mathcal{H}_{s_l}$ for $l < 2N-1$. Then, the operators $\{\widetilde{R}_{s_{2N-1}}\}$ form a conditioned comb in $\mathsf{Lin}(\bigotimes_{j=0}^{2N-1} \mathcal{H}'_{s_j})$. □

The dilation of a conditioned comb describes a sequence of single-Kraus quantum operations, each of them depending on the previously exchanged classical information. Loosely speaking, this theorem means that the "quantum part" of any strategy can be purified until the end of the protocol, still resulting in a valid strategy.

4. Comb formulation of the quantum bit commitment

A (generally multiparty) protocol establishes which single-party strategies are honest. A strategy is a choice of processing of classical/quantum information at each step, and specifies which quantum instrument a party will perform jointly on his ancillae and on the received quantum systems, conditioned on the available classical information. The honest strategies of the protocol fix the communication interface among parties, consisting of the complete specification of which classical and quantum systems are exchanged at each step. A cheating strategy can be any strategy that conforms to the communication interface.

A definition of security of a protocol generally depends on the specific goals of the involved parties. For the quantum bit commitment a protocol is defined as perfectly secure if the following conditions are satisfied:

concealingness: for all Alice's honest strategies Bob cannot read the committed bit before the opening;
bindingness: for all honest Bob's strategies Alice cannot change the value of the committed bit without being detected.

Note the asymmetry between the security condition for the two parties: on the one hand, security for Alice means that Bob has no chance at all to read the bit, while, one the other hand, security for Bob means that if Alice tries to cheat, she will be surely detected. Perfect security is relaxed to the case of ε-*concealingness* and δ-*bindingness*, where the probability for Bob to read the committed bit is bounded by ε, and the probability for Alice to change the bit value is bounded by δ.

In the following subsections we will formulate strategies in terms of quantum combs, and evaluate the probabilities of successfully cheating for both parties.

4.1. Alice's and Bob's strategies

As already noticed, there is no loss of generality in considering bit commitment protocols started by Bob. With the letter $k = 1, \dots, N$ we will denote the k-th Bob's and Alice's step. Thus $s_l = i_0 i_1 \dots i_l$ will represent the history of classical information with i_{2k-1} denoting the outcome of Bob's quantum operation at step k (which is the same as Alice's classical input at Alice's step k) and i_{2k-2} for $k > 1$ represents Bob's input classical information (which is Alice's output at step $k-1$). At the beginning of the protocol there is no classical and quantum information, whence $s_0 = i_0$ is the null string and $\mathcal{H}_0 = \mathbb{C}$. At the end of the commitment stage we can assume without loss of generality that Alice performs the last move (for a protocol where the last move is Bob's, we can always add a null move, in which no classical and quantum systems are sent).

We will now analyze the case in which the total number of steps in the protocol is uniformly bounded, and will denote by N the maximum number of steps. Moreover, since we can always add null moves, we will consider without loss of generality protocols where the number of steps N is independent of the history. Therefore classical history labeling the sequence of quantum operations will be s_{2N} for Alice, and s_{2N-1} for Bob.

We denote by A_0 and A_1 the sets of honest strategies that Alice can use to encode bit values 0 and 1, respectively. According to Section 3.7, a possible strategy in A_i is a conditioned quantum comb $\{A_{i,s_{2N}}\}$, where the index s_{2N} labels a history of classical information exchanged between Alice and Bob. For each history s_{2N}, $A_{i,s_{2N}}$ is a probabilistic comb on $\mathcal{K}_{s_{2N}} \otimes \mathcal{H}_{A,s_{2N}}$, where $\mathcal{K}_{s_{2N}} = \mathsf{Lin}(\bigotimes_{j=0}^{2N} \mathcal{H}_{s_j})$ is the Hilbert space of all quantum systems exchanged in the protocol and $\mathcal{H}_{A,s_{2N}}$ is the Hilbert space of Alice's private ancillae.

In the following we will denote by B the set of strategies (honest or not) that are available to Bob. An element of B is a collection of probabilistic quantum combs $\{B_{s_{2N-1}}\}$. For each s_{2N-1}, $B_{s_{2N-1}}$ is a comb on $\mathcal{H}_{s_{2N-1}} \otimes \mathcal{H}_{B,s_{2N-1}}$, $\mathcal{H}_{B,s_{2N-1}}$ being the Hilbert space of Bob's ancillae. The set B can be the whole set of strategies compatible with the communication interface, or a restricted subset. The only assumption is that if B contains a strategy, then it contains also its dilations. The reader should then regard B as a parameter of his own choice for the rest of the Letter. Therefore, the impossibility proof will state that if the protocol is concealing for a Bob restricted to B, then it is necessarily not binding for the same Bob.

Since a protocol that is not concealing at step k is also not concealing at any following step, we will now focus on the last step N before the opening. In the following we will drop the sub-index $2N$ ($2N-1$) labeling Alice's (Bob's) history. For the history s, the overall (unnormalized) state resulting from Alice and Bob playing the strategies $\{A_{i,s'}\}$ and $\{B_{s'}\}$, respectively, is given by the link product

$$\sigma_s^{(i)} = B_s * A_{i,s}. \tag{56}$$

The probability of the history s is then given by the trace

$$p_s^{(i)} = \mathrm{Tr}\big[\sigma_s^{(i)}\big]. \tag{57}$$

The local state at Bob before the opening is

$$\rho_s^{(i)} = \mathrm{Tr}_{\mathcal{H}_{A,s}}\big[\sigma_s^{(i)}\big] = B_s * R_{i,s}, \tag{58}$$

where

$$R_{i,s} = \mathrm{Tr}_{\mathcal{H}_{A,s}}[A_{i,s}] \tag{59}$$

is the restriction of Alice's comb to the quantum systems exchanged in the protocol.

4.2. Concealing protocols

For any strategy $\{B_{s'}\} \in \mathsf{B}$ and for any history s we denote by $\widetilde{B}_s$ the dilation of B_s. Since Bob is free to dilate his quantum operations using additional ancillae, he can exploit such a dilation to better discriminate Alice's strategies.

Definition 1 *(Concealing protocols).* A quantum bit commitment protocol is ε-concealing if there is at least a couple of honest strategies $\{A_{0,s'}\} \in \mathsf{A}_0$, $\{A_{1,s'}\} \in \mathsf{A}_1$ such that the following conditions hold:

$$\max_s \frac{\|\rho_s^{(1)} - \rho_s^{(0)}\|_1}{\mathrm{Tr}[\rho_s^{(1)} + \rho_s^{(0)}]} \leqslant \varepsilon, \quad \forall \{B_{s'}\} \in \mathsf{B}, \tag{60}$$

where $\rho_s^{(i)}$ is the unnormalized state on Bob's side $\rho_s^{(i)} = \widetilde{B}_s * R_{i,s}$, with $R_{i,s} = \mathrm{Tr}_{\mathcal{H}_{A,s}}[A_{i,s}]$.

As discussed in Section 3.5, the above condition means that, for any history of classical communication, the probability that Bob discriminates correctly between $R_{0,s}$ and $R_{1,s}$ is ε-close to $1/2$, the success probability of a random guess.

The concealment condition can be translated in terms of combs distances as follows:

Lemma 3. *A protocol is ε-concealing if and only if there is a couple of honest strategies $\{A_{0,s'}\}$ and $\{A_{1,s'}\}$ such that*

$$\max_s d(R_{1,s}, R_{0,s})|_{\mathsf{T}_s} \leqslant \varepsilon, \tag{61}$$

where $\mathsf{T}_s = \{T_s := \mathrm{Tr}_{\mathcal{H}_{B,s}}[B_s],\ B_s \in \{B_{s'}\} \in \mathsf{B}\}$.

Proof. Clearly, condition (60) holds if and only if

$$\max_s \sup_{\mathsf{B}_s} \frac{\|\rho_s^{(1)} - \rho_s^{(0)}\|_1}{\mathrm{Tr}[\rho_s^{(1)} + \rho_s^{(0)}]} \leqslant \varepsilon, \tag{62}$$

where $\mathsf{B}_s = \{B_s \in \{B_{s'}\} \in \mathsf{B}\}$. Moreover, since the set of Bob's strategies is closed under dilation, and since dilation improves the discrimination, the supremum can be taken over the dilations $\{\widetilde{B}_{s'}\}$. Now, denote by $\widetilde{T}_s$ the dilation of $T_s = \mathrm{Tr}_{\mathcal{H}_{B,s}}[B_s]$. Since $\widetilde{B}_s$ and $\widetilde{T}_s$ are both dilations of T_s, they are connected by a partial isometry on Bob's ancillae. The same is true for the states $\tilde{\rho}_s^{(i)} := \widetilde{B}_s * R_{i,s}$, and $\rho_{T_s}^{(i)} := \widetilde{T}_s * R_{i,s}$, for each value $i = 0, 1$, whence $\|\tilde{\rho}_s^{(0)} - \tilde{\rho}_s^{(1)}\|_1 = \|\rho_{T_s}^{(0)} - \rho_{T_s}^{(1)}\|_1$. This implies the identity

$$\max_s \sup_{\mathsf{B}_s} \frac{\|\rho_s^{(1)} - \rho_s^{(0)}\|_1}{\mathrm{Tr}[\rho_s^{(1)} + \rho_s^{(0)}]} = \max_s \sup_{\mathsf{B}_s} \frac{\|\tilde{\rho}_s^{(1)} - \tilde{\rho}_s^{(0)}\|_1}{\mathrm{Tr}[\tilde{\rho}_s^{(1)} + \tilde{\rho}_s^{(0)}]} = \max_s \sup_{\mathsf{T}_s} \frac{\|\rho_{T_s}^{(1)} - \rho_{T_s}^{(0)}\|_1}{\mathrm{Tr}[\rho_{T_s}^{(1)} + \rho_{T_s}^{(0)}]} = \max_s d(R_{1,s}, R_{0,s})|_{\mathsf{T}_s}. \qquad \square \tag{63}$$

4.3. Alice's cheating strategies

Let $\{A_{s'}\}$ and $\{A^\sharp_{s'}\}$ be an honest and a dishonest strategy by Alice, respectively (here we drop the index $i = 0, 1$ of the bit value, since it is unnecessary for the following discussion). When Bob chooses the strategy $\{B_{s'}\} \in \mathsf{B}$, for history s the unnormalized quantum states before the opening phase are

$$\sigma_s = B_s * A_s, \qquad \sigma_s^\sharp = B_s * A_s^\sharp. \tag{64}$$

Definition 2. The strategy $\{A^\sharp_{s'}\}$ is δ-close to the strategy $\{A_{s'}\}$ at the opening if for any strategy $\{B_{s'}\} \in \mathsf{B}$ one has

$$\max_s \frac{\|\sigma_s - \sigma_s^\sharp\|_1}{\mathrm{Tr}[\sigma_s + \sigma_s^\sharp]} \leqslant \delta. \tag{65}$$

If two strategies are δ-close, even if the history that takes place is the most favorable to Bob, Bob cannot distinguish between them.

Following the same argument used in the proof of Lemma 3, the notion of δ-closeness can be expressed in terms of comb distance as follows:

Proposition 3. *The strategy $\{A^\sharp_{s'}\}$ is δ-close to the strategy $\{A_{s'}\}$ at the opening if and only if*

$$\max_s d\big(A_s, A_s^\sharp\big)\big|_{\mathsf{T}_s} \leqslant \delta, \tag{66}$$

where $\mathsf{T}_s = \{T_s := \mathrm{Tr}_{\mathcal{H}_{B,s}}[B_s],\ B_s \in \{B_{s'}\} \in \mathsf{B}\}$.

Definition 3. Given two honest strategies $\{A_{0,s'}\} \in \mathsf{A}_0$, $\{A_{1,s'}\} \in \mathsf{A}_1$, a δ-cheating is a couple of strategies $\{A^\sharp_{0,s'}\}$ and $\{A^\sharp_{1,s'}\}$ satisfying the conditions

1. $\{A^\sharp_{i,s'}\}$ is δ-close to $\{A_{i,s'}\}$ for $i = 0, 1$;
2. for every history s, there exists a quantum channel $\mathscr{C}_s$ acting on Alice's ancilla space $\mathcal{H}_{A,s}$ such that

$$A^\sharp_{1,s} = (\mathscr{I}_s \otimes \mathscr{C}_s)\big(A^\sharp_{0,s}\big), \tag{67}$$

where $\mathscr{I}_s$ is the identity channel on the Hilbert space $\mathcal{K}_s$ of all quantum systems exchanged in the commitment phase.

The second condition means that Alice can follow the strategy $\{A^\sharp_{0,s'}\}$ until the end of the commitment, and switch to the strategy $\{A^\sharp_{1,s}\}$ with a local operation on her ancillae just before the opening.

5. The impossibility proof

5.1. Protocols with bounded number of rounds

Theorem 4. *If an N-round protocol is ε-concealing with honest strategies $\{A_{0,s}\} \in \mathsf{A}_0$ and $\{A_{1,s}\} \in \mathsf{A}_1$, then there is a $2\sqrt{\varepsilon}$-cheating with cheating strategies $\{A^\sharp_{0,s}\}$ and $\{A^\sharp_{1,s}\}$. In particular, the cheating strategy $\{A^\sharp_{0,s}\}$ coincides with the honest strategy $\{A_{0,s}\}$.*

Proof. According to Eq. (61), the concealing condition is for any history s

$$d(R_{1,s}, R_{0,s})|_{\mathsf{T}_s} < \varepsilon, \tag{68}$$

where $R_{i,s} = \mathrm{Tr}_{\mathcal{H}_{A,s}}[A_{i,s}]$ and $\mathsf{T}_s = \{T_s = \mathrm{Tr}_{\mathcal{H}_{B,s}}[B_s] \mid B_s \in \{B_{s'}\} \in \mathsf{B}\}$. We now focus on a fixed history s, and show the existence of two $2\sqrt{\varepsilon}$-cheating strategies $\{A^\sharp_{0,s'}\}$ and $\{A^\sharp_{1,s'}\}$. Since we are fixing s, we drop the index s everywhere.

Since the reduced combs $R_i = \mathrm{Tr}_{\mathcal{H}_A}[A_i] \in \mathsf{Lin}(\mathcal{K})$ satisfy the condition $d(R_1, R_0)|_{\mathsf{T}} < \varepsilon$, we can use the continuity of dilation stated by Lemma 2, thus finding a random unitary channel $\mathcal{P} = \sum_k p_k \mathcal{U}_k$ acting on $\mathcal{H}_A$ such that

$$d\big(\widetilde{R}_1, (\mathcal{I} \otimes \mathcal{P})\widetilde{R}_0\big)\big|_{\mathsf{T}} \leqslant 2\sqrt{d(R_1, R_0)|_{\mathsf{T}}}, \tag{69}$$

where $\widetilde{R}_i$ is the dilation $\widetilde{R}_i = |R_i^{\frac{1}{2}}\rangle\!\rangle\langle\!\langle R_i^{\frac{1}{2}}| \in \mathsf{Lin}(\mathcal{K} \otimes \mathcal{K}_A)$, with $\mathcal{K}_A \simeq \mathcal{K}$. Now consider the dilations of the honest strategies

$$\widetilde{A}_i := \big|A_i^{\frac{1}{2}}\rangle\!\rangle\langle\!\langle A_i^{\frac{1}{2}}\big|. \tag{70}$$

Here $\widetilde{A}_i$ is an operator in $\mathsf{Lin}(\mathcal{K} \otimes \mathcal{H}_A \otimes \mathcal{L}_A)$ where $\mathcal{L}_A \simeq \mathcal{K} \otimes \mathcal{H}_A$ is an additional ancilla space on Alice's side. By definition, $R_i = \mathrm{Tr}_{\mathcal{H}_A, \mathcal{L}_A}[\widetilde{A}_i]$. Since $\widetilde{A}_i$ and $\widetilde{R}_i$ are both dilations of R_i, there exist a channel $\mathcal{E}_i$ sending states on $(\mathcal{H}_A \otimes \mathcal{L}_A)$ to states on $\mathcal{K}_A$ such that

$$\widetilde{R}_i = (\mathcal{I}_{\mathcal{K}} \otimes \mathcal{E}_i)(\widetilde{A}_i), \tag{71}$$

and a channel $\mathcal{F}_i$ sending states on $\mathcal{K}_A$ to states on $(\mathcal{H}_A \otimes \mathcal{L}_A)$ such that

$$\widetilde{A}_i = (\mathcal{I}_{\mathcal{K}} \otimes \mathcal{F}_i)(\widetilde{R}_i). \tag{72}$$

Alice's cheating procedure is then the following:

- Use the dilated strategy $\widetilde{A}_0$.
- After the commitment decide the bit value. To commit 0, do nothing. To commit 1, apply the channel $\mathscr{C} = \mathcal{F}_1\mathcal{P}\mathcal{E}_0$ on the ancillae, where $\mathcal{P}(\rho) = \sum_i p_i U_i \rho U_i^\dagger$.
- Discard the additional ancilla $\mathcal{L}_A$.

This procedure defines for every history s the two cheating strategies $\{A^\sharp_{0,s'}\} := \{A_{0,s'}\}$ and $\{A_{1,s'}\} := \{(\mathscr{I}_{s'} \otimes \mathscr{C}_{s'})(A^\sharp_{0,s})\}$. Clearly, $\{A^\sharp_{0,s'}\}$ is $2\sqrt{\varepsilon}$-close to $\{A_{0,s'}\}$ (in fact, they coincide). Regarding $\{A^\sharp_{1,s'}\}$, for any history s (and hence dropping the index) we have

$$\begin{aligned} d\big(A_1, A_1^\sharp\big)\big|_{\mathsf{T}} &= d\big(A_1, \mathrm{Tr}_{\mathcal{L}_A}\big[(\mathcal{I} \otimes \mathcal{F}_1\mathcal{P}\mathcal{E}_0)(\widetilde{A}_0)\big]\big)\big|_{\mathsf{T}} \\ &\leqslant d\big(\widetilde{A}_1, (\mathcal{I} \otimes \mathcal{F}_1\mathcal{P}\mathcal{E}_0)(\widetilde{A}_0)\big)\big|_{\mathsf{T}} \\ &= d\big((\mathcal{I} \otimes \mathcal{F}_1)(\widetilde{R}_1), (\mathcal{I} \otimes \mathcal{F}_1\mathcal{P})(\widetilde{R}_0)\big)\big|_{\mathsf{T}} \\ &\leqslant d\big(\widetilde{R}_1, (\mathcal{I} \otimes \mathcal{P})(\widetilde{R}_0)\big)\big|_{\mathsf{T}} \\ &\leqslant 2\sqrt{d(R_1, R_0)|_{\mathsf{T}}} \leqslant 2\sqrt{\varepsilon}. \end{aligned} \tag{73}$$

Here, the first and the second inequalities derive from Lemma 1, the third one is Eq. (69), and the last is the concealing condition. $\square$

5.2. Protocols with unbounded number or rounds

Here we show how the impossibility result of the previous subsection can be easily extended to the case of protocols where the number of rounds is unbounded. In this case Alice's (Bob's) strategies are still described by collections of probabilistic combs $\{A_s\}$ and $(\{B_s\})$, where each probabilistic comb represents the sequence of quantum operations performed by Alice (Bob) for a given history s of classical communication. Note that, although the length of the strings is no longer bounded by a fixed number $N < \infty$, any given string s must have finite length. Indeed, a protocol allowing an infinitely long history s would be a protocol in which sometimes Alice and Bob have to continue their communication forever, without reaching neither a successful commitment, nor an abort.

For a protocol with unbounded number of rounds, the conditions of ε-concealment and δ-closeness are still given by Eqs. (60) and (65), respectively. Now, it is immediate to see that, given an ε-concealing protocol with unbounded number of rounds, one can always construct a new ε-concealing protocol with bounded number. Indeed, Alice can follow the original unbounded protocol, and decide to abort whenever the number of rounds exceeds a fixed number N. This change does not change the security of the protocol: it just reduces the probability of successful commitment by turning some histories that in the original protocol ended in a successful commitment into histories that end in an abort. For the new protocol with finite rounds, however, one apply Theorem 4, thus finding a $2\sqrt{\varepsilon}$-cheating for Alice. Since N is arbitrary and since for any N the cheating strategy coincides with the honest one up to the opening, Alice can take the number N to be sufficiently large to make the probability of successful commitment close to the one of the original protocol.

6. Summary

In this Letter we have provided a new short impossibility proof of quantum bit commitment. The present proof differs from the previous ones in the following main aspects: (a) The strategies, including all their "purifications", have a simple and univocal mathematical representation in terms of conditioned quantum combs in Eq. (54); (b) The definition of concealment and bindingness are worst-case over histories namely the conditions on cheating probabilities are defined uniformly over histories of classical communication rather than on average; (c) We consider the possibility of restricting the strategies of Bob to a set which however contains all their dilations, and show that if the protocol is concealing for Bob restricted in this way, then it is not binding. It is possible to prove along similar lines the impossibility theorem also with cheating probabilities averaged over histories, however the two impossibility theorems are not comparable, since worst-case concealment implies concealment in average, while bindingness in average implies worst-case bindingness, but not vice versa.

At the end of the Letter, we want to stress two points regarding abortion probabilities. First, concealment is defined regardless abortion, namely Bob cannot detect the bit value anyway, whether Alice catches him or not. Second, in order to cheat Alice plays an honest strategy $\{A_{0,s'}\}$ up to the very last moment of the opening, at which point her cheating is undetectable by Bob (by the impossibility theorem). Therefore, Alice always plays zero up to the abortion (if any), and takes her decision only when the opening is reached. Whence she successfully cheats also for protocols with abortions, and the impossibility theorem still holds. On the other hand, if we don't allow to repeat the protocol, then the only possibility is that the protocol aborts for honest Alice, whence there is no bit commitment at all, and the theorem applies trivially.

Acknowledgements

G.M.D. acknowledges interesting discussions with H. Yuen, H.K. Lo, and C. Bennett. G.C., G.M.D., P.P. acknowledge A. Bisio for useful observations. G.C. is supported the National Basic Research Program of China (973) 2011CBA00300 (2011CBA00301), by the National Natural Science Foundation of China through Grants 61033001 and 61061130540, and by the 1000 Youth Fellowship Program of China. G.C., G.M.D., and P.P. acknowledge support by EC through projects CORNER and COQUIT.

Appendix A. Proof of minimax equality in Eq. (45)

Lemma 4. *Let f be the function from $\mathsf{C} \times \mathsf{T}$ to $\mathbb{R}$:*

$$f(C,T) = \mathrm{Re}\langle\!\langle \Psi^{(1)}_{T,I} | \Psi^{(0)}_{T,C} \rangle\!\rangle, \tag{A.1}$$

$$\langle\!\langle \Psi^{(1)}_{T,I} | \Psi^{(0)}_{T,C} \rangle\!\rangle = \frac{\langle\!\langle R_1^{\frac{1}{2}} | T^\tau \otimes C | R_0^{\frac{1}{2}} \rangle\!\rangle}{\mathrm{Tr}[T^\tau (R_0 + R_1)]} \tag{A.2}$$

where $R_i \geqslant 0$. Then one has the identity

$$\inf_T{}' \sup_C f(C,T) = \sup_C \inf_T{}' f(C,T), \tag{A.3}$$

where the infimum over T is taken over the set of testers $T \in \mathsf{T}$ such that $\mathrm{Tr}[T^\tau(R_0 + R_1)] \neq 0$.

Proof. Define the compact convex set T_n as

$$\mathsf{T}_n := \left\{ T \in \mathsf{T} \,\middle|\, \mathrm{Tr}\big[T^\tau (R_0 + R_1)\big] \geqslant \frac{1}{n} \right\}. \tag{A.4}$$

We now restrict f to the set T_n and apply Sion's minimax theorem [29]. The hypotheses of the theorem are satisfied: First the function is continuous versus C and T and both sets C and T_n are compact and convex. Finally, the function f, being linear-fractional, is *quasi-linear* in T for every C, and it is linear in C for every $T \in \mathsf{T}$ [30].

Now, using the fact that T_n is included in T and applying Sion's theorem [29] we obtain for any n

$$\inf_{T \in \mathsf{T}_n} \sup_C f(C,T) = \sup_C \inf_{T \in \mathsf{T}_n} f(C,T). \tag{A.5}$$

Since the equality holds for any n, we also have

$$\begin{aligned} \inf_{T \in \mathsf{T}} \sup_C f(C,T) &= \inf_n \inf_{T \in \mathsf{T}_n} \sup_C f(C,T) \\ &= \inf_n \sup_C \inf_{T \in \mathsf{T}_n} f(C,T) = \lim_{n \to \infty} \sup_C \inf_{T \in \mathsf{T}_n} f(C,T) \\ &= \sup_C \inf_{T \in \mathsf{T}} f(C,T). \qquad \square \end{aligned} \tag{A.6}$$

References

[1] H.K. Lo, H.F. Chau, Phys. Rev. Lett. 78 (1997) 3410.
[2] D. Mayers, Phys. Rev. Lett. 78 (1997) 3414.
[3] G. D'Ariano, D. Kretschmann, D. Schlingemann, R.F. Werner, Phys. Rev. A 76 (2007) 032328.
[4] G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. Lett. 101 (2008) 060401.
[5] J. Kilian, in: Proceedings of the 20th ACM Symposium on Theory of Computing, ACM, New York, 1988, p. 20.
[6] M. Blum, SIGACT News 15 (1983) 23.
[7] C.H. Bennett, G. Brassard, C. Crépeau, M.H. Skubiszewska, in: Advances in Cryptology — Proceedings of CRYPTO'91, Springer, Berlin, 1991, p. 351.
[8] C. Crépeau, J. Mod. Opt. 41 (1994) 2455.
[9] A.C.C. Yao, in: Proceedings of the 27th ACM Symposium on Theory of Computing, ACM, New York, 1995, p. 67.
[10] C. Crépeau, J. van de Graaf, A. Tapp, in: Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'95), in: Lecture Notes in Computer Science, vol. 963, Springer, Berlin, 1995, p. 110.
[11] C.H. Bennett, G. Brassard, in: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984, IEEE, New York, 1984, pp. 175–179.
[12] A.K. Ekert, Phys. Rev. Lett. 67 (1991) 661.
[13] G. Brassard, C. Crépeau, R. Jozsa, D. Langlois, in: Proceedings of the 34th Annual IEEE Symposium on the Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, 1993, p. 362.

[14] A. Uhlmann, Rep. Math. Phys. 9 (1976) 273.
[15] A. Kitaev, D. Mayers, J. Preskill, Phys. Rev. A 69 (2004) 052326.
[16] H.P. Yuen, arXiv:quant-ph/0006109;
H.P. Yuen, arXiv:quant-ph/0305144;
H.P. Yuen, arXiv:quant-ph/0505132;
H.P. Yuen, arXiv:quant-ph/0702074.
[17] H.P. Yuen, arXiv:0808.2040.
[18] C.Y. Cheung, arXiv:quant-ph/0112120.
[19] R.W. Spekkens, T. Rudolph, Phys. Rev. A 65 (2001) 012310.
[20] K. Kraus, Ann. Phys. 64 (1971) 311.
[21] G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. A 80 (2009) 022339.
[22] G. Gutoski, J. Watrous, in: Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computation (STOC), 2007, pp. 565–574.
[23] G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. Lett. 101 (2008) 180501.
[24] A. Kent, Phys. Rev. Lett. 83 (1999) 1447.
[25] A. Kent, J. Cryptology 18 (2005) 313.
[26] W.F. Stinespring, Proc. Amer. Math. Soc. 6 (1955) 211.
[27] M. Ozawa, J. Math. Phys. 25 (1984) 79.
[28] D. Kretschmann, D. Schlingemann, R.F. Werner, J. Funct. Anal. 255 (2008) 1889.
[29] M. Sion, Pac. J. Math. 8 (1958) 171.
[30] S.P. Boyd, L. Vandenberghe, Convex Optimization, Cambridge University Press, Cambridge, 2008.