Reexamination of quantum bit commitment: The possible and the impossible

Giacomo Mauro D'Ariano,[1,*] Dennis Kretschmann,[2,3,†] Dirk Schlingemann,[3,4,‡] and Reinhard F. Werner[3,§]
[1]*Quantum Information Theory Group, Dipartimento di Fisica A. Volta, Università di Pavia, via Bassi 6, 27100 Pavia, Italy*
[2]*Centre for Quantum Computation, DAMTP, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, United Kingdom*
[3]*Institut für Mathematische Physik, Technische Universität Braunschweig, Mendelssohnstraße 3, 38106 Braunschweig, Germany*
[4]*ISI Foundation, Quantum Information Theory Unit, Viale S. Severo 65, 10133 Torino, Italy*
(Received 7 June 2006; revised manuscript received 10 July 2007; published 26 September 2007)

Bit commitment protocols whose security is based on the laws of quantum mechanics alone are generally held to be impossible. We give a strengthened and explicit proof of this result. We extend its scope to a much larger variety of protocols, which may have an arbitrary number of rounds, in which both classical and quantum information is exchanged, and which may include aborts and resets. Moreover, we do not consider the receiver to be bound to a fixed "honest" strategy, so that "anonymous state protocols," which were recently suggested as a possible way to beat the known no-go results, are also covered. We show that any concealing protocol allows the sender to find a cheating strategy, which is universal in the sense that it works against any strategy of the receiver. Moreover, if the concealing property holds only approximately, the cheat goes undetected with a high probability, which we explicitly estimate. The proof uses an explicit formalization of general two-party protocols, which is applicable to more general situations, and an estimate about the continuity of the Stinespring dilation of a general quantum channel. The result also provides a natural characterization of protocols that fall outside the standard setting of unlimited available technology and thus may allow secure bit commitment. We present such a protocol whose security, perhaps surprisingly, relies on decoherence in the receiver's laboratory.

DOI: 10.1103/PhysRevA.76.032328 PACS number(s): 03.67.Dd

I. INTRODUCTION

Bit commitment is a cryptographic primitive involving two mistrustful parties, conventionally called Alice and Bob. Alice is supposed to submit an encoded bit of information to Bob in such a way that Bob has (almost) no chance to identify the bit before Alice later decodes it for him, whereas Alice has (almost) no way of changing the value of the bit once she has submitted it: in technical terms, a good bit commitment protocol should be simultaneously *concealing* and *binding*.

Bit commitment has immediate practical applications and is also known to be a very powerful cryptographic primitive. It was conceived by Blum [1] as a building block for secure coin tossing. Bit commitment also allows one to implement secure oblivious transfer [2–4], which in turn is sufficient to establish secure two-party computation [5,6].

A standard example to illustrate bit commitment is for Alice to write 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 it by handing over the key to Bob. However, Bob has a well-equipped toolbox at home and may have been able to open the safe in the meantime. So while this scheme may offer reasonably good practical security, it is in principle insecure. Yet all bit commitment schemes that have wide currency today rely on such technological constraints: not on strongboxes and keys, but on unproven assumptions that certain computations are hard to perform. Several such protocols have been suggested, either computationally binding [1,7–9] or computationally concealing [10,11]. Cryptographers have long known that without such technological constraints, bit commitment (like any other interesting two-party cryptographic primitive) cannot be securely implemented in a classical world [5].

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 [12,13]—security is guaranteed by the laws of quantum physics alone.

A. Quantum bit commitment and the no-go theorem

The first quantum bit commitment protocol is due to Bennett and Brassard and appears in their famous 1984 quantum cryptography paper [12], in a version adapted to coin tossing. In their scheme, Alice commits to a bit value by preparing a sequence of photons in either of two mutually unbiased bases, in a way that the resulting quantum states are indistinguishable to Bob. The authors show that their protocol is secure against so-called *passive cheating*, in which Alice initially commits to the bit value k and then tries to unveil $1-k$ later. However, they also prove that Alice can cheat with a more sophisticated strategy, in which she initially prepares pairs of maximally entangled states instead, keeps one particle of each pair in her laboratory and sends the second particle to Bob. It is a direct consequence of the Einstein-Podolsky-Rosen (EPR) effect that Alice can then unveil either bit at the opening stage by measuring her particles in the appropriate basis and Bob has no way to detect the difference.

*dariano@unipv.it
†d.kretschmann@tu-bs.de
‡d.schlingemann@tu-bs.de
§r.werner@tu-bs.de

Subsequent proposals for bit commitment schemes tried to evade this type of attack by forcing the players to carry out measurements and communicate classically as they go through the protocol. At a 1993 conference Brassard *et al.* presented a bit commitment protocol [14] that was claimed and generally accepted to be unconditionally secure.

In 1996 it was then realized by Lo and Chau [15,16], and independently by Mayers [17–19], that all previously proposed bit commitment protocols are vulnerable to a generalized version of the EPR attack that renders the BB84 proposal insecure, a result they slightly extended to cover quantum bit commitment protocols in general. In essence, their proof goes as follows: 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 [20,21] 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, and Mayers argue that Alice can switch at will back and forth 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 nonbinding.

These results still hold true when both players are restricted by superselection rules [22]. 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. Spekkens and Rudolph [23] extended the no-go theorem by providing explicit bounds on the degree of concealment and bindingness that can be achieved simultaneously in any bit commitment protocol, some of which they showed can be saturated.

B. Two camps

In view of these negative results, subsequent research has primarily focused on bit commitment under plausible technological constraints, such as a limited classical [24,25] or quantum [26] memory or the difficulty of performing collective measurements [27]. In an alternative approach, researchers have slightly modified the standard setting to evade the no-go theorem: Kent [28,29] has shown that relativistic signaling constraints may facilitate secure bit commitment when Alice and Bob each run two labs a (large) distance apart and security is maintained through a continual exchange of messages. A different variant was introduced by Hardy and Kent [30] and independently by Aharonov *et al.* [31]: in *cheat-sensitive* bit commitment protocols, both players may have the chance to cheat, but face the risk of their fraud being detected by the adversary. Building on Kent's original proposal [32], the trade-off between bindingness and concealment in quantum *string* commitment protocols has recently been investigated [33–35].

At the same time, the Lo-Chau-Mayers no-go theorem [15,18] is continually being challenged. Yuen and others have repeatedly expressed doubts in Mayer's opaque paper [18], arguing that the no-go proof is not general enough to exclude all conceivable quantum bit commitment protocols. Several protocols have been proposed and claimed to circumvent the no-go theorem (see [36–40] and references therein, as well as the account in [41,42] of the controversy). These protocols seek to strengthen Bob's position with the help of "secret parameters" or "anonymous states," so that Alice lacks some information 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.

Two camps seem to have formed, a large one comprising most of the community, in which the impossibility of quantum bit commitment is accepted on the basis of the Lo-Chau-Mayers proof, and a smaller group of sceptics, which is not convinced, even though no provably secure protocol, and hence a counterexample to the no-go result, has surfaced so far.

It appears that much of this controversy stems from slightly differing approaches to the problem. A good way to pinpoint the basic disagreement is Kerckhoffs' principle, which goes back to the 19th century military cryptographer Auguste Kerckhoffs and is now universally embraced by cryptographers [43,44]. The principle states that the security of a cryptographic protocol should not rely on keeping parts of the algorithm secret. In the words of Schneier, "every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse" [45]. In this respect every secret parameter chosen by the human in a cryptographic protocol—e.g., a password—is regarded as a potential weakness. For this reason cryptographers usually think of their algorithms as being executed by machines, whose blueprints can be published without jeopardizing the security of the system.

Anonymous states and other secret parameters used in Yuen's protocols are apparently regarded as a violation of Kerckhoffs' principle, which suggests a restriction to fixed and automatizable strategies for both players. Deviations from these strategies are considered an attempted fraud. The Kerckhoffian security analysis then does not hold any provisions for the case in which *both* parties deviate from their "honest" strategies. Therefore Lo, Chau, and Mayers only consider the final committed state given that Bob sticks to his publicly known strategy, since Alice's cheat only has to work against this strategy. So while Kerckhoffs' principle is certainly high on the list of desiderata for cryptographic protocols, it appears that Lo, Chau, and Mayers only show that there is no bit commitment protocol *satisfying Kerckhoffs' principle*, whereas the next best thing—e.g., an anonymous state protocol–might still exist.

Another possible origin for disagreement is the style of Mayers' paper [18], along the lines of Mark Kac's dictum "A demonstration convinces a reasonable man; a proof convinces a stubborn man." [46] In this sense—i.e., according to the standards of "stubborn" mathematics or mathematical physics—Mayers gives merely a demonstration. Since the argument against Kerckhoffian protocols only involves the state directly after commitment, Mayers declares it irrelevant

to formalize the class of two-party protocols, even though an insufficiently specified domain usually leaves a no-go "theorem" rather fuzzy. Other aspects of the problem (e.g., the use of classical and quantum information together) get a similarly rough treatment. It hence appeared to us high time to convince ourselves, and hopefully some other stubborn men, of the exact scope and status of the no-bit-commitment statements.

C. Stronger no-go theorem: Overview and outline

In this contribution we propose to resolve the bit commitment controversy with a strengthened no-go theorem. We will give a precise description of general two-party protocols, which we hope no longer shows the hard work of keeping it fully explicit but still notationally manageable. This description should also be helpful for analyzing protocols for other tasks, involving any number of parties. Our description of bit commitment does not assume Kerckhoffs' principle, so that Bob is not honor bound to a particular course of action. Nevertheless, we show that any concealing protocol allows Alice a universal cheating strategy, working against all strategies of Bob simultaneously. Moreover, our result is stable against small errors, in the sense that nearly concealing protocols allow a nearly perfect cheat, with explicit universal error bounds. The result is based on a continuity theorem for Stinespring's representation [47], which generalizes Uhlmann's theorem from quantum states to channels.

Our proof includes a full treatment of classical and quantum information flow and also covers aborts and resets. It applies to bit commitment protocols with any (finite or infinite) number of rounds during each the commitment, holding, and opening phase. We only require that the expected number of rounds be finite. Moreover, the proof is not restricted to quantum systems on finite-dimensional Hilbert spaces. The strengthened no-go theorem shows the insecurity of all recently proposed bit commitment protocols [36–40]. A preliminary version of the proof, restricted to single-round commitments, has appeared in [48]. Our results generalize that of Ozawa [49] and recent work by Cheung [50], who showed that Alice can still cheat in protocols with secret parameters for the simpler case of perfect concealment and without a full reduction. Cheung's estimates [51] for approximately concealing protocols depend on the dimensions of the underlying Hilbert space and hence cannot rule out bit commitment protocols with high-dimensional or infinite-dimensional systems.

We also classify those protocols that fall outside the standard setting and thus may allow secure bit commitment. We propose such a bit commitment protocol whose security—perhaps paradoxically—relies on decoherence in Bob's laboratory. Interestingly, this protocol explores a purely quantum-mechanical effect: the distinction between the local erasure of information and the destruction of quantum correlations [56]. Well-known classical bit commitment protocols whose security relies on noisy communication channels are briefly reviewed, too.

The paper is organized as follows: In Sec. II we give a detailed description of the setup for quantum bit commitment protocols and list important types of protocols that fall within our definition. This will serve to specify the domain for the proof of the strengthened no-go theorem, which is then presented in Sec. III. In Sec. IV we briefly describe how to extend the no-go theorem to quantum bit commitment protocols in infinite-dimensional Hilbert spaces or with infinitely many rounds. Section V investigates provably secure bit commitment protocols whose security is built on decoherence in either Alice's or Bob's laboratory or in the transmission line. We conclude with a Summary and Discussion in Sec. VI. An appendix contains the necessary background on quantum states and channels, direct sums, and quantum-classical hybrid systems.

II. SETUP

In this section we describe the task of quantum bit commitment and define what a successful bit commitment protocol would have to achieve. We have attempted not to exclude any possibilities and have avoided all simplifications "without loss of generality" at this stage. In this way we hope to separate, more clearly than our predecessors, the definition of bit commitment to which the statement, "bit commitment is impossible," refers and, on the other hand, the simplifications which we will make in the course of the proof of this statement.

The analysis will be based solely on the principles of quantum mechanics, including classical physics. We do not consider relativistic signaling constraints, which are known to facilitate secure bit commitment [28,29]. For ease of presentation, we initially impose as a *finiteness condition* that all classical messages can only take finitely many values, that all quantum systems can be described in a finite dimensional Hilbert space, and that the total number of messages exchanged is uniformly bounded. These constraints will then be relaxed in Sec. IV.

A. Description in plain English

The basic task. Bit commitment is a cryptographic primitive involving two mistrustful parties, conventionally called Alice and Bob. Alice is supposed to submit an encoded bit of information to Bob in such a way that Bob has (almost) no chance to identify the bit before Alice decodes it for him and Alice has (almost) no way of changing the value of the bit after she has submitted it. In other words, Bob is interested in *binding* Alice to some commitment, whereas Alice would like to *conceal* her commitment from Bob.

Protocols and strategies. A *protocol* first of all 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 type of messages can depend on classical information generated previously. The collection of all these instructions will be called the *communication interface* of the protocol.

A particular plan for operating a local laboratory to supply the required messages is called a *strategy*. A strategy could determine that some message sent is obtained from a measurement on a system available in the local lab, but it could also specify the arbitrary invention of a classical value to be sent and the fresh preparation of an accompanying quantum system. We typically denote Alice's strategy by a and Bob's by b.

The second key element of the protocol specifies definite procedures for Alice to follow if she wants to commit the bit values 0 or 1, respectively. These special *honest strategies* will be denoted by a_0 and a_1.

Phases of the protocol. In any commitment scheme, we can distinguish three phases. The first is the *commitment phase*, in which Alice and Bob start from some (publicly known and trusted) shared quantum or classical state and go through a possibly complicated exchange of classical and quantum messages. By definition, at the end of this phase, the bit value is considered to be committed to Bob but, supposedly, concealed from him.

Alice and Bob then might split up for a while, without further communication. In this *holding phase* typically only local operations are possible; i.e., Bob might attempt to read the committed bit and Alice might attempt to prepare a cheat.

Finally they get in touch again to open the commitment. In the *opening phase*, Alice sends to Bob some classical or quantum information to reveal her commitment. 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 the bit value $k \in \{0,1\}$, indicating a successful commitment, or in a failure symbol "not OK," indicating an attempted cheat or abort.

A typical opening consists in Alice sending to Bob the value of the bit she claims to have committed, together will all the classical or quantum information needed for Bob to check this claim against his records. The protocol might also be ended in a *public opening*, which requires Alice and Bob to meet, bringing with them all quantum and classical systems in their possession, explaining what strategies they were using, and allowing Bob to choose arbitrary measurements on all these systems to verify, with Alice staying on to watch. That is, no possibility of cheating, withholding information, or making false claims about the outcome of verification exists in a public opening.

Conditions on successful protocols. We assume that Alice's strategies a_0 and a_1 can be distinguished with high probability by Bob's verification measurement: if Alice honestly played a_k, then Bob's measurement will result in the bit value k with probability $\geqslant(1-\eta)$ for some (small) $\eta \geqslant 0$. We call such a protocol η *verifiable*, or η *sound*. Since this condition depends only on the honest strategies, it is very easy to satisfy.

We call a protocol ε *concealing* if Alice's honest strategies cannot be distinguished by Bob (up to an error ε) before she opens the commitment. In general, of course, the probabilities he measures while applying his protocol b depend on whether Alice chooses a_0 or a_1. Here we require that no matter what strategy b Bob uses and no matter what measurement he makes, these probabilities never differ by more than ε throughout the commitment and holding phase. Note that the concealing condition makes no statement whatsoever about other strategies of Alice. If Alice cheats, there is usually nothing to be concealed anyway.

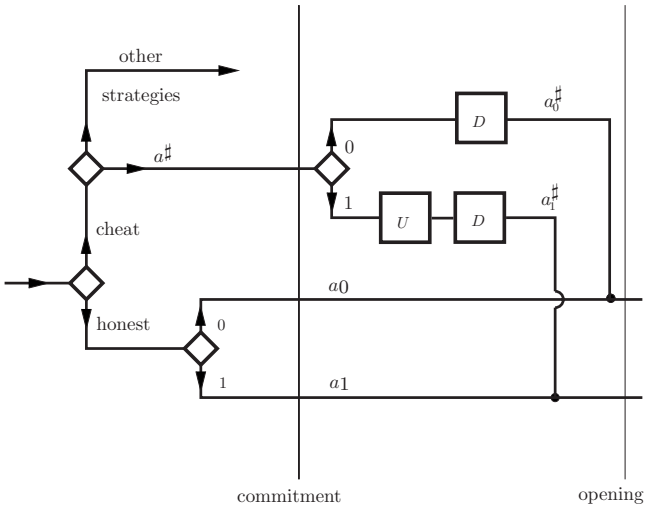

FIG. 1. Alice's basic strategic choices. Decisions she must take are indicated by diamonds, some actions necessary for a typical cheating strategy by squares. The cheating strategies $a_0^\sharp$ and $a_1^\sharp$ are identical throughout the commitment phase and might be equal to a purification of the honest strategy a_0. Then U indicates a unitary cheating transformation and D the introduction of suitable decoherence to reverse purification. In the opening phase the cheating strategies are identical to their honest counterparts.

A δ-*cheating strategy* for Alice is a pair of strategies $a_0^\sharp$ and $a_1^\sharp$ such that Bob cannot distinguish a_0 from $a_0^\sharp$, and a_1 from $a_1^\sharp$, better than with a probability difference δ, at any time, including the opening phase. Of course, these conditions would be trivially satisfied for $a_0=a_0^\sharp$ and $a_1=a_1^\sharp$. What makes $(a_0^\sharp,a_1^\sharp)$ cheating strategies is that Alice does not actually make the decision about the value of the bit until after the commitment phase. That is, the strategies $a_0^\sharp$ and $a_1^\sharp$ must be the same throughout the commitment phase and can only differ by local operations carried out in the holding or opening phase. Note, however, that Alice might have to decide from the outset that she wants to cheat, since the strategies $a_i^\sharp$ might be quite different from both a_0 and a_1. Figure 1 illustrates Alice's basic choices as she goes through the protocol. If no δ-cheating strategy exists for Alice, we call the protocol δ binding.

The condition we impose here is much stronger than the condition that Bob's standard verification measurements be fooled by the cheat (perhaps with a bound on the success probability): We require that no measurement whatsoever could detect a difference. With a public opening rule one could even say that after the cheat not even Alice herself could help Bob to tell the difference. Clearly, these conditions make it very hard for Alice to cheat. Therefore, our proof that Alice can still cheat under such conditions automatically includes all protocols with weaker conditions on successful cheats.

Real-time checks for cheating. It is perhaps helpful to point out the difference between two kinds of checks on Alice's honesty, which Bob might perform. We have granted

him unlimited technological power in the definition of ε concealing. But for running the protocol no such fantastic abilities are required and he will not actually do all those complicated tests. In fact, the concealing and binding properties of the protocol cannot be ascertained by any practical tests, but are there to be checked theoretically by Alice and Bob on the basis of the publicly available description of the protocol. It is on the basis of such considerations that Alice and Bob will consent to use the protocol in the first place.

During a single run of the protocol, Bob can employ some tests on Alice's behavior as part of the protocol. If Bob suspects a problem, he may be entitled to calling an abort of the protocol (clearly a classical message) and the procedure would start at the beginning. The total number of such resets must be limited on the grounds of bounding Alice's probability of cheating. The possibility of such checks at run time is the main reason why we must consider protocols with a large number of rounds, possibly differing from run to run.

Result. We will prove in Sec. III G that any protocol which is ε concealing allows a δ-cheating strategy for Alice, where $\delta \leqslant 2\sqrt{\varepsilon}$. These bounds coincide with those obtained by Spekkens and Rudolph [23] in the Kerckhoffian setting.

As illustrated in Fig. 1, Alice's cheating strategy $a^\sharp$ consists in playing a purification of the honest strategy a_0 throughout the commitment and holding phase. If she then opts for the bit value $k=1$ instead, she will apply a unitary operation U on the purifying system and thenceforth follow the honest strategy a_1.

B. Formal description of protocols

In this section we will cast the above description more explicitly into the formalism of quantum theory. Thereby we further reduce possible ambiguities in the statement of the problem, but also prepare the notation for the proof.

The basic formalism of quantum theory is briefly reviewed in the Appendix. We will generally identify systems by their observable algebras. This has the advantage that combinations of classical and quantum information are naturally covered: a quantum system with Hilbert space $\mathcal{H}$ is then represented by the algebra $\mathcal{B}(\mathcal{H})$ of operators on $\mathcal{H}$, and a system characterized by a classical parameter x, and has Hilbert space $\mathcal{H}_x$ in that case is described by the direct sum $\oplus_x \mathcal{B}(\mathcal{H}_x)$. A state on such an algebra is of the form $\oplus_x p_x \rho_x$ and is specified first by a probability distribution p_x for the x's and second by a collection of density operators ρ_x on $\mathcal{H}_x$, which are used to compute expectations if the value of the classical parameter is known to be x. Since this formalism for handling classical information in protocols is not generally familiar, we describe it in some more detail in the Appendix.

Many algebras (indexed by the nodes of the communication tree) will appear in the description of the protocol, indicating that with each operation the type of quantum system in the respective laboratory might change completely. By choosing the laboratory algebras large enough this dependence might be avoided. However, even when the laboratory systems remain the same, it is helpful to keep the distinguishing indices for keeping track of the progress of the protocol.

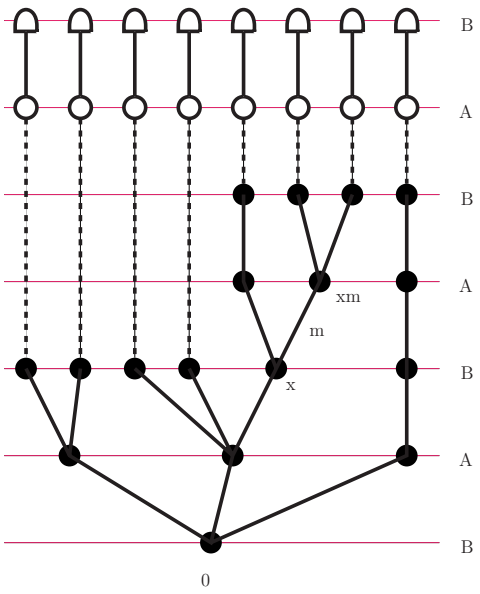

FIG. 2. (Color online) Example of a communication tree. Each node corresponds to one history of classical communications, with the different lines from each node representing a possible classical signal. The dashed lines represent the holding phase, in which no communication occurs, followed by the opening move (open circle) by Alice and a measurement by Bob.

1. Communication tree

At every stage of the protocol a certain amount of shared classical information will have accumulated. Classical information never gets lost, so the stages of the protocol, together with the currently available classical information, naturally form the nodes of a tree, which we call the *communication tree*. An example is depicted in Fig. 2. Every node x carries the following information

(i) Whose turn is it, Alice's or Bob's? This follows from the position of the node in the tree, when we assume, without loss of generality, that Bob always starts and from then turns alternate.

(ii) What are the classical signals which might be sent from this person to the other? The admissible signals form a finite set M_x by assumption. This set labels the branches continuing from this node to successor nodes which we denote by $x'=xm$, for $m \in M_x$.

(iii) For each possible classical signal, what kind of quantum system is accompanying it? If the classical message is m, we take its observable algebra to be $\mathcal{M}_m^x$ and assume this to be the full algebra of $d \times d$ matrices for some $d=d(x,m) < \infty$. The value $d(x,m)=1$ ($\simeq$ no accompanying quantum system) is a possible choice.

(iv) Each node x is completely characterized by the entire history of the classical messages exchanged between Alice and Bob; i.e., we can write $x=m_1 m_2 \cdots m_N$.

At every node, we denote the observable algebras of Alice's and Bob's laboratories by $\mathcal{A}_x$ and $\mathcal{B}_x$, respectively. These are only partly determined by the communication interface and depend on the strategy, which we sometimes em-

phasize by writing $\mathcal{A}_x(a)$ and $\mathcal{B}_x(b)$. The description of the communication step below shows in detail how these algebras develop as one moves along the communication tree. Let X_c denote the set of nodes at which a commitment is supposed to be reached. Since only local operations and the opening phase follow, we can consider these as the leaves of the communication tree. The joint observable algebra at that stage is

$$\bigoplus_{x\in X_c} \mathcal{A}_x(a)\otimes\mathcal{B}_x(b) \tag{1}$$

(see the Appendix for the interpretation of direct sums). The algebras of Alice and Bob could themselves be direct sums, representing classical information only available to Alice and Bob, respectively, but we do not look at this for the moment.

2. Elementary communication step

Now consider some node x and assume that it is Alice's turn (everything holds mutatis mutandis for Bob). We know that some message $m\in M_x$ is expected from Alice, accompanied by a quantum system with observable algebra $\mathcal{M}_m^x$. The most general way of doing this is a quantum operation sending states on $\mathcal{A}_x$ to states on $\oplus_m \mathcal{A}_{xm}\otimes\mathcal{M}_m^x$. Written in the Heisenberg picture Alice hence chooses a channel (completely positive normalized map; cf. Appendix)

$$T_x(a)\colon \bigoplus_{m\in M_x} \mathcal{A}_{xm}(a)\otimes\mathcal{M}_m^x \to \mathcal{A}_x(a), \tag{2}$$

$$\mathcal{B}_{xm}(b) = \mathcal{M}_m^x \otimes \mathcal{B}_x(b). \tag{3}$$

Here we have added a parameter a to T_x to make it clear that choosing these channels for all x is precisely what defines Alice's strategy. Note that the choice of the channel includes that of their domain and range algebras. The channel $T_x(a)$, together with the input state, determines the probabilities for the classical outcomes m. Of course, the channel could be one that simply forces one of the results. Hence m could equally well be the result of Alice's free choice of strategy or of a measurement on a system she recently obtained from Bob. If m is found, Alice also splits the output system into a part $\mathcal{A}_{xm}(a)$, which Alice keeps, and the part $\mathcal{M}_m^x$ she sends to Bob. This splitting is included in the specification of $T_x(a)$. That $\mathcal{M}_m^x$ changes ownership is expressed in the above equation by including it in Bob's algebra at the next round (i.e., $\mathcal{B}_{xm}$) as a tensor factor. At Bob's nodes everything is the same, but since we always order tensor factors as Alice $\otimes$ Message $\otimes$ Bob, the analogs of the above equations at Bob's nodes are

$$T_x(b)\colon \bigoplus_{m\in M_x} \mathcal{M}_m^x\otimes\mathcal{B}_{xm}(b) \to \mathcal{B}_x(b), \tag{4}$$

$$\mathcal{A}_{xm}(a) = \mathcal{A}_x(a)\otimes\mathcal{M}_m^x. \tag{5}$$

3. From commencement to commitment

We assume that Alice and Bob initially share the quantum or classical state $\rho_0\colon \mathcal{A}_0\otimes\mathcal{B}_0\to\mathbb{C}$. The joint state

$$\rho_c(a,b,\rho_0)\colon \bigoplus_{x\in X_c} \mathcal{A}_x(a)\otimes\mathcal{B}_x(b)\to\mathbb{C} \tag{6}$$

at commitment time is then $\rho_c(a,b,\rho_0)=\rho_0\circ T(a,b)$, where

$$T_c(a,b)\colon \bigoplus_{x\in X_c} \mathcal{A}_x(a)\otimes\mathcal{B}_x(b)\to\mathcal{A}_0\otimes\mathcal{B}_0 \tag{7}$$

is the direct sum channel that arises from the concatenation of all the elementary step channels $T_x(a)$ and $T_x(b)$ up to commitment time. Of course, Eq. (7) holds correspondingly for the shared states at all other stages of the protocol. In particular, the final state $\rho_f(a,b,\rho_0)$ on which Bob carries out the verification measurement arises from the initial state ρ_0 by means of a quantum operation

$$T_f(a,b)\colon \bigoplus_{x\in X_f} \mathcal{A}_x(a)\otimes\mathcal{B}_x(b)\to\mathcal{A}_0\otimes\mathcal{B}_0, \tag{8}$$

where X_f is the collection of all the leaves of the communication tree. We will assume that the initial state $\rho_0\colon \mathcal{A}_0\otimes\mathcal{B}_0\to\mathbb{C}$ is known to both Alice and Bob and henceforth write $\rho_c(a,b)$ instead of $\rho_c(a,b,\rho_0)$, and $\rho_f(a,b)$ instead of $\rho_f(a,b,\rho_0)$, to streamline the presentation.

4. Can Bob distinguish Alice's strategies?

In the concealing condition, as well as in the description of cheating strategies, it is important to decide whether Bob can distinguish two strategies of Alice at commitment time. Clearly, this depends only on the restriction $\rho_c^B(a_i,b)$ of the state $\rho_c(a_i,b)$ to Bob's laboratory, which has observable algebra $\oplus_x\mathcal{B}_x$.

The security criterion given in Sec. II A asks for the largest probability difference obtainable by Bob. It is convenient to express this in a trace norm difference: the largest difference of expectations in "yes-no" experiments with density matrices ρ_1,ρ_2 is $\sup_F|\mathrm{tr}(\rho_1-\rho_2)F|$, where F ranges over all so-called *effects* F with $0\leqslant F\leqslant 1$. That is, the largest probability difference is $\frac{1}{2}\|\rho_1-\rho_2\|_1$, where $\|\cdot\|_1$ denotes the trace norm. This naturally leads us to the following definition of concealing protocols and cheating strategies:

Definition 1. (Concealing). We say that a protocol with a strategy pair (a_0,a_1) for Alice is ε concealing iff for all strategies b of Bob

$$\|\rho_c^B(a_0,b)-\rho_c^B(a_1,b)\|_1\leqslant 2\varepsilon. \tag{9}$$

When this condition holds with $\varepsilon=0$, we say that the protocol is perfectly concealing. ■

Note that one possible measuring strategy for Bob is to actually make the measurement at an earlier time, record the result, and send only dummy messages to Alice afterwards. So saying that two strategies are ε equivalent *at* some stage is the same as saying that they are equivalent *up to* that stage of the protocol. Hence the ε-concealing condition implies the only apparently stronger statement that at no time during the commitment phase Bob is able to discriminate the honest commitments better than with probability ε.

Definition 2. (Cheating). A pair of strategies $(a_0^\sharp,a_1^\sharp)$ for Alice that coincide until after the commitment phase is called a δ-cheating strategy iff

$$\|\rho_f^B(a_i^\sharp,b)-\rho_f^B(a_i,b)\|_1 \leqslant 2\delta, \tag{10}$$

for Alice's honest strategies (a_0,a_1), $i=0,1$ and all of Bob's strategies b. ■

Definition 2 requires a cheating strategy to work against *all* of Bob's strategies—not only against some *fixed* strategy, as suggested by Kerckhoffs' principle. We will show in Sec. III G that Alice can always find such a universally good cheating strategy. As explained in the Introduction, this extends the no-go theorem to protocols relying on secret parameters or "anonymous states." If Bob's strategy b is supposed to be fixed and publicly known in Eq. (10), our no-go proof will reduce in essence to the one obtained previously by Lo, Chau, and Mayers [15–18].

C. Protocols covered by our definition

In this section we describe some ideas from the literature about possible protocols, in increasing complexity. Of course, none of them are ultimately successful. But this is in many cases not obvious from the outset, so these ideas serve well to illustrate the richness of two-party protocols as formalized in our scheme.

1. Beginning

As explained in the Introduction, the first observation concerning quantum bit commitment was made in the classic paper of Bennett and Brassard on quantum cryptography [12]. In this basic scenario the commitment phase has only one round, in which Alice prepares one of two orthogonal Bell states $\psi_0,\psi_1 \in \mathcal{H}_A \otimes \mathcal{H}_B$. These have the same restriction on Bob's system, so the protocol is perfectly concealing. But they are also connected by a unitary on Alice's side (as all maximally entangled states are), and this unitary constitutes her *sneak flip* cheating strategy, which under these circumstances also works perfectly.

2. Alice sends a state

The natural generalization of this protocol is to replace the Bell states by arbitrary pure states generated by Alice [15,18]. When these have the same restriction on Bob's side, they are purifications of the same state and hence connected by a partial isometry on Alice's side, which serves as a sneak flip operation. A crucial step is now to go away from perfect concealment [$\varepsilon=0$ in Eq. (9)], which seems to have been considered first in [18]. In this case one has to use a continuity result for purifications: i.e., that nearby states have nearby purifications. In other words, one needs an estimate [21] of Uhlmann's fidelity (which measures the distance between purifying vectors) and the trace norm.

3. Classical communication

Classical communication occurs naturally in cryptographic protocols, so it needs to be included in the analysis. In contrast to some of our predecessors, who choose a purely quantum description from the outset, we treat classical information explicitly throughout. In particular, classical information in the Lo-Chau-Mayers approach is treated quantum mechanically and sent over noiseless quantum channels, while our description explicitly allows information transfer over classical channels and thus provides a natural setting to include purely classical protocols in the analysis.

Cheating becomes harder for Alice if the protocol requires some exchange of classical information, for she no longer has full control over the purification spaces of the two commitment states. Roughly speaking, unitaries which introduce superpositions of states, which belong to different classical values already sent to Bob, are forbidden. In the formalism introduced above this means that Alice has to find a cheating unitary for every classical communication history x.

Mayers' heuristic paper [18] has some provisions for this case by sending classical values to a special quantum repository in the environment and effectively coherentifying all classical information. In contrast, in this text the classical communication flow is treated explicitly and, in fact, emerges naturally as a framework for the description of the protocol. This approach should also prove helpful in the analysis of other cryptographic tasks.

4. Bob supplies the paper

The protocols so far were characterized by the property that Bob really had no strategic choices to make during the commitment phase. Hence the state at the end of the commitment phase, written in our scheme as $\rho_c(a,b)$, really does not depend on Bob's strategy b. So Alice only has to connect the purifications of two states which are explicitly known to her. Clearly, her task of finding a clever sneak flip becomes harder if there is a proper dependence on b. Lo, Chau, and Mayers restrict their analysis to those protocols in which Bob follows a specified "honest" strategy $b_\star$, which is assumed to be publicly known in accordance with Kerckhoffs' principle. In these cases, Alice knows how to cheat and the no-go result immediately applies.

As explained in the Introduction, we do not require that Bob follows such a publicly known standard strategy. Alice then indeed has to find a sneak flip working for all of Bob's admissible strategies b. The easiest such protocol begins with Bob sending a system to Alice, in some state known only to him (in [38] this is called an *anonymous* state). The honest strategies require Alice to encode the bit by using this system in some way and then returning a committing system to Bob. Effectively Alice now chooses not a *state* but a *channel* to encode her commitment. The purification idea and Uhlmann fidelity estimate no longer work for this, so these protocols are not covered by Lo, Chau, and Mayers. Instead, the purification construction has to be generalized to the Stinespring representation of channels and an appropriate continuity result has to be shown. This will be done in Sec. III.

5. Decoherence monster in Bob's laboratory

That the idea of states supplied by Bob may introduce interesting new aspects is demonstrated by a scenario which is not a bit commitment protocol in the sense of this section, because it makes additional assumptions about things happening in Bob's laboratory: Suppose that after Bob has sent some quantum state to Alice, a decoherence monster (such as

the cleaning service) enters his lablaboratory and all quantum information is destroyed. Only his classical records survive. That is, he still knows what preparation he made, but cannot use the entangled records he made during the preparation. Now suppose that Alice and Bob can rely on this happening. Then they can design a bit commitment protocol that works. So, paradoxically, the monster strengthens Bob's position, because it weakens the assumptions about his ability to break the concealment. Hence one can make protocols which are binding in the strong sense described above, but concealing only if we assume that coherence in Bob's lab is indeed destroyed. We will analyze this possibility in Sec. V B.

6. Alice can choose more strategies

An apparent generalization would allow Alice to choose her honest strategy a_0 at will from some set A_0 of honest strategies and a_1 from A_1. The idea is that now some $a_0 \in \mathsf{A}_0$ might well be distinguishable from some $a_1 \in \mathsf{A}_1$ for Bob. Concealment under such circumstances means that Bob, on seeing data compatible with some a_0 during the commitment or holding phase, can never be sure that they do not come from a certain a_1. In other words, for every $a_0 \in \mathsf{A}_0$ there must be an ε-equivalent strategy $a_1 \in \mathsf{A}_1$. But then, according to our result, Alice might develop a sneak flip attack on the basis of these two protocols alone.

7. More communication in the holding phase

In Sec. II A, we excluded any communication in the holding phase and, apart from a single message from Alice to Bob, also in the opening phase. There is, however, no problem to allow such communication, and some protocols, like Kent's protocol using relativistic signal speed constraints [28,29], require a lot of communication in the holding phase.

Of course, protocols with no rounds at all in the holding phase are directly covered by our definition. The only strategic difference between holding and commitment phase is that Alice's cheating strategies $a_0^\sharp$ and $a_1^\sharp$ are only required to coincide during the commitment phase. She might start cheating with different tricks for 0 and 1 during the holding phase.

Clearly, declaring the holding phase a part of the commitment phase only weakens Alice's cheating possibility. However, she does not need these extra options anyway: a sneak flip attack at the end of the holding phase is always possible, as we show.

8. Aborts and resets

Often in cryptography one considers protocols which allow the parties to call an "abort." We can distinguish two kinds of abort: when a *constructive abort*, or *reset*, occurs, the protocol is started anew, whereas at a *full abort* the whole protocol is terminated as unsuccessful.

Both kinds of aborts are covered in our scheme, but they would be typical of different phases. Resets are quite natural in the commitment phase. For example, Bob might make a test measurement on some message he receives and refuse to continue if there is a slight deviation from what is expected from Alice playing honest. A reasonable requirement at this point is that the probability for reaching a commitment after some number of rounds with an honest Alice be positive. Then allowing even more retrials one could bring the probability for reaching commitment close to 1 and allow some arbitrary choice in the remaining cases—i.e., if the allotted total number of rounds is exhausted without a commitment. In this way one would get a protocol satisfying our finiteness condition, while retaining the potential value of resets for a commitment protocol. Strictly speaking, resets can only occur during the commitment phase, since we have demanded a partitioning of each protocol run into three successive phases (without relapses into earlier phases). However, the holding phase can be essentially united with the commitment phase (see Sec. II C 7). Hence we can effectively also cover constructive aborts during the holding phase.

In the opening phase we can consider *full*, or destructive, aborts. This is a move right to an endpoint of the communication tree, labeled accordingly. Clearly this possibility weakens Bob's discrimination powers and makes it much easier to cheat for Alice. In particular, each sneak flip attack becomes successful. Therefore, the abort possibility does not seem to present any interesting strategic options for quantum bit commitment. The proof in Sec. III shows that this is indeed the case.

9. Concatenated protocols

Sometimes one considers settings in which a variety of different cryptographic protocols are run in parallel or in succession, usually with dependent inputs. Obtaining bounds on the security of concatenated protocols in terms of the security parameters of their component parts is often far from straightforward and a subject of ongoing research even in classical cryptography [52]. However, in this work we are chiefly concerned with impossibility results, which easily transfer to concatenated protocols: Running a finite number of (possibly different) bit commitment protocols in parallel or succession and assuming that those protocols all fall into the framework described in this section, the concatenated protocol is again a quantum bit commitment protocol, with suitably enlarged Hilbert and classical messenger spaces and possibly a larger number of rounds. Since the latter protocol is covered by our impossibility result, concatenating finitely many insecure bit commitment protocols cannot help to establish secure bit commitment.

The formulation of two party protocols that we describe in Sec. II B is by no means limited to quantum bit commitment and hence could also be used to model larger cryptographic environments, of which quantum bit commitment might be a subroutine. In Fig. 2, such a protocol would appear as a subtree. Concealment and bindingness would have to be guaranteed for the entire tree and hence, by restriction, for the subtree. Thus, no two-party cryptographic protocol covered by the framework described in Sec. II B can contain a secure bit commitment protocol.

The composability analysis is of course much more involved for *secure* protocols. The security proof we provide in Sec. V B for the decoherence monster protocol in general only applies to the protocol as a stand-alone object. If this

protocol is then used as a subroutine in a larger and complicated cryptographic context, the security analysis will usually have to be tailored to the specific protocol. Fortunately, at least the norm of complete boundedness (cb-norm) estimates we use in the proof of theorem 12 are stabilized distance measures and hence well behaved under concatenation (cf. the Appendix).

III. PROOF

In the exposition of the task of bit commitment and the admissible protocols we have tried not to restrict generality by simplifying assumptions, in order not to weaken the scope of the no-go theorem. This leads to a rather wild class of strategies to be considered: arbitrarily many rounds of communication of varying length, infinite-dimensional local laboratory Hilbert spaces, and all that. Clearly, in the course of the proof we want to get rid of this generality. The main idea for simplifications is that obviously inferior methods of analysis for Bob, or inferior cheating methods for Alice, need not be considered. We therefore begin with an explanation of what it means that one strategy is "obviously inferior," or *weaker*, than another (see Sec. III A).

The first application of this idea is the process of *purification*, by which a general strategy is turned into another one, which avoids all measurements not demanded by the communication interface and turns all decohering operations into coherent information transfer to ancillas. Stinespring's dilation theorem guarantees that this can always be done. We explain in Sec. III B how the purifications result in *locally coherent strategies*, which will be crucial for Alice's cheat later on and have been a part of all no-go results.

Once a player has chosen a locally coherent strategy, it is possible to reduce the laboratory spaces considerably. For example, if a strategy requires the choice of a mixed state, this state may have an infinite-dimensional support Hilbert space. Its purification, however, is a single vector, so up to a unitary transformation, which can be absorbed into subsequent operations, it suffices to take a one-dimensional Hilbert space. We show that this works for operations as well: for every locally coherent strategy there is a stronger one (in the sense of Sec. III A), using only finite-dimensional Hilbert spaces, with a universal dimension bound depending only on the dimension of quantum messages exchanged so far and the trusted ressources shared initially. In particular, an infinite-dimensional laboratory space will not give more power to Bob. This will be shown in Sec. III C and leads to the consequence that effectively (up to any desired level of accuracy) we need only consider a finite number of strategies for Bob.

The next step is in some sense a dual of purification: purification means that we can avoid measurements during a protocol, deferring all such operations to the final measurement. Similarly, we can move the acts of decision making during the protocol to the very beginning by introducing a *strategy register* (see Sec. III D), which is described in the Hilbert space $\ell^2(S)$, for some finite set S of strategies. The choice of a strategy is then expressed by preparing some initial state of the strategy register and then letting controlled unitaries transcribe this information into suitable operations at all later rounds. Let us denote by b_σ Bob's strategy of installing the strategy register mechanism and preparing the initial state σ for that register. The state $\rho_c(a,b_\sigma)$ at commitment time then depends linearly on σ, and after specifying the trusted initial state ρ_0 and tracing out Alice's laboratory, we find a channel $\Gamma^B(a)$ depending on Alice's strategy a, such that

$$\Gamma^B(a): \bigoplus_{x\in X_c} \mathcal{B}_x \to \mathcal{B}(\ell^2(S)), \tag{11}$$

$$\mathrm{tr}\sigma\Gamma^B(a)(B) = \mathrm{tr}\rho_c^B(a,b_\sigma)B, \tag{12}$$

for all $B \in \oplus_x \mathcal{B}_x$. This channel now summarizes everything that Bob can possibly learn about Alice's strategy by choosing his own strategy and making a measurement in his laboratory after the commitment. In a simple, purely Kerckhoffian scenario the analogous object is just the state at commitment time, since one does not allow Bob a choice of different legitimate strategies. However, in our more general framework we do need to consider the dependence on σ and correspondingly, cheats which work uniformly well for all σ.

As an instructive special case, we next suppose that the protocol is *perfectly* concealing, which is expressed by $\Gamma^B(a_0)=\Gamma^B(a_1)$. We show in Sec. III E that Alice then has a perfect cheat. Its existence is guaranteed by the uniqueness clause in the Stinespring dilation theorem. From this prototype of Alice's cheat one can see how an approximate cheat in response to approximate concealment $\Gamma^B(a_0)\approx\Gamma^B(a_1)$ should work.

In the next section we look more carefully into the kind of approximation $\Gamma^B(a_0)\approx\Gamma^B(a_1)$ sufficient to draw the desired conclusion. It turns out that we need to consider a special attempt of concealment breaking for Bob: namely keeping an entangled record of the strategy register and making a joint measurement on the rest of his system and this "backup copy" after commitment. Clearly, this is a legitimate attempt in our framework and hence must already be implicit in the strategies controlled by the strategy register. However, making this scheme explicit provides the right kind of norm (cb norm) on channels so that a small $\|\Gamma^B(a_0)-\Gamma^B(a_1)\|_{cb}$ guarantees the existence of an approximately ideal cheat. The technical result guaranteeing this is a new continuity theorem [46] for the Stinespring dilation construction, which we review in Sec. III G.

A. Comparing the strength of strategies

Consider two strategies a and a' of Alice. We will say that a' is *stronger* than a if whatever Alice can achieve by strategy a she can also achieve by a'. More explicitly, we require that there exists a suitable *revert* operation $R_x: \mathcal{A}_x(a) \to \mathcal{A}_x(a')$ bringing Alice back to strategy a at whatever node x she so chooses (observe the direction of arrows due to the Heisenberg picture). That she actually comes back to a is guaranteed inductively; i.e., we require that

$$R_x T_x(a) = T_x(a') \bigoplus_{m\in M_x} (R_{xm} \otimes \mathrm{id}_{\mathcal{M}_m^x}) \tag{13}$$

at Alice's nodes and

$$R_{xm} = R_x \otimes \mathrm{id}_{\mathcal{M}_m^x} \tag{14}$$

at Bob's nodes, where $\mathrm{id}_{\mathcal{M}_m^x}$ denotes the identity operation on $\mathcal{M}_m^x$. Tracing this all the way back to the root of the tree we get, for any of Bob's protocols b and for any stage of the protocol, in particular for the commitment stage X_c,

$$\mathrm{tr}\rho_c(a,b)(\bigoplus_x F_x \otimes G_x) = \mathrm{tr}\rho_c(a',b)(\bigoplus_x R_x(F_x) \otimes G_x). \tag{15}$$

Taking $F_x = \mathbf{1}_x$ in Eq. (15) (corresponding to the partial trace over Alice's laboratory space in the Schrödinger picture), we see that Bob's subsystems are completely unaffected; i.e., Bob will never be able to tell the difference between a and a'. The strategic significance of passing to a stronger strategy is different for Alice and for Bob.

For Bob a stronger b' is just another strategy to be considered in the concealing condition and in the condition for a successful cheat. Since Bob does not lose any discriminating power in playing coherent, Alice (and we) might as well assume that he is always using the strongest strategy available. This simplifies the analysis, as we will see in more detail below.

For an honest Alice there is no option. Whatever the honest strategies a_0 and a_1 specify, she has to follow. However, since Bob will never know the difference, it is easy to check from the definitions of concealing and binding in Sec. II B that whenever (a_0, a_1) is a bit commitment protocol with security parameters ε and δ, then so is any pair of stronger strategies (a_0', a_1'), with the same parameters. Hence we could assume for the sake of an impossibility proof that Alice's honest strategies are strengthened in some way. However, there is hardly an advantage in that assumption, and we will not do so.

For a cheating Alice, using all the power of her infinitely well equipped laboratory, and hence using the strongest available strategies is clearly the best choice. Indeed, this will be the only difference between the honest and the cheating strategies during the commitment phase: these consists of playing until commitment, a particular strengthening of an honest strategy: namely, the local purification discussed in the next subsection.

B. Local purification

Intuitively, maintaining coherence during quantum operations is more demanding than allowing thermal noise and other sources of decoherence to have their way. Therefore, doing only those measurements needed for satisfying the communication interface rules, but avoiding all other decoherence, should lead to a stronger protocol in the sense of Sec. III A.

The simplified "locally coherent" strategies are more easily expressed in terms of operators acting on Hilbert spaces than by superoperators acting on algebras. Therefore we need a notation for the message Hilbert spaces as well; i.e., we set $\mathcal{M}_m^x = \mathcal{B}(\mathcal{K}_m^x)$, where $\dim \mathcal{K}_m^x = d(x,m)$ is the dimension parameter from the description of the communication tree in Sec. II B 1.

Definition 3. (locally coherent strategy). We call a strategy a of Alice locally coherent iff for all communication nodes x we have $\mathcal{A}_x(a) = \mathcal{B}(\mathcal{H}_x(a))$ and, at all of Alice's nodes, the quantum channel $T_x(a): \oplus_m \mathcal{A}_{xm}(a) \otimes \mathcal{M}_m^x \to \mathcal{A}_x(a)$ from Eq. (2) is given by operators

$$V_{x,m}(a): \mathcal{H}_x(a) \to \mathcal{H}_{xm}(a) \otimes \mathcal{K}_m^x \tag{16}$$

such that

$$T_x(a)(\bigoplus_m A_m \otimes Y_m) = \sum_m V_{x,m}(a)^*(A_m \otimes Y_m)V_{x,m}(a) \tag{17}$$

for all $A_m \in \mathcal{B}(\mathcal{H}_{xm}(a))$ and $Y_m \in \mathcal{B}(\mathcal{K}_m^x)$. ■

The point here is that each summand in this $T_x(a)$ is *pure*—i.e., given by a single Kraus operator $V_{x,m}(a)$. This is equivalent to the property that the mth term in this sum cannot be decomposed into a nontrivial sum of other completely positive maps, which would in turn correspond to the extraction of further classical information. Using a nonpure map in a strategy would therefore mean to exercise less than the maximal control allowed by quantum theory. Note that m is in general a random outcome, but Alice can make it deterministic by choosing her strategy a corresponding to $V_{x,m}(a) = \delta_{m,m_0} V_x$, with an isometry V_x.

There is a canonical way to convert any strategy into a locally coherent one, which is provided by the basic structure theorem for completely positive maps. We state it in a form appropriate for the finite-dimensional case which is needed here. We refer to Paulsen's text [57] for further details and the proof.

Proposition 1. (Stinespring dilation). Let $\mathcal{A}$ be a finite dimensional C^* algebra, $\mathcal{H}$ a Hilbert space, and $T: \mathcal{A} \to \mathcal{B}(\mathcal{H})$ a completely positive map. Then there is another Hilbert space $\mathcal{K}$, a *-representation $\pi: \mathcal{A} \to \mathcal{B}(\mathcal{K})$, and a bounded operator $V: \mathcal{H} \to \mathcal{K}$ such that, for all $A \in \mathcal{A}$,

$$T(A) = V^* \pi(A) V. \tag{18}$$

If $(\mathcal{K}_0, \pi_0, V_0)$ and $(\mathcal{K}_1, \pi_1, V_1)$ are two such representations, there is a partial isometry $U: \mathcal{K}_0 \to \mathcal{K}_1$ such that

$$UV_0 = V_1, \tag{19}$$

$$U^* V_1 = V_0, \tag{20}$$

$$U\pi_0(A) = \pi_1(A)U, \tag{21}$$

for all $A \in \mathcal{A}$. ■

We will use this proposition several times, but ignore the uniqueness statement for the moment. Then we can iteratively generate a locally coherent protocol $\breve{a}$ from a, together with the required revert operations showing that $\breve{a}$ is indeed stronger than a. Suppose the space $\mathcal{H}_x(\breve{a})$ and the revert channel $R_x: \mathcal{A}_x(a) \to \mathcal{B}(\mathcal{H}_x(\breve{a})) = \mathcal{A}_x(\breve{a})$ has already been defined along with these objects for all earlier nodes. We need to extend this definition to all successor nodes xm. If the node x belongs to Bob, there is nothing to do since Eq. (14) explicitly defines R_{xm}. At Alice's nodes, we apply the Stinespring theorem to the composition:

$$R_x T_x(a): \bigoplus_{m \in M_x} \mathcal{A}_{xm}(a) \otimes \mathcal{M}_m^x \to \mathcal{B}(\mathcal{H}_x(\check{a})). \tag{22}$$

The dilation theorem then provides us with a representation π_x of $\oplus_{m\in M_x}\mathcal{A}_{xm}(a)\otimes\mathcal{M}_m^x$ on some Hilbert space $\mathcal{K}_x$ and an isometry $V_x:\mathcal{H}_x(\check{a})\to\mathcal{K}_x$. Now the projections P_m in $\oplus_{m\in M_x}\mathcal{A}_{xm}(a)\otimes\mathcal{M}_m^x$ which correspond to the direct sum decomposition over m are mapped by π_x to projections on $\mathcal{K}_x$, so we get a decomposition into orthogonal subspaces $\mathcal{K}_x=\oplus_m\pi_x(P_m)\mathcal{K}_x$. Since the P_m commute with all other elements of the algebra, the projections $\pi_x(P_m)$ commute with all $\pi_x(A)$, and $A\mapsto\pi_x(P_m)\pi_x(A)$ becomes a representation on $\pi_x(P_m)\mathcal{K}_x$. This representation can be restricted to the message algebra $\mathcal{M}_m^x$, and since the representation of a full matrix algebra is unique up to multiplicity (and up to unitary equivalence indicated by "≅" in the equations below), we can split the subspace $\pi_x(P_m)\mathcal{K}_x$ into a tensor product:

$$\pi_x(P_m)\mathcal{K}_x \cong \mathcal{H}_{xm}(\check{a}) \otimes \mathcal{K}_m^x, \tag{23}$$

$$\pi_x(1\otimes X)\pi_x(P_m) \cong 1 \otimes X, \tag{24}$$

$$\pi_x(A\otimes 1)\pi_x(P_m) \cong \pi_{xm}(A) \otimes 1. \tag{25}$$

At the last line we have used that all $\pi_x(A\otimes\mathbf{1})$ commute with all $\pi_x(\mathbf{1}\otimes X)\cong(\mathbf{1}\otimes X)$, so must be of the form $A'\otimes\mathbf{1}$ for some $A'=\pi_{xm}(A)$. We have already indicated in the notation that the space $\mathcal{H}_{xm}(\check{a})$ arising in this construction will be chosen as Alice's laboratory Hilbert space for the coherent strategy $\check{a}$. The revert operation will simply be $R_{xm}=\pi_{xm}:\mathcal{A}_{xm}(a)\to\mathcal{B}(\mathcal{H}_{xm}(\check{a}))$ and, finally, the isometries of the pure strategy will be

$$\begin{aligned} V_{x,m}(\check{a}) &\cong \pi_x(P_m)V_x(a):\mathcal{H}_x(\check{a}) \to \pi_x(P_m)\mathcal{K}_x \\ &\cong \mathcal{H}_{xm}(\check{a}) \otimes \mathcal{K}_m^x. \end{aligned} \tag{26}$$

Then Eq. (13) holds by virtue of the Stinespring representation and we have shown that $\check{a}$ is indeed stronger than a.

To summarize: for every strategy a there is a stronger locally coherent strategy $\check{a}$. Moreover, the corresponding revert operation can be chosen to be a representation for all x. Of course, the same construction holds for Bob's nodes.

In the sequel we will assume from now on that Bob uses coherent strategies, since this does not constrain his power to resolve Alice's actions at any stage. As we will show in the proof of theorem 4, Alice's cheat consists in playing suitable purified strategies, too. By means of Eq. (15), purification on Alice's side will give Bob no clue whatsoever about her cheating attempt.

C. Bounding local Hilbert space dimensions

It is a crucial point in the definition of concealment that no limitations are imposed on Bob's capabilities. In particular, he could choose to use arbitrarily large local lab Hilbert spaces. In principle, this makes scanning all of Bob's strategies for checking ε concealment an infinite task. However, the purification construction takes care of this aspect as well, and we will show that without loss of discrimination power Bob can fix the dimension of his laboratory spaces uniformly over all his strategies.

The Stinespring construction respects finite dimensionality. Usually one takes a "minimal" dilation, which means that the vectors $\pi(A)V\phi$ with $A\in\mathcal{A}$ and $\phi\in\mathcal{H}$ are dense in $\mathcal{K}$. Hence $\dim\mathcal{K}\leqslant\dim\mathcal{A}\,\dim\mathcal{H}$. However, since this bound still contains the algebra $\mathcal{A}$, which is part of the strategy whose purification generates the locally coherent protocol, and which is not *a priori* bounded, this argument does not suffice to derive a uniform dimension bound on local laboratory spaces.

The desired bound can be constructed by looking directly at the definition of locally coherent strategies. Here the growth of Bob's lab space is given by the two operations

$$V_{x,m}(b):\mathcal{H}_x(b) \to \mathcal{K}_m^x \otimes \mathcal{H}_{xm}(b) \tag{27}$$

at Bob's nodes and

$$\mathcal{H}_{xm}(b) = \mathcal{K}_m^x \otimes \mathcal{H}_x(b) \tag{28}$$

at Alice's nodes. Given the dimensions of $\mathcal{H}_x(b)$ and $\mathcal{K}_m^x$, the first line *per se* does not imply a bound on the dimension of $\mathcal{H}_{xm}(b)$. However, the range of $V_{x,m}$ has known finite dimension, so most of these dimensions will never be used. More precisely, we can find a subspace $\mathcal{H}'_{xm}(b)\subset\mathcal{H}_{xm}(b)$ such that

$$V_{x,m}(b)(\mathcal{H}_x(b)) \subset \mathcal{K}_m^x \otimes \mathcal{H}'_{xm}(b). \tag{29}$$

Indeed, we can take $\mathcal{H}'_{xm}(b)$ as the span of all vectors $\phi_{\alpha,j}$ appearing in the expansion $V_{x,m}(b)\phi_\alpha=\Sigma_j\psi_j\otimes\phi_{\alpha,j}$, where $\{\psi_j\}\subset\mathcal{K}_m^x$ and $\{\phi_\alpha\}\subset\mathcal{H}_x(b)$ are orthonormal bases. Hence

$$\dim\mathcal{H}'_{xm}(b) \leqslant \dim\mathcal{H}_x(b)\dim\mathcal{K}_m^x. \tag{30}$$

We can now apply this idea inductively—i.e., with a previously constructed $\mathcal{H}'_x(b)\subset\mathcal{H}_x(b)$ on the left-hand side of Eq. (29). Note that at Alice's nodes there is nothing to choose and the dimension bound Eq. (30) holds with equality anyhow. At the root we have $\dim\mathcal{H}_0(b)=\dim\mathcal{H}'_0(b)=:d_0^B\in\mathbb{N}$ for all strategies, the dimension of Bob's initial state space.

Hence we have a new strategy, using the same isometries $V_{x,m}(b)$ as b, but with domains and ranges restricted to a subspace $\mathcal{H}_x(b')\equiv\mathcal{H}'_x(b)\subset\mathcal{H}_x(b)$ for all b. We show now that b' is stronger than b. The required revert operation is implemented by the subspace embedding $j_x:\mathcal{H}_x(b')\to\mathcal{H}_x(b)$, as $R_x(B)=j_x^*Bj_x$ and, due to Eq. (29), the operators $V_{x,m}$ for the new strategies are connected by

$$V_{xm}(b)j_x = (\mathbf{1}\otimes j_{xm})V_{xm}(b'):\mathcal{H}_x(b') \to \mathcal{K}_m^x \otimes \mathcal{H}_{xm}(b), \tag{31}$$

where j_{xm} is the embedding of $\mathcal{H}'_{xm}(b)$ into $\mathcal{H}_{xm}(b)$. Equation (13) then follows by combining this with Eq. (17) in a version adapted to Bob's pure strategies. An intuitive description of this revert operation in the Schrödinger picture is to ask Bob to consider his density operator on $\mathcal{H}_x(b')$ as a density operator on the larger space $\mathcal{H}_x(b)$ by setting it equal to zero on the orthogonal complement.

It is perhaps paradoxical that in this case the strategy using less resources is stronger. But in fact, they are just equally strong. The revert operation in the opposite direction is $S_x:\mathcal{B}(\mathcal{H}_x(b'))\to\mathcal{B}(\mathcal{H}_x(b))$, with

$$S_x(B)=j_xBj_x^*+\rho_x(B)(\mathbf{1}-j_xj_x^*), \tag{32}$$

where ρ_x is an arbitrary state on $\mathcal{B}(\mathcal{H}_x(b'))$. The second term is added to satisfy the channel normalization $S_x(\mathbf{1})=\mathbf{1}$. Since $j_x^*j_x=\mathbf{1}$, we have $R_xS_x=\mathrm{id}$. The revert operation in this case is thus the projection on the subspace $\mathcal{H}_x(b')\subset\mathcal{H}_x(b)$.

Taking together the reduction operation and, possibly, an expansion as described (adding some extra dimensions on which all states vanish), we can convert any strategy b to another one, for which the dimension bound Eq. (30) holds with equality, at both Bob's and Alice's nodes. But then we can identify all the spaces $\mathcal{H}_x(b')$ with a fixed space of appropriate dimension, say $\mathcal{H}_x^B$.

Applying the same construction to Alice's operations, we find a strategy-independent Hilbert space $\mathcal{H}_x^A$. In particular, we will henceforth assume $\mathcal{H}_x(\breve{a}_0)=\mathcal{H}_x(\breve{a}_1)=\mathcal{H}_x^A$ at all nodes x for Alice's locally coherent strategies $\breve{a}_i$. This will simplify the discussion of Alice's cheating strategy in Secs. III E and III G below.

We summarize this section in the following proposition, which we formulate for Bob's strategies. It holds equally for Alice's strategies, too.

Proposition 2. (dimension bound). Let $\mathcal{H}_x^B$ denote a family of Hilbert spaces with dimensions satisfying

$$\dim\mathcal{H}_{xm}^B=\dim\mathcal{H}_x^B\dim\mathcal{K}_m^x \tag{33}$$

and

$$\dim\mathcal{H}_0^B=d_0^B\in\mathbb{N} \tag{34}$$

for all nodes x. Then for every locally coherent strategy b of Bob there is an equally strong locally coherent strategy b' with $\mathcal{H}_x(b')=\mathcal{H}_x^B$ for all x. ■

The entire strategy dependence is now contained in the choice of the operators $V_{x,m}(b')$.

Corollary 3. In the definitions of ε-concealing and δ-cheating strategy, we may restrict the quantifier over all of Bob's strategies to locally coherent strategies with a strategy-independent laboratory Hilbert space $\mathcal{H}_x^B$.

For every $\xi>0$ there is a finite set S of such strategies approximating all of Bob's discriminating procedures to within ξ. That is, for any strategy b of Bob we can find $b'\in S$ such that for all of Alice's strategies a

$$\|\rho_c(a,b)-\rho_c(a,b')\|_1\leq\xi. \tag{35}$$

■

The proof of corollary 3 is obvious from the dimension bound, and the observation that the set of bounded operators between Hilbert spaces of fixed finite dimension is compact in the norm topology.

D. Bob's strategy register

The next simplification we would like to introduce will significantly reduce the complexity of the many-round scenario. The basic idea is to replace all of Bob's choices by a single choice he makes at the beginning by preparing a suitable initial state. His later choices will then be taken over by a sequence of "quantum controlled operations." This reorganization of Bob's choices requires the expansion of the lab space by an additional register, to hold the control information. It is perhaps worthwhile to emphasize that this strategy register serves merely as a technical tool in the no-go proof.

We will choose a finite approximation S to Bob's strategy space in the sense of corollary 3, with a very small value of ξ, which will be taken to zero at the end. The strategy register will be described by the Hilbert space $\ell^2(S)$, the complex-valued functions on S, with the usual scalar product. In other words, we have one basis vector $|b\rangle$ for each strategy $b\in S$. Then we set

$$\widetilde{\mathcal{H}}_x^B=\mathcal{H}_x^B\otimes\ell^2(S), \tag{36}$$

$$\widetilde{V}_{x,m}:\widetilde{\mathcal{H}}_x^B\to\widetilde{\mathcal{H}}_{xm}^B\otimes\mathcal{K}_m^x, \tag{37}$$

$$\widetilde{V}_{x,m}=\sum_{b\in S}V_{x,m}(b)\otimes|b\rangle\langle b|. \tag{38}$$

Observe that $\widetilde{V}_{x,m}$ is now independent of Bob's strategy (it depends on S). However, Bob still has a choice to make: namely, the choice of the initial state for the strategy register. If he wants to play strategy b, he will set it to $|b\rangle\langle b|$ and then let the preprogrammed controls take over.

The construction also opens up the rather interesting possibility for Bob to play strategies in superposition simply by initially preparing a superposition of the basis states $|b\rangle$. For this case it is helpful to bear in mind that the "control" by "controlled unitary operations" is not a one way affair. As soon as Bob prepares superpositions, the strategy register is in general affected by the interaction, so by "measuring the strategy" after a while, Bob could pick up some clues about Alice's actions. This is required by basic laws of quantum mechanics, because the controlled-unitary operation creates entanglement.

Let us consider the overall effect of the protocol up to commitment, with the trusted shared initial state ρ_0 considered fixed, Bob choosing an arbitrary initial state $\sigma\in\mathcal{B}_*(\ell^2(S))$ (possibly mixed) for the strategy register, and Alice playing strategy a. At commitment, the observable algebra is now $\oplus_{x\in X_c}\mathcal{A}_x(a)\otimes\mathcal{B}(\widetilde{\mathcal{H}}_x^B)$. The state obtained on this algebra depends linearly on the initial state σ, and being implemented by a series of completely positive transformations, this dependence is given by a quantum channel $\Gamma(a)$. In the Heisenberg picture we thus have

$$\Gamma(a):\bigoplus_{x\in X_c}\mathcal{A}_x(a)\otimes\mathcal{B}(\widetilde{\mathcal{H}}_x^B)\to\mathcal{B}(\ell^2(S)). \tag{39}$$

The restriction of the final state to Bob's side is what decides his chances of distinguishing different strategies of Alice. These restrictions are given by the reduced channel $\Gamma^B(a):\oplus_{x\in X_c}\mathcal{B}(\widetilde{\mathcal{H}}_x^B)\to\mathcal{B}(\ell^2(S))$, given by

$$\Gamma^B(a)(\bigoplus_{x\in X_c} B_x) = \Gamma(a)(\bigoplus_{x\in X_c} 1_{\mathcal{A}_x(a)} \otimes B_x). \quad (40)$$

The concealment condition requires that $\Gamma^B(a_0) \approx \Gamma^B(a_1)$. The aim of the impossibility proof is to conclude from this the existence of a good cheating strategy for Alice. For this conclusion it turns out to be crucial how the approximate equality of these channels is expressed quantitatively. We defer this discussion to Sec. III F and treat first the case $\Gamma^B(a_0)=\Gamma^B(a_1)$, which requires only the Stinespring dilation theorem and shows more clearly what properties we need to establish in the approximate case.

E. Case of perfect concealment

In the sequel Bob is always understood to take advantage of his strategy register and preprogrammed controls, as described in Sec. III D. So we will henceforth drop the tilde on Bob's Hilbert spaces $\tilde{\mathcal{H}}_x^B$ to streamline the presentation.

For the case of perfect concealment, suppose that $\Gamma^B(a_0) = \Gamma^B(a_1)$ and that Alice is preparing to cheat. She will then play the local purification $\check{a}_i$ $(i=0,1)$ of one of the honest strategies until commitment time. Note that both Alice's and Bob's strategies are assumed to be locally coherent in the sense of Sec. III B, with Hilbert space dimensions independent of their respective strategies as explained in Sec. III C. The concatenated channel $\Gamma(\check{a}_i): \oplus_x \mathcal{B}(\mathcal{H}_x^A) \otimes \mathcal{B}(\mathcal{H}_x^B) \to \mathcal{B}(\ell^2(S))$ is then likewise pure and is hence given by operators $V_{i,x}: \ell^2(S) \to \mathcal{H}_x^A \otimes \mathcal{H}_x^B$ as

$$\Gamma(\check{a}_i)(\bigoplus_{x\in X_c} (A_x \otimes B_x)) = \sum_{x\in X_c} V_{i,x}^*(A_x \otimes B_x)V_{i,x} = V_i^*(\bigoplus_{x\in X_c} (A_x \otimes B_x))V_i. \quad (41)$$

For the last step we have combined all the $V_{i,x}$ into a single operator $V_i: \ell^2(S) \to \mathcal{K} := \oplus_x \mathcal{H}_x^A \otimes \mathcal{H}_x^B$, and the direct sum refers to the direct sum decomposition of the underlying Hilbert space $\mathcal{K}$. Note that this Hilbert space carries a representation π of Bob's observable algebra $\oplus_x \mathcal{B}(\mathcal{H}_x^B)$ at commitment time simply by setting $\pi(\oplus_x B_x) = \oplus_x \mathbf{1}_x^A \otimes B_x$. Hence $(\mathcal{K}, \pi, V_i)$ is a dilation of the channel $\Gamma^B(\check{a}_i)$ in the sense of proposition 1.

But now, by assumption, $\Gamma^B(\check{a}_0) = \Gamma^B(a_0) = \Gamma^B(a_1) = \Gamma^B(\check{a}_1)$. Hence we get two dilations of the same channel, which must be connected by a unitary operator $U \in \mathcal{B}(\mathcal{K})$ as in proposition 1. Essentially, this U will be Alice's cheat operation. What we have to show is that she can execute this operation on the system under her control, given the classical information x.

The condition $U\pi(Y) = \pi(Y)U$, applied to a projection $Y = P_x$ of one of the summands, implies that U can be broken into blocks, $U\pi(P_x) = \pi(P_x)U \in \mathcal{B}(\mathcal{H}_x^A \otimes \mathcal{H}_x^B)$. The intertwining relation for $\pi(B_x)$ allows us to conclude that this operator is of the form $U_x \otimes \mathbf{1}_x^B$, with a unitary operator $U_x \in \mathcal{B}(\mathcal{H}_x^A)$. Clearly, U_x is an operator between possible lab spaces of Alice, depending only on publicly available information $x \in X_c$. This will be Alice's cheat channel. Setting

$$C_x: \mathcal{B}(\mathcal{H}_x(\check{a}_1)) \to \mathcal{B}(\mathcal{H}_x(\check{a}_0)), \quad C_x(A) = U_x^* A U_x, \quad (42)$$

we immediately conclude from $UV_0 = V_1$ that

$$\Gamma(\check{a}_0)(\bigoplus_x C_x \otimes \mathrm{id}_x^B) = \Gamma(\check{a}_1). \quad (43)$$

Let us summarize Alice's perfect cheat. She will play the purification $\check{a}_0$ of the honest strategy a_0 until commitment time. If at that time she decides to go for the bit value 0, she will just apply the revert operation from the purification construction. After that nobody can tell the difference between her actions and the honest a_0, not even with full access to both labs. On the other hand, if she wants to choose bit value 1, she will apply the cheat channel C_x. We see from Eq. (43) that afterwards nobody will be able to tell the difference between her actions and $\check{a}_1$. Finally, she will apply the revert operation from $\check{a}_1$ to a_1, hiding all her tracks. Note that the revert operation by construction works at any step: indeed Alice can cheat at any time, since the protocol must be concealing for all steps in order to be concealing at the commitment stage.

F. Bob's entangled strategy record

In the previous section we have seen how Stinespring's theorem allows Alice to find a perfect cheat in a perfectly concealing bit commitment protocol. The continuity theorem presented in Sec. III G below shows that the same cheating strategy still works for Alice with high probability under more realistic conditions—when only approximate concealment is guaranteed, $\Gamma^B(a_0) \approx \Gamma^B(a_1)$. The result crucially depends on the way in which the distance between these two channels is evaluated: Bob can test the condition $\Gamma^B(a_0) \approx \Gamma^B(a_1)$ by preparing a state σ for the strategy register $\ell^2(S)$ and making a measurement on the system $\mathcal{H}_x^B$ he receives back from Alice. This includes both the possibility to superpose his original strategies $|b\rangle$ and the possibility to mix such strategies in the sense of game theory. However, this still does not exhaust his options: he can *keep an entangled record of his strategy*. This would be pointless for just classical mixtures of his basic strategies $|b\rangle$. In that case all his density operators would commute with the "strategy observable" and he could extract the initial strategy by a von Neumann measurement from the state at any later step. However, if he also uses superpositions of strategies, the controlled unitaries may properly "change" the strategy. It therefore makes sense to keep a record—i.e., to not only use a mixed initial state, which would correspond to a mixed strategy in the sense of von Neumann's game theory, but to use an entangled pure state on $\ell^2(S) \otimes \ell^2(S')$, with some reference system S'. It turns out that one can always choose $S' \cong S$ (cf. proposition 8.11 in Paulsen's text [57]). While the first copy in this tensor product is used as before to drive the conditional strategy operators V_x, the second is the record and is completely left out of the dynamics. In other words, Bob not only uses a von Neumann mixed strategy, but the purification of this mixture. Concealment will then have to be guaranteed against his joint measurements on $\mathcal{H}_B^x \otimes \ell^2(S')$.

We will see in Sec. V B that this procedure in general does increase Bob's resolution for the difference of channels.

Of course, if the initial selection of strategies S is large enough, an approximation of this quantum randomized strategy will already be contained in S and the gain may be negligible. Mathematically, the introduction of randomized strategies corresponds to using a different norm: to guarantee concealment in the sense of definition 1, Alice will have to make sure that $\|[\Gamma^B(a_0)-\Gamma^B(a_1)]\otimes \mathrm{id}_\nu\| \leq \varepsilon$ if ν-dimensional bystander systems are taken into account, for all $\nu \in \mathbb{N}$. As explained in the Appendix, this just means that these two channels need to be indistinguishable in the cb norm, $\|\Gamma^B(a_0)-\Gamma^B(a_1)\|_{\mathrm{cb}} \leq \varepsilon$ for some small $\varepsilon > 0$.

G. Full impossibility proof

The full impossibility proof goes beyond the case of perfect concealment discussed in Sec. III E. It shows that Alice can still cheat if the bit commitment protocol is only approximately concealing and provides explicit dimension-independent bounds on Alice's probability to pass Bob's tests undetected:

Theorem 4 (no-go theorem). Any ε-concealing bit commitment protocol in the sense of Sec. II B allows Alice to find a $2\sqrt{\varepsilon}$-cheating strategy. ■

These bounds coincide with those obtained by Spekkens and Rudolph [23] in the Kerckoffian framework. Our proof shows that they still hold if Bob no longer sticks to a publicly known strategy. This is a significant improvement over Cheung's dimension-dependent estimates [51], which do not suffice to rule out bit commitment protocols with large systems.

The full no-go proof is based on a continuity result for Stinespring's dilation theorem, which we cite here from [46]. It states that two quantum channels Γ_0^B and Γ_1^B are close in cb-norm iff there exist corresponding Stinespring isometries V_0 and V_1 which are close in operator norm. This generalizes the uniqueness clause in Stinespring's theorem to cases in which two quantum channels differ by a finite amount and hence is precisely the type of result we need to rule out approximately concealing bit commitment protocols.

Proposition 5 (continuity theorem). Let $\mathcal{H}$ and $\mathcal{H}^B$ be finite-dimensional Hilbert spaces, and suppose that

$$\Gamma_0^B, \Gamma_1^B : \mathcal{B}(\mathcal{H}^B) \to \mathcal{B}(\mathcal{H}) \tag{44}$$

are quantum channels with Stinespring isometries $V_0, V_1 : \mathcal{H} \to \mathcal{H}^A \otimes \mathcal{H}^B$ and a common dilation space $\mathcal{H}^A$ such that $\dim \mathcal{H}^A \geq 2 \dim \mathcal{H} \dim \mathcal{H}^B$. We then have

$$\begin{aligned} \inf_U \|(U \otimes 1_B)V_0 - V_1\|^2 &\leq \|\Gamma_0^B - \Gamma_1^B\|_{\mathrm{cb}} \\ &\leq 2 \inf_U \|(U \otimes 1_B)V_0 - V_1\|, \end{aligned} \tag{45}$$

where the minimization is over all unitary $U \in \mathcal{B}(\mathcal{H}^A)$. ■

We refer to [46] for a proof of proposition 5 and further applications of the continuity theorem. In this form the result applies to quantum channels whose common domain is a full matrix algebra, while in our case the domain algebra of the commitment channels $\Gamma_i^B \equiv \Gamma^B(\breve{a}_i)$ is the direct sum $\oplus_x \mathcal{B}(\mathcal{H}_x^B)$. Again we have dropped the tilde from Bob's Hilbert spaces in an attempt to streamline the presentation. In order to apply the continuity theorem to our setting, we extend the channels $\Gamma_i \equiv \Gamma(\breve{a}_i) : \oplus_x \mathcal{B}(\mathcal{H}_x^A) \otimes \mathcal{B}(\mathcal{H}_x^B) \to \mathcal{B}(\mathcal{H})$ to channels $\hat{\Gamma}_0, \hat{\Gamma}_1 : \mathcal{B}(\mathcal{H}^A \otimes \mathcal{H}^B) \to \mathcal{B}(\mathcal{K})$, where we have introduced the shortcuts $\mathcal{H} := \ell^2(S)$, $\mathcal{H}^A := \oplus_x \mathcal{H}_x^A$ and $\mathcal{H}^B := \oplus_x \mathcal{H}_x^B$. Note that the tensor product $\mathcal{H}^A \otimes \mathcal{H}^B$ has the direct sum decomposition $\oplus_{xy} \mathcal{H}_x^A \otimes \mathcal{H}_y^B$, and that $\oplus_x \mathcal{B}(\mathcal{H}_x^A \otimes \mathcal{H}_x^B)$ is the subalgebra in $\mathcal{B}(\mathcal{H}^A \otimes \mathcal{H}^B)$ which consists of those operators that are supported on the diagonal subspace $\oplus_x \mathcal{H}_x^A \otimes \mathcal{H}_x^B$. For direct sum channels $\Gamma_i(\oplus_x A_x \otimes B_x) = \Sigma_x V_{i,x}^*(A_x \otimes B_x)V_{i,x}$ as in Eq. (41), the extensions $\hat{\Gamma}_i = \hat{V}_i^*(\cdot)\hat{V}_i$ have Stinespring isometries $\hat{V}_0, \hat{V}_1 : \mathcal{H} \to \mathcal{H}^A \otimes \mathcal{H}^B = \oplus_{xy} \mathcal{H}_x^A \otimes \mathcal{H}_y^B$ given by

$$\hat{V}_i \psi := \bigoplus_{xy} \delta_{xy} V_{i,x} \psi. \tag{46}$$

In the sequel we assume that the dilation spaces are chosen sufficiently large such that the dimension bound in proposition 5 is met. The restrictions of $\hat{\Gamma}_i$ to Bob's output system $\mathcal{H}^B$ will be denoted by $\hat{\Gamma}_i^B$. We then have $\hat{\Gamma}_i^B = \Gamma_i^B \circ P$, where the cp map

$$P : \mathcal{B}(\mathcal{H}^B) \to \oplus_x \mathcal{B}(\mathcal{H}_x^B), \quad P(B) = \oplus_x P_x B P_x \tag{47}$$

is composed of the projections P_x in $\mathcal{H}^B$ onto $\mathcal{H}_x^B$. Since

$$\|\hat{\Gamma}_0^B - \hat{\Gamma}_1^B\|_{\mathrm{cb}} = \|(\Gamma_0^B - \Gamma_1^B) \circ P\|_{\mathrm{cb}} \leq \|\Gamma_0^B - \Gamma_1^B\|_{\mathrm{cb}}, \tag{48}$$

we may now apply the left half of the continuity estimate Eq. (45) to the extended quantum channels $\hat{\Gamma}_i^B$ to conclude that

$$\inf_U \|(U \otimes 1_B)\hat{V}_0 - \hat{V}_1\|^2 \leq \|\hat{\Gamma}_0^B - \hat{\Gamma}_1^B\|_{\mathrm{cb}} \leq \|\hat{\Gamma}_0 - \hat{\Gamma}_1\|_{\mathrm{cb}}. \tag{49}$$

The minimization at this point is with respect to all unitary $U \in \mathcal{B}(\mathcal{H}^A)$, which can be written in the block decomposition

$$U\psi = \bigoplus_x \sum_y U_{xy}\psi_y, \tag{50}$$

with operators $U_{xy} : \mathcal{H}_y^A \to \mathcal{H}_x^A$. It turns out that the minimization in Eq. (49) can always be restricted to unitary operators whose off-diagonal blocks vanish. To see this, note that the left-hand side of Eq. (49) can be rewritten as

$$\begin{aligned} \inf_U \|(U \otimes \mathbf{1}_B)\hat{V}_0 - \hat{V}_1\|^2 &= \inf_U \sup_\varrho \mathrm{tr}\varrho(\hat{V}_0^*(U^* \otimes \mathbf{1}_B) - \hat{V}_1^*) \\ &\quad \times [(U \otimes \mathbf{1}_B)\hat{V}_0 - \hat{V}_1] \\ &= \inf_U \sup_\varrho (2 - 2\mathrm{Re}\ \mathrm{tr}\varrho \hat{V}_1^*(U \otimes 1_B)\hat{V}_0), \end{aligned} \tag{51}$$

where the supremum is taken over all states $\varrho \in \mathcal{B}_*(\mathcal{H})$. From the definition of the isometries $\hat{V}_i$ in Eq. (46) above it is straightforward to verify that

$$\hat{V}_1^*(U \otimes \mathbf{1}_B)\hat{V}_0 = \sum_x V_{1,x}^*(U_{xx} \otimes \mathbf{1}_x)V_{0,x} \tag{52}$$

in Eq. (51). Therefore, the minimization procedure on the left-hand side of Eq. (49) is not affected by the off-diagonal

blocks $\{U_{xy}, x \neq y\}$, which implies that the infimum is attained at a unitary operator that is a direct sum of unitaries, $U = \oplus_x U_x \in \oplus_x \mathcal{B}(\mathcal{H}_x^A)$. On the other hand, the cb-norm difference $\|\Gamma_0^B - \Gamma_1^B\|_{\mathrm{cb}}$ is easily seen to be upper bounded by $2\|(U \otimes 1_B)V_0 - V_1\|$ for any unitary operator $U = \oplus_x U_x$.

In summary, we have shown that the continuity theorem extends to direct sum channels with a unitary U that respects the direct-sum decomposition.

Proposition 6. (continuity theorem for direct sum channels). Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and let $\{\mathcal{H}_x^B\}_{x \in X}$ and $\{\mathcal{H}_x^A\}_{x \in X}$ be collections of finite-dimensional Hilbert spaces. Suppose that $V_0, V_1 : \mathcal{H} \to \oplus_x \mathcal{H}_x^A \otimes \mathcal{H}_x^B$ are Stinespring isometries for the quantum channels $\Gamma_1, \Gamma_2 : \oplus_x \mathcal{B}(\mathcal{H}_x^A \otimes \mathcal{H}_x^B) \to \mathcal{B}(\mathcal{H})$ such that

$$\Gamma_i\Big(\bigoplus_x (A_x \otimes B_x)\Big) = \sum_x V_{i,x}^*(A_x \otimes B_x)V_{i,x} = V_i^*\Big(\bigoplus_x (A_x \otimes B_x)\Big)V_i \tag{53}$$

and $\dim \mathcal{H}_x^A \geq 2 \dim \mathcal{H}_x^B \dim \mathcal{H}$ for all $x \in X$. Let $\Gamma_i^B : \oplus_x \mathcal{B}(\mathcal{H}_x^B) \to \mathcal{B}(\mathcal{H})$ be the local restrictions given by $\Gamma_i^B(\oplus_x B_x) := V_i^*(\oplus_x 1_x^A \otimes B_x)V_i$. We then have

$$\inf_U \|(U \otimes 1_B)V_0 - V_1\|^2 \leq \|\Gamma_0^B - \Gamma_1^B\|_{\mathrm{cb}} \leq 2 \inf_U \|(U \otimes 1_B)V_0 - V_1\|, \tag{54}$$

where the minimization is over all unitary operators $U = \oplus_x U_x \in \oplus_x \mathcal{B}(\mathcal{H}_x^A)$. ■

The proof of the no-go theorem now immediately follows from proposition 6.

Proof of theorem 4. Alice will play the purification $\check{a}_0$ of the honest strategy a_0 until commitment time. If at that time she decides to go for the bit value 0, she will just apply the revert operation R from the purification construction, as described in Sec. III B. It is then no longer possible to tell the difference between her actions and the honest a_0, not even with full access to both labs. On the other hand, if she wants to choose bit value 1, she will apply the cheat channel $C_x : \mathcal{B}(\mathcal{H}_x(\check{a}_1)) \to \mathcal{B}(\mathcal{H}_x(\check{a}_0))$ given by $C_x(A) := U_x^* A U_x$, where $U := \oplus_x U_x \in \oplus_x \mathcal{B}(\mathcal{H}_x^A)$ is the unitary operator that attains the infimum in Eq. (54) above. In the purification construction detailed in Sec. III B we have for simplicity assumed minimal dilation spaces. Yet in order to apply the sneak flip operation, Alice may possibly need to double her local lab space $\oplus_x \mathcal{B}(\mathcal{H}_x^A)$ to satisfy the dimension bound in proposition 6. However, this can always be postponed right until before the cheat, only requires an additional (sufficiently large) ancilla system, and hence does not constrain Alice's options.

Given an ε-concealing bit commitment protocol with local channels $\Gamma^B(a_i)$ in the sense of defition 1, we conclude from our discussion in Sec. III F that $\|\Gamma^B(a_0) - \Gamma^B(a_1)\|_{\mathrm{cb}} \leq \varepsilon$. Hence, the continuity estimate implies that

$$\|\Gamma(\check{a}_0)(\bigoplus_x C_x \otimes \mathrm{id}_x^B) - \Gamma(\check{a}_1)\|_{\mathrm{cb}} \leq 2\|(U \otimes 1^B)V(\check{a}_0) - V(\check{a}_1)\| \leq 2\sqrt{\|\Gamma^B(a_0) - \Gamma^B(a_1)\|_{\mathrm{cb}}} \leq 2\sqrt{\varepsilon}, \tag{55}$$

where $V(\check{a}_0)$ and $V(\check{a}_1)$ are Stinespring isometries for $\Gamma(\check{a}_0)$ and $\Gamma(\check{a}_1)$, respectively. Since the cb-norm difference cannot increase under quantum channels, the same bound holds after Alice's revert operation R,

$$\|\Gamma(\check{a}_0)(\bigoplus_x C_x \otimes \mathrm{id}_x^B)R - \Gamma(a_1)\|_{\mathrm{cb}} \leq 2\sqrt{\varepsilon}. \tag{56}$$

Alice can then confidently announce the bit value 1 in the opening. The probability of her cheat being detected is upper bounded by $2\sqrt{\varepsilon}$. This concludes the proof of the strengthened no-go theorem. ■

IV. QBC IN INFINITE DIMENSIONS

In this section we will relax the general finiteness condition imposed in Secs. II and III and show how to extend the no-go proof to quantum bit commitment protocols in which the dimension of the underlying Hilbert spaces (Sec. IV A), the number of rounds (Sec. IV B), or the set of classical signals (Sec. IV C) are infinite.

A. Continuous-variable systems

We have so far restricted the discussion of the no-go theorem to systems that can be described in finite-dimensional (albeit arbitrarily large) Hilbert spaces. In this section we show that the results can be easily extended to continuous variable systems—as long as the systems obey a global energy constraint of a reasonably generic form. The total available energy for the protocol needs to be finite but can otherwise be as high as desired, and yet secure quantum bit commitment remains impossible. Purists might dismiss this additional energy constraint on the basis that it restricts the domain for the impossibility proof. Yet most physicists know that infinite energy is seldom available. In fact, the continuity theorem for Stinespring's dilation may be generalized to completely positive maps between arbitrary C^* algebras [53], and hence the no-go theorem applies to continuous-variable systems with unbounded energy, too. But these results are somewhat beyond the scope of the present paper, so we assume a uniform energy constraint to simplify the presentation.

To set the stage, assume that $\mathcal{H}$ is a separable (but no longer necessarily finite-dimensional) Hilbert space. As before, let $\mathcal{B}_*(\mathcal{H})$ denote the Banach space of trace-class operators on $\mathcal{H}$ and $\mathcal{S}(\mathcal{H}) \subset \mathcal{B}_*(\mathcal{H})$ the closed convex set of states. We further assume that $H : \mathcal{D} \to \mathcal{H}$ is an unbounded self-adjoint (energy) operator defined on a dense set $\mathcal{D} \subset \mathcal{H}$. [From the Hellinger-Toeplitz theorem (cf. Sec. III D in [54]) we know that a symmetric unbounded operator cannot be defined on all of $\mathcal{H}$, so we always assume a dense subset $\mathcal{D}$.] For the proof we assume that H has discrete spectrum, that all of its eigenvalues h_n have finite multiplicity, and that $\lim_{n \to \infty} h_n = \infty$. Under these conditions, the set of states

$$\mathcal{S}_E(\mathcal{H}) := \{\varrho \in \mathcal{S}(\mathcal{H}) | \mathrm{tr}\varrho H \leqslant E\} \tag{57}$$

can be shown to be compact for every $E \geqslant 0$ [55]. As we assume this energy constraint to be global, we impose that it is respected by the quantum operation T_*, which describes the full bit commitment protocol: $T_*(\varrho) \in \mathcal{S}_E(\mathcal{H})$ for all $\varrho \in \mathcal{S}_E(\mathcal{H})$.

Since the continuity theorem applies in this setting [46], the proof presented in Sec. III goes through unchanged. There is also a simpler proof, which avoids the compactness arguments and is based on a useful approximation result: any infinite-dimensional system with energy constraints as in Eq. (57) can be approximated to arbitrary degree of accuracy by a sufficiently large finite-dimensional system. This allows us to reduce any bit commitment protocol to its finite-dimensional counterpart:

Proposition 7. Given an ε-concealing and δ-binding quantum bit commitment protocol with a global energy constraint as in Eq. (57). Then for any $\gamma > 0$ there is a corresponding protocol on finite-dimensional Hilbert spaces with dimension $d = d(\gamma)$ which is $(\varepsilon + \gamma)$ concealing and $(\delta + \gamma)$ binding. ■

Since the latter protocol is unfeasible for sufficiently small parameters ε, δ, and γ, so is the former.

The finite-dimensional approximation needed for the proof of proposition 7 relies on the following two lemmas.

Lemma 8. Let $\gamma > 0$ and $\mathcal{S}_E(\mathcal{H})$ as in Eq. (57). Then there exists a finite-dimensional projector P_γ such that

$$\mathrm{tr}\varrho P_\gamma \geqslant 1 - \gamma \,\forall\, \varrho \in \mathcal{S}_E(\mathcal{H}) \,. \quad ■ \tag{58}$$

As a consequence, every system with energy constraints is essentially supported on a finite-dimensional Hilbert space.

Lemma 9. Let $\gamma > 0$ and P_γ as in lemma 8. Then for every quantum channel $T_* : \mathcal{B}_*(\mathcal{H}) \to \mathcal{B}_*(\mathcal{H})$ which respects the energy constraint Eq. (57) we have

$$\left\| T_*(\varrho) - \frac{1}{\mathrm{tr} P_\gamma T_*(P_\gamma \varrho P_\gamma) P_\gamma} P_\gamma T_*(P_\gamma \varrho P_\gamma) P_\gamma \right\|_1 \leqslant 4\sqrt{\gamma} + \frac{2\gamma}{1-\gamma} \tag{59}$$

for all $\varrho \in \mathcal{S}_E(\mathcal{H})$. ■

The proof of proposition 7 is then straightforward: Given the continuous-variable bit commitment protocol with energy bound E and security parameters ε and δ, we construct its finite-dimensional companion by projecting on the subspace $P_\gamma \mathcal{H}$, with the finite-dimensional projector P_γ chosen as in lemma 8. We know from the discussion in Sec. III that both the concealment and bindingness conditions can be expressed in terms of appropriately chosen quantum channels T_*. By assumption, these will respect the energy constraint. The approximation in lemma 9 then guarantees that for sufficiently small γ the companion protocol has nearly identical security parameters. Substituting $4\sqrt{\gamma} + \frac{2\gamma}{1-\gamma} \mapsto \gamma$, this concludes the proof.

It remains to prove the approximation lemmas. The proof of lemma 8 appears in [55]. We include it here for completeness.

Proof of lemma 8. Let the eigenvalues of H be arranged in increasing order: $h_1 \leqslant h_2 \leqslant h_3 \leqslant \cdots$, with eigenprojector P_n corresponding to the eigenvalue h_n. For $N \in \mathbb{N}$, we set $\hat{P}_N := \sum_{n=1}^N P_n$. We then have for all $\psi \in \mathcal{H}$

$$\begin{aligned} \langle\psi| h_{N+1}(\mathbf{1} - \hat{P}_N) |\psi\rangle &= \langle\psi| h_{N+1} \sum_{n=N+1}^{\infty} P_n |\psi\rangle \leqslant \langle\psi| \sum_{n=N+1}^{\infty} h_n P_n |\psi\rangle \\ &\leqslant \langle\psi| H |\psi\rangle, \end{aligned} \tag{60}$$

implying that $h_{N+1}(\mathbf{1} - \hat{P}_N) \leqslant H$ for all $N \in \mathbb{N}$. We may then conclude that

$$\mathrm{tr}\varrho(\mathbf{1} - \hat{P}_N) \leqslant \frac{1}{h_{N+1}} \mathrm{tr}\varrho H \leqslant \frac{E}{h_{N+1}} \tag{61}$$

for all $\varrho \in \mathcal{S}_E(\mathcal{H})$. Since the sequence $\{h_N\}_N$ diverges, the result follows by choosing $P_\gamma := \hat{P}_{N_0}$ for some sufficiently large N_0. ■

Proof of lemma 9. An application of the triangle inequality shows that

$$\begin{aligned} \|\varrho - P_\gamma \varrho P_\gamma\|_1 &\leqslant \|\varrho - P_\gamma \varrho\|_1 + \|P_\gamma \varrho - P_\gamma \varrho P_\gamma\|_1 \\ &\leqslant \|(\mathbf{1} - P_\gamma)\varrho\|_1 + \|\varrho(\mathbf{1} - P_\gamma)\|_1. \end{aligned} \tag{62}$$

For $\varrho \in \mathcal{S}_E(\mathcal{H})$ we know from lemma 8 that $\mathrm{tr}(\mathbf{1} - P_\gamma)\varrho \leqslant \gamma$, and thus the two terms on the right of Eq. (62) may be bounded as follows:

$$\begin{aligned} \|(\mathbf{1} - P_\gamma)\varrho\|_1 &= \mathrm{tr} U(\mathbf{1} - P_\gamma)\varrho \\ &\leqslant \mathrm{tr}^{1/2} \sqrt{\varrho} U U^* \sqrt{\varrho} \mathrm{tr}^{1/2} \sqrt{\varrho}(\mathbf{1} - P_\gamma)\sqrt{\varrho} \\ &\leqslant \sqrt{\gamma}, \end{aligned} \tag{63}$$

where we have used the Cauchy-Schwarz inequality for the Hilbert-Schmidt inner product and U denotes the polar isometry of $(\mathbf{1} - P_\gamma)\varrho$. Analogously, we have $\|\varrho(\mathbf{1} - P_\gamma)\|_1 \leqslant \sqrt{\gamma}$, which together with Eqs. (62) and (63) implies that

$$\|\varrho - P_\gamma \varrho P_\gamma\|_1 \leqslant 2\sqrt{\gamma}. \tag{64}$$

For all $\varrho \in \mathcal{S}_E(\mathcal{H})$, the renormalized state $\frac{1}{\mathrm{tr} P_\gamma \varrho} P_\gamma \varrho P_\gamma$ satisfies the estimate

$$\frac{1}{\mathrm{tr} P_\gamma \varrho} P_\gamma \varrho P_\gamma - P_\gamma \varrho P_\gamma \leqslant \frac{\gamma}{1-\gamma} P_\gamma \varrho P_\gamma, \tag{65}$$

which in combination with Eq. (64) implies that

$$\left\| \varrho - \frac{1}{\mathrm{tr} P_\gamma \varrho} P_\gamma \varrho P_\gamma \right\|_1 \leqslant 2\sqrt{\gamma} + \frac{\gamma}{1-\gamma}. \tag{66}$$

Since the trace norm cannot increase under quantum operations [21], the upper bound also holds for the norm difference $\|T_*(\varrho) - \frac{1}{\mathrm{tr} P_\gamma \varrho} T_*(P_\gamma \varrho P_\gamma)\|_1$. As the quantum channel T_* is supposed to respect the energy constraint, Eq. (57), an analogous chain of estimates for the output states of the channel and yet another application of the triangle inequality then yield the desired result. ■

B. Infinite number of rounds

In this section we will show how the no-go proof can be extended to cover quantum bit commitment protocols with a

possibly infinite number of rounds—as long as the expected number of total rounds remains finite. Just as with the energy constraints discussed in Sec. IV A, for any practical purpose this additional assumption does not restrict the domain of the impossibility proof.

We begin by explaining how the framework introduced in Sec. II can be modified to easily accommodate bit commitment protocols with an infinite number of rounds in each commitment, holding, and opening phase. As in the previous section, the impossibility proof will then follow from an approximation argument.

As described in detail in Sec. II B, each layer X_t of the communication tree consists of a finite number of nodes. Each node $x \in X_t$ is connected with nodes $xm \in X_{t+1}$ of the following layer, corresponding to the classical message $m \in M_x$. However, there is no longer a definite layer for which a commitment or opening has been reached. Instead, there are now infinitely many layers $X_t, t \in \mathbb{N}$. If Alice and Bob choose a definite pair of strategies, they check by means of suitable measurements how many rounds t have been performed and whether they are willing to continue. The number of rounds then naturally plays the role of a classical random variable. Introducing the bundle of algebras

$$\underline{\mathcal{F}}: t \mapsto \underline{\mathcal{F}}_t := \bigoplus_{x \in X_t} \mathcal{A}_x \otimes \mathcal{B}_x, \tag{67}$$

the total system is now described by the algebra $C(\underline{\mathcal{F}})$ of all bounded sections,

$$F: t \mapsto F(t) \in \underline{\mathcal{F}}_t, \tag{68}$$

where the norm in $C(\underline{\mathcal{F}})$ is the standard supremum norm given by $\|F\| = \sup_{t \in \mathbb{N}} \|F(t)\|$.

Alice's observable algebra, which we denote by $C(\underline{\mathcal{A}})$, is the subalgebra in $C(\underline{\mathcal{F}})$ which consists of all bounded sections A that assign to every number of rounds t an operator $A(t)$ belonging to Alice's subsystem:

$$A: t \mapsto A(t) \in \underline{\mathcal{A}}_t := \bigoplus_{x \in X_t} \mathcal{A}_x \otimes 1_{B,x}. \tag{69}$$

The observable algebra $C(\underline{\mathcal{B}})$ of Bob's system is defined completely analogously. In our setup for protocols, each strategy a that Alice chooses is related to a channel

$$\Gamma(a): C(\underline{\mathcal{F}}) \to \mathcal{B}(\ell^2(S)), \tag{70}$$

containing all her possible responses to strategies that Bob can play by a suitable preparation of his strategy register $\ell^2(S)$.

The channels $\Gamma(a)$ include naturally the necessary tests to decide for each round whether to remain in the commitment phase or to proceed with the holding or opening phase. The measurement of the number of rounds corresponds to the embedding of the Abelian C^* algebra of bounded functions on $\mathbb{N}$—denoted by $C(\mathbb{N})$—which is obviously a subalgebra of $C(\underline{\mathcal{F}})$. Let δ_t be the function in $C(\mathbb{N})$ which takes the value $\delta_t(t)=1$ and $\delta_t(s)=0$ if $s \neq t$, and let σ be some state on $\mathcal{B}(\ell^2(S))$ determining Bob's strategy. Then, by definition, the quantity

$$P(a, \sigma|t) := \mathrm{tr}[\sigma \Gamma(a)(\delta_t)] \tag{71}$$

is the probability that the commitment phase has been reached at round t, provided Alice plays a and Bob plays σ.

As advertised above, we now impose the reasonable assumption that whenever Alice plays honestly the expected number of rounds until commitment is uniformly bounded in the choice of Bob's initial state σ: denoting by a_0 and a_1 Alice's honest strategies to commit either 0 or 1, respectively, there is a finite constant $T \in \mathbb{R}$ such that

$$\sup_{\sigma} \sum_{t \in \mathbb{N}} P(a_i, \sigma|t) t \leqslant T \tag{72}$$

holds for $i=0,1$. The basic idea for the proof of the no-go result is now to relate this bound to the energy bound of the previous subsection and hence approximate a protocol with possibly infinitely many rounds by a protocol with *a priori* finitely many moves. As "Hamiltonian," the number-of-rounds operator

$$H = \sum_{t \in \mathbb{N}} \delta_t \tag{73}$$

is perfectly suited. In line with Eq. (57), it is then enough to ensure that the states $\Gamma(a_i)_*(\sigma)$ lie inside $\mathcal{S}_E(L_2(\underline{\mathcal{H}}))$ for an appropriately chosen constant E, where $L_2(\underline{\mathcal{H}})$ is the Hilbert space of square-integrable sections

$$\psi: t \mapsto \psi(t) \in \underline{\mathcal{H}}_t := \bigoplus_{x \in X_t} \mathcal{H}_x^A \otimes \mathcal{H}_x^B. \tag{74}$$

Indeed, we conclude from Eq. (72) that for each initial state σ the inequality

$$\mathrm{tr}[\Gamma(a_i)_*(\sigma) H] = \sum_{t \in \mathbb{N}} \mathrm{tr}[\sigma \Gamma(a_i)(\delta_t)] \leqslant T \tag{75}$$

is fulfilled for $i=0,1$. Hence, $\Gamma(a_i)_*(\sigma) \in \mathcal{S}_T(L_2(\underline{\mathcal{H}}))$ and we immediately obtain the following corollary as consequence of proposition 7.

Corollary 10. Suppose an ϵ-concealing and δ-binding protocol with infinitely many rounds such that the expected number of rounds until commitment is uniformly bounded for Alice playing honest as in Eq. (72). Then for any $\gamma > 0$ there is a corresponding protocol on a priori finite number of rounds $N(\gamma)$ which is $(\varepsilon + \gamma)$ concealing and $(\delta + \gamma)$ binding. ■

Thus, even protocols with an infinite number of rounds do not admit unconditional secure bit commitment.

C. Continuous-communication tree

So far we have assumed that our protocol is based on a communication tree with a discrete set of nodes and a finite number of options or messages. In this subsection we are going to relax this condition by allowing that the nodes as well as the options are taken from an *continuous set*. The set of time steps, however, is kept discrete. For simplicity, we restrict the discussion to protocols with a fixed number of rounds c until commitment. What does the structure of a continuous communication tree look like? Each layer X_t that is associated with the number of the time step t is now taken

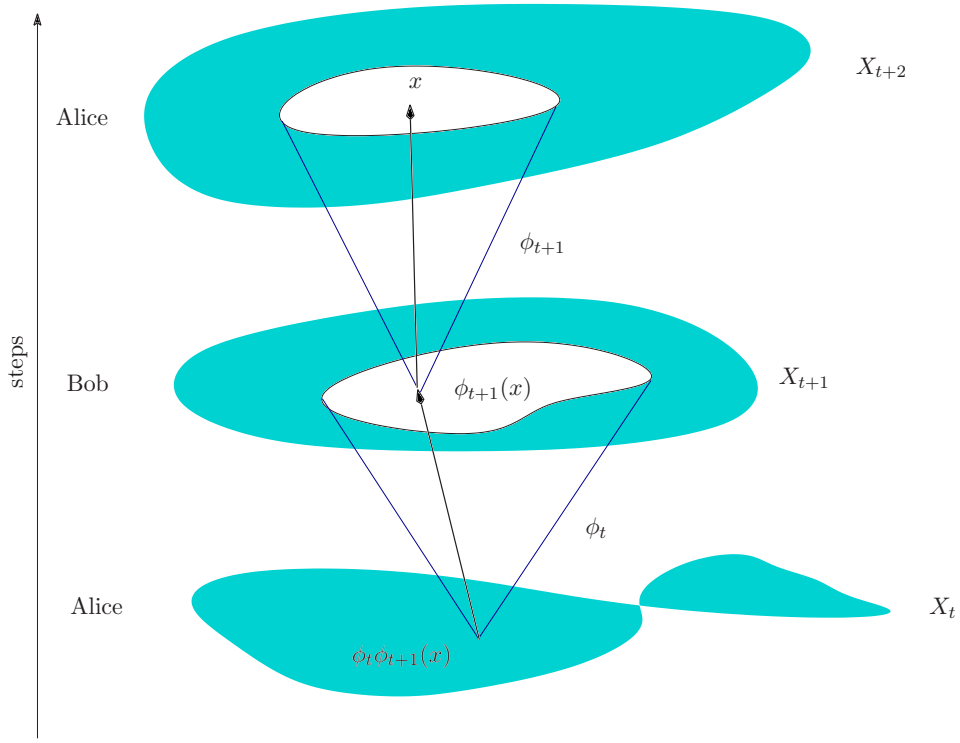

FIG. 3. (Color online) Part of a path in a continuous-communication tree. The layer X_t belongs to Alice's move. She sends the message $(\phi_{t+1}(x), \phi_t\phi_{t+1}(x))$ to Bob. The next layer is Bob's turn and consists in sending the message $(x, \phi_{t+1}(x))$ to Alice.

to be a continuous compact manifold. The continuous version of connecting each "node" of the layer X_t to some nodes of the following slice X_{t+1} is given by a continuous surjective map $\phi_t: X_{t+1} \to X_t$. The preimage $\phi_t^{-1}(x) \in X_{t+1}$ of a point $x \in X_t$ corresponds to the nodes in X_{t+1} that are connected to x. A pair $(x, \phi_t(x))$, $x \in X_{t+1}$, is regarded as a classical message that was sent from the node $\phi_t(x) \in X_t$ and was received at the node $x \in X_{t+1}$. Figure 3 shows a part of such a continuous communication tree. As with discrete communication trees, we associate to each message $(x, \phi_t(x))$ of the continuous tree a message system that is given by a full matrix algebra $\mathcal{M}(x, \phi_t(x)) = \mathcal{B}(\mathcal{K}_{(x,\phi_t(x))})$. Furthermore, to each point $x \in X_t$ we associate a finite-dimensional full matrix algebra for Alice $\mathcal{A}(x) = \mathcal{B}(\mathcal{H}_x^A)$ and likewise for Bob $\mathcal{B}(x) = \mathcal{B}(\mathcal{H}_x^B)$. These algebras are defined recursively: if $t+1$ is Alice's turn, then her algebra $\mathcal{A}(x)$ can be chosen arbitrarily. Bob's algebra is defined in terms of his previous choices of algebras and the message systems, as follows:

$$\mathcal{B}(x) := \mathcal{M}(x, \phi_t(x)) \otimes \mathcal{B}(\phi_t(x)) \tag{76}$$

for each $x \in X_{t+1}$. Since X_t is continuous, we need to replace direct sums by bounded sections within a bundle of observable algebras. Introducing the bundle of algebras

$$\underline{\mathcal{E}}_t: X_t \ni x \mapsto \mathcal{E}_t(x) := \mathcal{A}(x) \otimes \mathcal{B}(x), \tag{77}$$

the total system at time step t is described in terms of the C^* algebra $C(\underline{\mathcal{E}}_t)$ of bounded continuous sections in $\underline{\mathcal{E}}_t$. Alice's subsystem $C(\underline{\mathcal{A}}_t)$ is determined by the constraint that for each $A \in C(\underline{\mathcal{A}}_t)$ the value $A(x)$ is contained in the algebra $\mathcal{A}(x)$. In other words, A is a section in the subbundle $\underline{\mathcal{A}}_t: x \mapsto \mathcal{A}(x)$. Bob's system $C(\underline{\mathcal{B}}_t)$ is defined in the same manner.

For every strategy a played by Alice we hence obtain a corresponding channel $\Gamma(a): C(\underline{\mathcal{E}}_c) \to \mathcal{B}(\ell^2(S))$ modeling all the local operations and the entire exchange of messages up until commitment time $t=c$. As described in Sec. III D, Bob's strategies are programmed by the choice of the initial state σ on $\mathcal{B}(\ell^2(S))$. Just as before, these channels can be decomposed into a sequence of operations, each corresponding to a move made by Alice or Bob:

$$\Gamma(a) = T_{(a,1)} \circ T_{(a,2)} \circ \cdots \circ T_{(a,c)}. \tag{78}$$

We may assume that Alice and Bob play locally coherent strategies. Then all the channels

$$T_{(a,t)}: C(\underline{\mathcal{E}}_{t+1}) \to C(\underline{\mathcal{E}}_t) \tag{79}$$

in the decomposition, Eq. (78), are pure. Depending on whose turn it is, the channels $T_{(a,t)}$ need to respect Alice's and Bob's subsystems: if $t+1$ is Alice's move, then $T_{(a,t)}$ maps Alice's subsystem $C(\underline{\mathcal{A}}_{t+1})$ into Alice's subsystem of the previous step $C(\underline{\mathcal{A}}_t)$, whereas Bob's system $C(X_{t+1}, \underline{\mathcal{B}})$ remains unaffected. Consequently,

$$T_{(a,t)}(A)(x) \in \mathcal{A}(x) \tag{80}$$

and

$$T_{(a,t)}(B \circ \phi_t)(x) = B(x) \tag{81}$$

for all $x \in X_t$ and for all $B \in C(\underline{\mathcal{B}}_t)$. Note that for each section $B \in C(\underline{\mathcal{B}}_t)$ corresponding to Bob's system, the section

$$B \circ \phi_t : y \mapsto B(\phi_t(y)) \in \mathcal{B}(\phi_t(y)) \subset \mathcal{B}(y), \tag{82}$$

also belongs to Bob's system $C(\underline{\mathcal{B}}_{t+1})$ at the preceding step.

In complete analogy to the concealing condition for the discrete tree, for a protocol with a continuous communication tree to be ϵ concealing we require that

$$\|\Gamma^B(a_0) - \Gamma^B(a_1)\|_{\mathrm{cb}} \leq \epsilon, \tag{83}$$

where $\Gamma^B(a)$ is the restriction of $\Gamma(a)$ to Bob's subsystem $C(\underline{\mathcal{B}}_c)$. The range and domain algebras of the channels $\Gamma^B(a_i)$ are no longer finite-dimensional matrix algebras; nor do they admit a straightforward approximation in terms of finite-dimensional systems. Nevertheless, the concealing condition, Eq. (83), implies that Alice may find a $2\sqrt{\varepsilon}$-cheating strategy, as before. The result follows from a generalization of the continuity theorem for Stinespring's representation theorem to general C^* algebras [53].

V. PROTOCOLS RELYING ON DECOHERENCE

In this section we will demonstrate how trusted decoherence in Alice's laboratory (Sec. V A), Bob's lab (Sec. V B), or the transmission line (Sec. V C) may be employed to design secure and fair bit commitment protocols.

A. Trusted coherence shredder

A trusted third party makes perfect bit commitment a trivial task: Alice may submit the bit to an incorruptible notary public, who will store the bit in his vault throughout the holding phase and later pass it on to Bob on Alice's notice. In this scenario, the notary public will have to be paid for the long-term safe storage of the bit. Clearly, Alice and Bob would get away with much lower fees, if the notary's presence were only required once and only as a witness, without even having to store a file about the event. Such a possibility is offered by quantum mechanics.

The basic idea is that the notary is present in Alice's laboratory until the end of the commitment phase and sees to it that Alice plays honest. If the honest protocols were locally coherent, even that would be no help, since we have seen that Alice could carry out her cheating transform later, in the holding phase. However, if the honest protocols (a_0, a_1) involve some measurement or other decoherence, the notary overseeing these actions can make a difference. He could prevent a later cheat by taking some part of the system with him and destroying it. In our example below it is even sufficient for him to just watch Alice make a measurement and, if he so chooses, to forget about the result straight away. The protocol is perfectly concealing, and is as binding as desired, if a dimension parameter d is chosen large enough.

The setting requires a d-dimensional Hilbert space and two mutually unbiased orthonormal bases $\{|e_j\rangle\}_j$, $\{|f_k\rangle\}_k$, which means that $\langle e_j|e_k\rangle = \langle f_j|f_k\rangle = \delta_{jk}$ and $|\langle e_j|f_k\rangle|^2 = 1/d$ for all $j,k = 1,\ldots,d$. While the maximum number of mutually unbiased bases in a Hilbert space of given dimension d is the subject of ongoing research, here we only need two such bases, which are always easily constructed: starting from any given orthonormal basis $\{|e_j\rangle\}_j$, we may choose $\{|f_k\rangle\}_k$ as the Fourier-transformed basis,

$$|f_k\rangle := \frac{1}{\sqrt{d}} \sum_{j=1}^{d} e^{(2\pi i/d)jk} |e_j\rangle. \tag{84}$$

The protocol begins by Alice sending Bob a half of the maximally entangled state,

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_j |e_j\rangle \otimes |e_j\rangle = \frac{1}{\sqrt{d}} \sum_j |f_j\rangle \otimes |\overline{f_j}\rangle, \tag{85}$$

where $|\overline{f_j}\rangle$ denotes the complex conjugate of $|f_j\rangle$ with respect to the basis $|e_j\rangle$. Then, if she wants to commit the bit value "0," she makes a von Neumann measurement in the basis $|e_j\rangle$ and records the result. Similarly, to commit a "1," she makes a measurement in the basis $|f_j\rangle$. Thus, if she plays honest, as vouched for by the notary public, she will have no quantum system left in her laboratory, only the classical information about the bit value and her measurement result. This is the information she sends to Bob at the opening. To verify, he will make a measurement in the basis $|e_j\rangle$, if Alice claims to have submitted "0," and in the basis $|\overline{f_j}\rangle$ otherwise, finding the same result as Alice with probability 1.

The protocol is perfectly concealing, since in either case Bob gets a system in the chaotic state $\rho_B = \frac{1}{d}\mathbf{1}$. It is also binding, because whatever false bit value and measurement result Alice claims, Bob will confirm this only with probability $1/d$, i.e., practically never, if d is large.

This is essentially the bit commitment protocol originally proposed by Bennett and Brassard in 1984 [12]. Alice's EPR attack does not work in our scenario, since the notary public will not permit her to delay the measurements until after the commitment phase. There is also a variant of this protocol, in which the measurement is not actually carried out. In that case Alice prepares one of the mixed states

$$\rho_0 = \frac{1}{d} \sum_j |e_j \otimes e_j\rangle\langle e_j \otimes e_j|, \tag{86}$$

$$\rho_1 = \frac{1}{d} \sum_j |f_j \otimes \overline{f_j}\rangle\langle f_j \otimes \overline{f_j}|, \tag{87}$$

for committing "0" or "1," respectively. Now the notary watching her will see to it that she actually prepares these mixed states, and not their purifications. For verification Bob uses the support projections $P_{0,1} = d \cdot \rho_{0,1}$.

Once again, the protocol is perfectly concealing. Let us analyze Alice's cheating options, after she prepared ρ_0, with the trusted notary watching and then leaving. If she wants to change her commitment to "1," she can only employ some local channel $T \otimes \mathrm{id}$ and hope to pass Bob's test with the projection P_1. The probability for this is

$$\begin{aligned}\mathrm{tr}\rho_0(T\otimes \mathrm{id})(P_1) &= \frac{1}{d}\sum_{k,j=1}^{d}\langle e_j,e_j|(T\otimes \mathrm{id})(|f_k,\overline{f_k}\rangle\langle f_k,\overline{f_k}|)|e_j,e_j\rangle \\ &= \frac{1}{d}\sum_{k,j=1}^{d}|\langle e_j|\overline{f_k}\rangle|^2\,\langle e_j|T(|f_k\rangle\langle f_k|)|e_j\rangle \\ &= \frac{1}{d^2}\sum_{k,j=1}^{d}\langle e_j|T(|f_k\rangle\langle f_k|)|e_j\rangle \\ &= \frac{1}{d^2}\sum_{j=1}^{d}\langle e_j|T(\mathbf{1})|e_j\rangle = \frac{1}{d}. \end{aligned} \tag{88}$$

The same computation applies to $\mathrm{tr}\,\rho_1(T\otimes \mathrm{id})(P_0)$, so Alice's success probability is $1/d$ independently of her cheating channel and may hence be chosen to be arbitrarily small.

B. Decoherence monster in Bob's lab

In the proof of theorem 4 we have shown that Alice has a cheating strategy for any concealing protocol. Hence it is not surprising that by weakening Alice's position; namely, when decoherence eliminates her favorite cheating option, bit commitment protocols like those described in the previous section become possible. But it may seem rather paradoxical that decoherence acting on Bob's side, presumably further hampering the weaker partner, can also lead to successful protocols.

Suppose that every morning, the cleaning service comes to Bob's lab, unplugs all vacuum pumps, and restores what they take for tidiness. Only classical records survive this procedure. When Alice is convinced that she can rely on this, she might reassess her demands on concealment and the two might agree on a bit commitment protocol, which under such circumstances is indeed both concealing and binding. This example shows very clearly that the entangled record introduced in the proof is essential.

The protocol we suggest relies on the distinction between the local erasure of information and the destruction of quantum correlations, as seen in a pair of channels demonstrating the separation between ordinary operator norm and cb norm in an extreme way [56].

Lemma 11. Let $\varepsilon,\delta>0$. Then for sufficiently large d there is a pair of channels $R,S:\mathcal{B}(\mathbb{C}^d)\to\mathcal{B}(\mathbb{C}^d)$ such that $\|R\text{-}S\|\leqslant\varepsilon$ and $\|R\text{-}S\|_{\mathrm{cb}}\geqslant 2-\delta$. ■

Since standard operator norm and cb norm coincide for channels with classical (Abelian) output space (cf. theorem 3.9 in Paulsen's text [57]), lemma 11 demonstrates a purely quantum-mechanical effect.

Proof of lemma 11. According to Ref. [56], a quantum channel $R:\mathcal{B}(\mathbb{C}^d)\to\mathcal{B}(\mathbb{C}^d)$ is ε *randomizing* iff

$$\|R_*(\varrho)-S_*(\varrho)\|_1\leqslant\varepsilon\ \ \forall\ \ \varrho\in\mathcal{B}_*(\mathbb{C}^d), \tag{89}$$

where S denotes the completely depolarizing channel,

$$S(e)=\frac{1}{d}\mathrm{tr}e \Leftrightarrow S_*(\varrho)=\frac{\mathrm{tr}\rho}{d}\mathbf{1} \tag{90}$$

for all $e\in\mathcal{B}(\mathbb{C}^d)$ and $\varrho\in\mathcal{B}_*(\mathbb{C}^d)$, respectively. Equation (89) implies the norm estimate $\|R\text{-}S\|\leqslant\varepsilon$, as required in lemma 11.

Hayden *et al.* show that for $d>\frac{10}{\varepsilon}$, such an ϵ-randomizing quantum channel can be obtained with high probability from a random selection of at most $\mu:=\lceil\frac{134}{\varepsilon^2}d\log d\rceil$ unitary operators $\{U_i\}_{i=1}^{\mu}\subset\mathcal{B}(\mathbb{C}^d)$,

$$R(e):=\frac{1}{\mu}\sum_{i=1}^{\mu}U_i^*eU_i. \tag{91}$$

In striking contrast, exact randomization of quantum states [such that $\varepsilon=0$ in Eq. (89)] is known to require an ancilla system of dimension $d^2\geqslant\mu$ [58]. However, this significant reduction in the size of the ancilla space comes at a price: while the randomizing map R erases local information, it preserves almost all the correlations with a bystander system if d is sufficiently large. In fact, it is straightforward to show the upper bound

$$\|(R_*-S_*)\otimes \mathrm{id}|\Omega\rangle\langle\Omega|\|_1\geqslant 2-\frac{2\mu}{d^2}, \tag{92}$$

where $|\Omega\rangle:=\frac{1}{\sqrt{d}}\Sigma_{i=1}^{d}|i,i\rangle$ again denotes the maximally entangled state on $\mathbb{C}^d\otimes\mathbb{C}^d$. Equation (92) implies the bound $\|R\text{-}S\|_{\mathrm{cb}}\geqslant 2-\delta$, where $\delta:=\frac{2\mu}{d^2}$ can be made as small as desired by choosing d sufficiently large. ■

We can now set up a bit commitment protocol in which Bob initially supplies a pure state $|\psi\rangle$ on a d-dimensional Hilbert space $\mathcal{H}_B$ according to the unitarily invariant Haar measure. There is only one round for Alice, requiring her to send back a system with the same Hilbert space. Her honest strategies are specified by a pair of channels $T_k:\mathcal{B}(\mathcal{H}_A^k\otimes\mathcal{H}_B)\to\mathcal{B}(\mathcal{H}_B)$ $(k=0,1)$. We take them to be locally coherent—i.e., implemented by a single isometry $V_k:\mathcal{H}_B\to\mathcal{H}_A^k\otimes\mathcal{H}_B$ each. Their restrictions to Bob's side will be channels as provided by lemma 11: $T_0^B(X)=V_0^*(1\otimes X)V_0=R(X)$ and, similarly, $T_1^B=S$.

To reveal her commitment, Alice will later supply Bob with the ancilla system $\mathcal{H}_A^k$, alongside with the bit value k. Bob will then verify Alice's claim with a projective measurement on $V_k|\psi\rangle$, as illustrated in Fig. 4. Clearly, this protocol is perfectly *sound*, since Bob's measurement will confirm the bit value k with unit probability if both parties have followed their honest strategies. The protocol is $\frac{\varepsilon}{2}$ concealing, provided the decoherence monster strikes as planned, implementing some entanglement-breaking channel [59] on Bob's reference system. By definition, these are the channels $D:\mathcal{B}(\mathcal{H}_B)\to\mathcal{B}(\mathcal{H}_B)$ such that $D\otimes \mathrm{id}(\varrho)$ is separable for any input state ϱ. Hence, these channels are sometimes also called *separable*. In Fig. 4, the decoherence inflicted by D is indicated by the rubbish bin. We will show below that the maximal probability difference Bob can detect by preparing suitable states and making suitable measurements is then indeed just $\|R-S\|/2$.

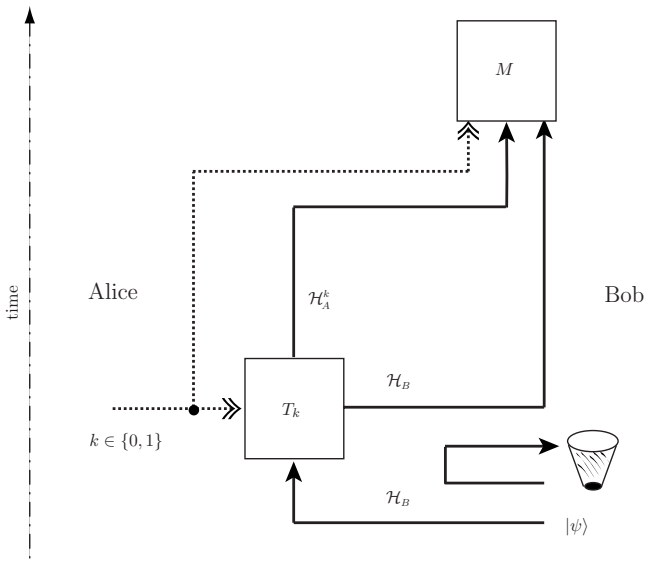

FIG. 4. A quantum bit commitment protocol with local decoherence in Bob's lab. The rubbish bin symbolizes an entanglement-breaking channel acting on Bob's reference system. The figure shows the flow of quantum (solid) and classical (dashed) information if both Alice and Bob play honestly. Alice controls all systems on the left-hand side of the figure, Bob those on the right-hand side. Time flows upwards. The protocol starts with Bob submitting some pure quantum state $|\psi\rangle \in \mathbb{C}^d$ to Alice and ends with Bob's measurement M.

To see that the protocol is binding note first, that Alice's usual cheating strategy cannot work: If there were an operator U such that $(U \otimes \mathbf{1})V_0 \approx V_1$ in norm, the two channels R and S could immediately be estimated to be cb-norm close, in contradiction to the second property guaranteed by lemma 11.

However, it is clearly not enough to argue that there is no *universal* cheating strategy for Alice, which succeeds regardless of Bob's input state. We need to rule out strategies which would allow Alice to fool Bob's test in many cases, or with high probability. In addition, we also have to show security for arbitrary cheating strategies and, in particular, we have to make certain that the reduction of Bob's lab capabilities by the decoherence monster does not also give Alice a bit more freedom to cheat. That is, in order to prove security we have to explain why the coherent record makes a difference for Bob's ability to distinguish the honest strategies, but not for his ability to distinguish honest from cheating strategies in the opening phase. This is the essence of the following theorem.

Theorem 12. Let $\varepsilon > 0$, $\delta > 0$. Then for sufficiently large dimension d the bit commitment protocol described above is perfectly sound, ε concealing, and δ binding. ■

In the proof of theorem 12 we will need to employ some of the standard properties of distance measures for quantum states and operations, which we collect here for reference. We start with the well-known equivalence of the trace-norm distance and the fidelity:

Lemma 13. Let $F(\varrho,\sigma) := \mathrm{tr}\sqrt{\sqrt{\varrho}\sigma\sqrt{\varrho}}$ denote the fidelity of two quantum states ϱ, $\sigma \in \mathcal{B}_*(\mathcal{H})$. We then have

$$1 - F(\varrho,\sigma) \leq \frac{1}{2}\|\varrho - \sigma\|_1 \leq \sqrt{1 - F^2(\varrho,\sigma)}\,. \quad \blacksquare \tag{93}$$

A proof of lemma 13 can be found in Chap. 9.2 of [21].

The fidelity $F(\varrho,\sigma) = \mathrm{tr}\sqrt{\sqrt{\varrho}\sigma\sqrt{\varrho}}$ is symmetric in its inputs and unitarily invariant. It never decreases under quantum operations. If $\varrho = |\varphi\rangle\langle\varphi|$ is pure, we have $F(\varphi,\sigma) = \sqrt{\langle\varphi|\sigma|\varphi\rangle}$. We will also need the following lemma, which appears as lemma 2 in [23]:

Lemma 14. For any two quantum states ϱ, $\sigma \in \mathcal{B}_*(\mathcal{H})$ we have

$$\sup_{\omega \in \mathcal{B}_*(\mathcal{H})} \{F^2(\varrho,\omega) + F^2(\sigma,\omega)\} = 1 + F(\varrho,\sigma)\,. \quad \blacksquare \tag{94}$$

We now proceed from quantum states to quantum operations: The *channel fidelity* of a quantum channel $T: \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ is defined as

$$F_c(T) := F^2(\Omega, T \otimes \mathrm{id}(|\Omega\rangle\langle\Omega|)) = \langle\Omega|T \otimes \mathrm{id}(|\Omega\rangle\langle\Omega|)|\Omega\rangle, \tag{95}$$

where $|\Omega\rangle = \frac{1}{\sqrt{d}}\sum_{j=1}^d |j\rangle \otimes |j\rangle$ is maximally entangled on $\mathbb{C}^d \otimes \mathbb{C}^d$, as before. The channel fidelity $F_c(T)$ is a measure for the quantum channel T to preserve entanglement with a bystander system and is closely related to the *average fidelity* of the channel T,

$$\bar{F}(T) := \int \langle\psi|T(|\psi\rangle\langle\psi|)|\psi\rangle\, d\psi, \tag{96}$$

where the integral is over the normalized Haar measure:

Lemma 15. For any quantum channel $T: \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$, we have

$$\bar{F}(T) \geq F_c(T) \geq \bar{F}(T) - \frac{1}{d}\,. \quad \blacksquare \tag{97}$$

The proof of lemma 15 is immediate from the relation [60,61]

$$\bar{F}(T) = \frac{dF_c(T) + 1}{d + 1}. \tag{98}$$

In the protocol described above we grant the decoherence monster the freedom to apply an arbitrary *entanglement-breaking* quantum channel on Bob's bystander system. Any such channel $D: \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_B)$ can be decomposed [59] as $D = D_1 \circ D_2$, where

$$D_1: \mathcal{C}_X \to \mathcal{B}(\mathcal{H}_B) \tag{99}$$

and

$$D_2: \mathcal{B}(\mathcal{H}_B) \to \mathcal{C}_X, \tag{100}$$

and $\mathcal{C}_X$ denotes the Abelian algebra of the complex-valued functions on the finite set X (with $|X|$ elements). In other words, any entanglement-breaking channel can be thought of as being built from a measurement channel D_1, with resulting

classical output system $\mathcal{C}_X$, followed by a repreparation D_2. [Note that Eqs. (99) and (100) describe the channels D_k in the Heisenberg picture, so the direction of arrows is inverted; cf. the Appendix.]

In order to confirm ε concealment of the monster protocol, we will need to show that any such entanglement-breaking channel D renders Bob's bystander system useless for the analysis of Alice's actions.

Lemma 16. For any linear map $L:\mathcal{B}(\mathcal{H})\to\mathcal{B}(\mathcal{K})$ and any entanglement-breaking channel $D:\mathcal{B}(\mathcal{H}_1)\to\mathcal{B}(\mathcal{K}_1)$,

$$\|L\otimes D\| = \|L\|. \qquad \blacksquare \tag{101}$$

Since entanglement-breaking channels have a decomposition $D_1\circ D_2$ with an intermediate classical system $\mathcal{C}_X$, it will turn out sufficient to verify this property for the noiseless classical channel id_X.

Lemma 17. For any linear map $L:\mathcal{B}(\mathcal{H})\to\mathcal{B}(\mathcal{K})$ and any classical observable algebra $\mathcal{C}_X$,

$$\|L\otimes \mathrm{id}_X\| = \|L\|. \qquad \blacksquare \tag{102}$$

Proof of lemma 17. For any $a\in\mathcal{B}(\mathcal{H})$ we have

$$\|L(a)\| = \|L\otimes \mathrm{id}_X(a\otimes 1_X)\| \leq \|L\otimes \mathrm{id}_X\|\,\|a\|, \tag{103}$$

which shows that $\|L\|\leq\|L\otimes \mathrm{id}_X\|$.

For the converse implication, note that any classical-quantum state ϱ on $\mathcal{B}(\mathcal{K})\otimes\mathcal{C}_X$ is of the form

$$\varrho = \sum_{x=1}^{|X|} p_x\,\varrho_x\otimes|x\rangle\langle x|, \tag{104}$$

where $\{p_x\}_{x=1}^{|X|}$ is a classical probability distribution, $\{\varrho_x\}_{x=1}^{|X|}$ is a set of quantum states on $\mathcal{B}(\mathcal{K})$, and $\{|x\rangle\}_{x=1}^{|X|}$ denotes an orthonormal basis for $\mathbb{C}^{|X|}$ (cf. proposition 2.2.4 in [62]). We may now estimate

$$\begin{aligned}\|(L_*\otimes \mathrm{id}_X)\varrho\|_1 &\leq \sum_{x=1}^{|X|} p_x\,\|L_*(\varrho_x)\otimes|x\rangle\langle x|\|_1 = \sum_{x=1}^{|X|} p_x\,\|L_*(\varrho_x)\|_1\\ &\leq \sum_{x=1}^{|X|} p_x\,\|L\| = \|L\|,\end{aligned} \tag{105}$$

and hence $\|L\otimes \mathrm{id}_X\|\leq\|L\|$, as claimed. $\blacksquare$

Proof of lemma 16. Choosing $a\in\mathcal{B}(\mathcal{H})$, we immediately have

$$\begin{aligned}\|L(a)\| &= \|L(a)\otimes \mathbf{1}_{\mathcal{K}_1}\|\\ &= \|(L\otimes D)(a\otimes \mathbf{1}_{\mathcal{H}_1})\|\\ &\leq \|L\otimes D\|\,\|a\otimes 1_{\mathcal{H}_1}\|\\ &= \|L\otimes D\|\,\|a\|,\end{aligned} \tag{106}$$

implying $\|L\|\leq\|L\otimes D\|$.

For the converse implication, let $D=D_1\circ D_2$ be a decomposition as in Eqs. (99) and (100) above. We may then estimate

$$\begin{aligned}\|L\otimes D\| &= \|L\otimes(D_1\circ D_2)\|\\ &= \|(\mathrm{id}_{\mathcal{K}}\otimes D_1)(L\otimes \mathrm{id}_X)(\mathrm{id}_{\mathcal{H}}\otimes D_2)\|\\ &\leq \|\mathrm{id}_{\mathcal{K}}\otimes D_1\|\,\|L\otimes \mathrm{id}_X\|\,\|\mathrm{id}_{\mathcal{H}}\otimes D_2\|\\ &\leq \|D_1\|_{\mathrm{cb}}\|L\otimes \mathrm{id}_X\|\,\|D_2\|_{\mathrm{cb}}\\ &= \|L\|,\end{aligned} \tag{107}$$

where in the last step we have used lemma 17 and the fact that $\|T\|_{\mathrm{cb}}=1$ for any channel T (cf. the Appendix). $\blacksquare$

We now have all the tools at hand to complete the security proof.

Proof of theorem 12. Soundness of the protocol is clear. Setting $L:=R-S$ in lemma 16, ε concealment follows immediately from lemma 11.

Thus, it only remains to show that the protocol is δ binding. As a warm-up exercise, let us first exclude the possibility of Alice committing to the bit value k in the commitment phase and then announcing the bit $1-k$ in the opening phase. This is sometimes called *passive cheating*.

If Bob has initially supplied the pure state $|\psi\rangle\in\mathbb{C}^d$, the probability of successfully passing Bob's projective measurement in such a scenario is $P(\psi):=|\langle V_0\psi|\,V_1\psi\rangle|^2$, resulting in the overall cheating probability

$$P := \int P(\psi)\,d\psi = \int \langle\psi|V_0^*V_1(|\psi\rangle\langle\psi|)V_1^*V_0|\psi\rangle\,d\psi \overset{(96)}{=} \bar{F}(V_0^*V_1). \tag{108}$$

For δ and d as in lemma 11, we then have the estimate

$$\begin{aligned}2-\delta &\overset{(92)}{\leq} \|T^B_{0*}\otimes \mathrm{id}(|\Omega\rangle\langle\Omega|) - T^B_{1*}\otimes \mathrm{id}(|\Omega\rangle\langle\Omega|)\|_1\\ &\leq \|(V_0\otimes 1)|\Omega\rangle\langle\Omega|(V_0^*\otimes 1) - (V_1\otimes 1)|\Omega\rangle\langle\Omega|(V_1^*\otimes 1)\|_1 \overset{(93)}{\leq} 2\sqrt{1-F^2(V_0\otimes 1|\Omega\rangle, V_1\otimes 1|\Omega\rangle)}\\ &\overset{(95)}{=} 2\sqrt{1-F_c(V_0^*V_1)} \overset{(97)}{\leq} 2\sqrt{1-\bar{F}(V_0^*V_1)+\frac{1}{d}}\\ &\overset{(108)}{=} 2\sqrt{1-P+\frac{1}{d}},\end{aligned} \tag{109}$$

where in the second step we have used that the trace norm cannot increase under the partial trace operation [21]. From Eq. (109) we conclude that

$$P \leq \frac{1}{d}+\delta. \tag{110}$$

Since the right-hand side of Eq. (110) can be made as small as desired by stepping up the dimension, this gives the desired upper bound on Alice's probability of successfully passing Bob's test.

So far we have only proven bindingness against passive cheating attacks. As illustrated in Fig. 5, Alice's most general attack consists of applying some quantum channel $T^\sharp:\mathcal{B}(\mathcal{H}_\sharp)\otimes\mathcal{B}(\mathcal{H}_B)\to\mathcal{B}(\mathcal{H}_B)$ during the commitment phase, independently of the bit value $k\in\{0,1\}$. She will send a d-dimensional quantum system $\mathcal{H}_B$ to Bob without having committed to either bit. Only before the opening will she

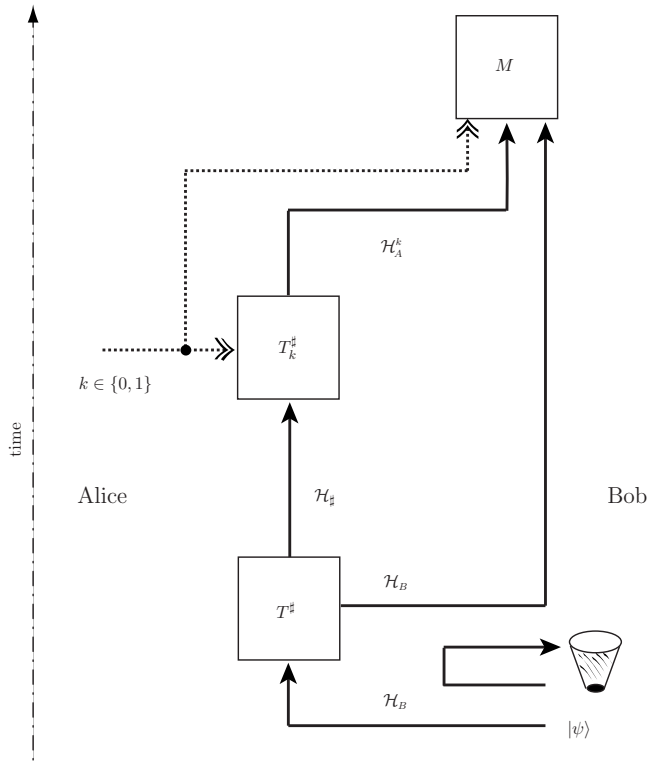

FIG. 5. Alice's cheating strategy consists of applying some quantum channel $T^\sharp$ in the commitment phase and then another quantum channel $T_k^\sharp$ to commit to the bit value $k \in \{0,1\}$ only before the opening. Her goal is to pass Bob's projective measurement M.

then decide on a bit value k, apply a corresponding quantum channel $T_k^\sharp : \mathcal{B}(\mathcal{H}_A^k) \to \mathcal{B}(\mathcal{H}_\sharp)$ on her remaining system, and hope to pass Bob's projective measurement.

Assuming that Alice is a not prejudiced towards either bit, the probability of passing Bob's test is then $P := \frac{1}{2}P_0 + \frac{1}{2}P_1$, where for $k \in \{0,1\}$ we set

$$P_k := \int \langle V_k\psi | (T_{k*}^\sharp \otimes \mathrm{id}_B) T_*^\sharp (|\psi\rangle\langle\psi|) | V_k\psi\rangle \, d\psi. \quad (111)$$

This probability can be bounded as follows:

$$\begin{aligned} P_k &= \int \langle\psi| V_k^* (T_{k*}^\sharp \otimes \mathrm{id}_B) T_*^\sharp (|\psi\rangle\langle\psi|) V_k |\psi\rangle \, d\psi \\ &\overset{(96)}{=} \bar{F}(V_k^* (T_{k*}^\sharp \otimes \mathrm{id}_B) T_*^\sharp V_k) \overset{(97)}{\leqslant} F_c(V_k^* (T_{k*}^\sharp \otimes \mathrm{id}_B) T_*^\sharp V_k) + \frac{1}{d} \\ &\overset{(95)}{=} F^2(V_k \otimes \mathbf{1}_{B'} |\Omega\rangle, (T_{k*}^\sharp \otimes \mathrm{id}_B \otimes \mathrm{id}_{B'})(T_*^\sharp \otimes \mathrm{id}_{B'})(|\Omega\rangle\langle\Omega|)) \\ &\quad + \frac{1}{d} \leqslant F^2(T_{k*}^B \otimes \mathrm{id}_{B'}(|\Omega\rangle\langle\Omega|), \mathrm{tr}_{\mathcal{H}_\sharp} T_*^\sharp \otimes \mathrm{id}_{B'}(|\Omega\rangle\langle\Omega|)) \\ &\quad + \frac{1}{d}, \end{aligned} \quad (112)$$

where in the final step we have used the monotonicity of the fidelity under the partial trace operation. Combining this estimate with lemma 14 and Eq. (92) then immediately yields the bound

$$\begin{aligned} P &\leqslant \frac{1}{2} + \frac{1}{d} + \frac{1}{2} F(R \otimes \mathrm{id}_{B'}(|\Omega\rangle\langle\Omega|), S \otimes \mathrm{id}_{B'}(|\Omega\rangle\langle\Omega|)) \\ &\leqslant \frac{1}{2} + \frac{1}{d} + \frac{1}{2}\sqrt{\delta}. \end{aligned} \quad (113)$$

The right-hand side can be brought as close to $\frac{1}{2}$ as desired by stepping up the dimension. Resubstituting $\frac{1}{d} + \frac{1}{2}\sqrt{\delta} \mapsto \delta$, the protocol is δ binding. This concludes the proof of theorem 12. ■

C. Decoherence in the transmission line

While noise in the transmission line is generally considered a nuisance and coding theorists have designed elaborate error correcting codes to cope with it, Wyner [63] was the first to realize that noise may sometimes be beneficial for cryptographic applications—in his case for key distribution. Crépeau and Kilian [64] later showed that classical noisy channels may also be employed to establish secure bit commitment. Their results have subsequently been improved in [65,66]. Recently Winter *et al.* [67] have considered the asymptotic version of string commitment and have obtained a single-letter expression for the commitment capacity of a classical noisy channel. Their results show that any nontrivial noisy channel can be used to establish secure bit commitment. The theorem can be extended to so-called *classical-quantum* channels. But it remains an open question whether fully quantum channels can also be useful for bit commitment.

Misaligned spatial reference frames can also effectively act as a noisy channel and facilitate secure bit commitment. An example for a secure protocol was recently given by Harrow *et al.* [68].

VI. SUMMARY AND DISCUSSION

In summary, we have presented a general framework for two-party cryptographic protocols and have shown that secure quantum bit commitment is impossible within that framework—by giving explicit bounds on the degree of concealment and bindingness that can be simultaneously achieved in any given protocol. Our proof covers protocols on finite- or infinite-dimensional Hilbert spaces with any number of rounds in each of the commitment, holding, and opening phases. In contrast to earlier proofs, we do not assume the receiver to be bound to a publicly known strategy. Thus, our strengthened no-go result also covers the anonymous state protocols that have been repeatedly suggested as a way to circumvent the standard no go arguments. If the receiver's strategy is fixed and common knowledge, our bounds coincide with those obtained by Spekkens and Rudolph [23], and hence the standard no-go proof is recovered in that case.

Our formulation of the no-go proof contains an explicit treatment of the classical information flow, possibly of independent interest for other cryptographic applications. As a

consequence, the framework directly applies to the purely classical setting, in which no quantum information is exchanged and all local Hilbert spaces are one dimensional. Note, however, that in order to cheat with a sneak flip operation as described in the proof of theorm 4, in general Alice will nevertheless need to apply a quantum operation. This is so because the commutant of Bob's classical system is usually a hybrid containing both classical and quantum parts. Hence, a classical protocol embedded in a quantum world allows Alice to cheat, but the fully classical no-go proof is not directly recovered.

We emphasize that in our setup, Alice and Bob may draw on an unlimited supply of certified classical or quantum correlations, in the form of an arbitrary shared initial state ρ_0, and yet secure quantum bit commitment remains impossible. This is in striking contrast to quantum coin tossing: starting with a maximally entangled qubit state and measuring in a fixed basis, Alice and Bob can obviously implement a perfectly fair and secure coin tossing protocol.

In the second part of the paper, we have analyzed quantum bit commitment protocols relying on decoherence. We have presented a protocol in which provably secure bit commitment is guaranteed through an entanglement-breaking channel in the receiver's lab. The protocol relies on the separation between local erasure of information and the destruction of correlations, which is a purely quantum mechanical effect.

In accordance with most of the literature, throughout this work we have restricted the discussion to quantum bit commitment protocols in which concealment is guaranteed for all branches of the communication tree. This is sometimes called *strong* bit commitment, in order to distinguish it from a weaker form in which Bob may possibly learn the value of the bit—as long as Alice receives a message stating that the bit value has been disclosed. *Weak* bit commitment protocols have been analyzed by Hardy and Kent [30] and independently by Aharonov *et al.* [31]. Such protocols are sufficient whenever bit commitment is only part of a larger cryptographic environment and the value of the bit itself does not reveal any useful information. In particular, secure weak bit commitment protocols could be applied to implement quantum coin tossing. However, weak bit commitment is likewise impossible, with identical bounds on the concealment and bindingness. The no-go proof follows our analysis for strong bit commitment in this paper, but the concealment condition now only has to be guaranteed for a subtree and hence for a subchannel. Alice then finds a sneak flip operation from a version of Stinespring's continuity theorem for subnormalized quantum channels [53].

ACKNOWLEDGMENTS

We would like to thank A. Winter, A. S. Holevo, M. Mosca, A. Kent, J. Oppenheim, M. Christandl, R. Renner, R. König, R. Colbeck, L. Ioannou, M. Keyl, and C. Döscher for fruitful and committed discussions that generated both heat and light. A. Harrow generously shared his insight on bit commitment with local decoherence in Bob's lab. G.M.D. acknowledges extensive and detailed discussions with H. Yuen, whose work essentially stimulated the present one. G.M.D. also acknowledges interesting discussions with H. K. Lo and R. Spekkens and with C. Bennett for clarifying the general philosophy and attitude at the basis of the previous impossibility proofs. D.K. is grateful for financial support from the European Union project RESQ and the German Academic Exchange Service (DAAD). G.M.D acknowledges financial support from Ministero Italiano dell'Università e della Ricerca (MIUR) through PRIN (bandi 2001, 2003, and 2005) and FIRB (bando 2001), and from the U.S. Defence Advanced Research Project Agency under Grant No. F30602-01-2-0528. Part of the work was done at the Max Planck Institute of Complex Systems in Dresden during the International Summer School on Quantum Information.

APPENDIX: LANGUAGE AND NOTATIONS

This appendix contains the necessary background on observables, states, and quantum channels, as well as on direct sums and their role for the description of algebraically encoded classical information. We restrict the discussion to the basics and refer to the textbook of Bratteli and Robinson [69] and Keyl's survey article [62] for a more complete presentation.

Observables, states, and quantum channels

The statistical properties of quantum systems are characterized by spaces of operators on a Hilbert space $\mathcal{H}$: The observables of the system are given by bounded linear operators on $\mathcal{H}$, written $\mathcal{B}(\mathcal{H})$. This is the prototype of a C^* algebra and is usually called the *observable algebra* of the system. The physical states are then those positive linear functionals $\omega:\mathcal{B}(\mathcal{H})\to\mathbb{C}$ which satisfy the normalization condition $\omega(\mathbf{1})=1$. We restrict our discussion to finite-dimensional Hilbert spaces, for which all linear operators are bounded and every linear functional ω can be expressed in terms of a trace-class operator $\varrho_\omega\in\mathcal{B}_*(\mathcal{H})$ such that $\omega(A)=\mathrm{tr}\varrho_\omega A$ for all $A\in\mathcal{B}(\mathcal{H})$. The normalization of the functional ω than translates into the condition $\mathrm{tr}\varrho_\omega=1$. The physical states can thus be identified with the set of normalized density operators $\varrho\in\mathcal{B}_*(\mathcal{H})$.

A *quantum channel* T which transforms input systems described by a Hilbert space $\mathcal{H}_A$ into output systems described by a (possibly different) Hilbert space $\mathcal{H}_B$ is represented (in the Heisenberg picture) by a completely positive and unital map $T:\mathcal{B}(\mathcal{H}_B)\to\mathcal{B}(\mathcal{H}_A)$. By unitality we mean that $T(\mathbf{1}_B)=\mathbf{1}_A$, with the identity operator $\mathbf{1}_X\in\mathcal{B}(\mathcal{H}_X)$. Complete positivity means that $\mathrm{id}_\nu\otimes T$ is positive for all $\nu\in\mathbb{N}$, where id_ν denotes the identity operation on the $(\nu\times\nu)$ matrices.

The physical interpretation of the quantum channel T is the following: when the system is initially in the state $\varrho\in\mathcal{B}_*(\mathcal{H}_A)$, the expectation value of the measurement of the observable $B\in\mathcal{B}(\mathcal{H}_B)$ at the output side of the channel is given in terms of T by $\mathrm{tr}\varrho T(B)$. Unitality provides the normalization, while complete positivity guarantees that all expectation values remain positive even if the channel is only part of a larger network.

Alternatively, we can focus on the dynamics of the states and introduce the dual map $T_*:\mathcal{B}_*(\mathcal{H}_A)\to\mathcal{B}_*(\mathcal{H}_B)$ by means of the duality relation

$$\mathrm{tr}T_*(\varrho)B=\mathrm{tr}\varrho T(B)\ \ \forall\ \ \varrho\in\mathcal{B}_*(\mathcal{H}_A),\ B\in\mathcal{B}(\mathcal{H}_B). \tag{A1}$$

T_* is a completely positive and trace-preserving map and represents the channel in the *Schrödinger picture*, while T provides the *Heisenberg picture* representation. For finite-dimensional systems, the Schrödinger and Heisenberg pictures provide a completely equivalent description of physical processes. The interconversion is always immediate from Eq. (A1).

Direct sums and quantum-classical hybrid systems

Our general description of bit commitment protocols includes a full treatment of the classical and quantum information flow. As explained in Sec. II B, the nodes of the communication tree correspond to the classical information accumulated in the course of the protocol. Direct sums are a convenient way to encode this information in the observable algebras: For a finite collection of observable algebras $\{\mathcal{A}_x\}_{x\in X}$, the direct sum algebra

$$\bigoplus_{x=1}^{X}\mathcal{A}_x:=\{\bigoplus_{x=1}^{X}A_x|A_x\in\mathcal{A}_x\} \tag{A2}$$

represents the physical situation in which the system under consideration is described by an observable algebra $\mathcal{A}_x$ if the classical information $x\in X$ has been accumulated. Sums and products as well as adjoints in this algebra are defined componentwise, i.e.,

$$\bigoplus_x A_x+\bigoplus_x B_x:=\bigoplus_x(A_x+B_x), \tag{A3}$$

$$\bigoplus_x A_x\cdot\bigoplus_x B_x:=\bigoplus_x(A_x\cdot B_x), \tag{A4}$$

$$\alpha\cdot\bigoplus_x A_x:=\bigoplus_x(\alpha\cdot A_x), \tag{A5}$$

$$(\bigoplus_x A_x)^*:=\bigoplus_x A_x^*, \tag{A6}$$

for all operators A_x, $B_x\in\mathcal{A}_x$ and coefficients $\alpha\in\mathbb{C}$. It is straightforward to verify that with these definitions $\oplus_x\mathcal{A}_x$ is indeed an algebra with identity $\mathbf{1}=\oplus_x\mathbf{1}_x$, where for each $x\in X$ $\mathbf{1}_x$ denotes the identity in $\mathcal{A}_x$. The norm on $\oplus_x\mathcal{A}_x$ is given by

$$\left\|\bigoplus_x A_x\right\|:=\max_{x\in X}\|A_x\|. \tag{A7}$$

If $\mathcal{A}_x=\mathcal{B}(\mathcal{H}_x)$ for a collection of Hilbert spaces $\{\mathcal{H}_x\}_{x=1}^X$, then $\oplus_x\mathcal{B}(\mathcal{H}_x)\subset\mathcal{B}(\oplus_x\mathcal{H}_x)$. The physical states on such a system are of the form $\oplus_x p_x\varrho_x$, where $\varrho_x\in\mathcal{B}_*(\mathcal{H}_x)$ are states on the component algebras and $\{p_x\}_{x=1}^X$ is a classical probability distribution.

As explained in Sec. II B, in our formulation of the bit commitment protocol the component algebras $\mathcal{A}_x$ will usually be tensor products of observable algebras in Alice's and Bob's lab, respectively: $\mathcal{A}_x=\mathcal{A}_x(a)\otimes\mathcal{B}_x(b)$. The local algebras $\mathcal{A}_x(a)$ and $\mathcal{B}_x(b)$ could be full matrix algebras or could themselves be direct sums, representing local classical information available to Alice or Bob exclusively. The strategic operations that are performed by Alice and Bob are described by channels acting on these direct sum algebras. In the Heisenberg picture, these channels are completely positive unital maps $T:\mathcal{A}\to\mathcal{B}(\mathcal{H})$ with $\mathcal{A}=\oplus_x\mathcal{A}_x$. Their interpretation is easily seen from Stinespring's representation (proposition 1): There exists a Hilbert space $\mathcal{K}$ and an isometry $V:\mathcal{H}\to\mathcal{K}$ as well as a representation π of $\mathcal{A}$ such that $T(A)=V^*\pi(A)V$ holds. For each $x\in X$, the identity operator of the direct summand $\mathcal{A}_x$ is a projection P_x in $\mathcal{A}$ that commutes with all operators in $\mathcal{A}$. These projections generate an abelian subalgebra $C(\mathcal{A})$ called the *center* of $\mathcal{A}$. Since π is a*-representation and therefore respects the product of operators, $\pi(P_x)$ projects onto the subspace $\pi(P_x)\mathcal{K}:=\mathcal{K}_x$, which is invariant under the action of all represented operators $\pi(\mathcal{A})$. Hence we obtain for every x a representation of $\mathcal{A}$ on $\mathcal{K}_x$ according to

$$\pi_x(A):=\pi(P_x)\pi(A)\pi(P_x)=\pi(A)\pi(P_x). \tag{A8}$$

Since each direct summand $\mathcal{A}_x=\mathcal{B}(\mathcal{H}_x)$ is a full matrix algebra, the Hilbert spaces $\mathcal{K}_x$ can be chosen to be of the form $\mathcal{K}_x=\mathcal{H}_x\otimes\mathcal{M}_x$ with appropriate multiplicity spaces $\mathcal{M}_x$. The representation π_x is then given by $\pi_x(\oplus_x A_x)=A_x\otimes\mathbf{1}_{\mathcal{M}_x}$. In terms of the representations π_x, the action of the channel T on an operator A can be written as

$$T(A)=\sum_{x\in X}V^*\pi_x(A)V. \tag{A9}$$

How is this kind of representation interpreted in operational terms? We first have a look at measurement operations in the Heisenberg picture. Usually a measurement operation is described by a *positive operator valued measure* (POVM), i.e., a collection

$$\left\{M_x\in\mathcal{B}(\mathcal{K})|0\leqslant M_x\leqslant\mathbf{1},\ \sum_x M_x=\mathbf{1}\right\}. \tag{A10}$$

The set X is interpreted as the set of possible measurement outcomes. In the Heisenberg picture, this corresponds to a completely positive normalized map M from the Abelian algebra $\oplus_x\mathbb{C}=\mathbb{C}^X$ into $\mathcal{B}(\mathcal{K})$. Namely, the operator $f\in\mathbb{C}^X$ is mapped to $M(f)=\Sigma_x M_x f_x$. Hence, measurement operations are a special class of channels on direct sum algebras, where each summand is chosen to be one dimensional, $\mathcal{A}_x=\mathbb{C}$. Thus, if we restrict the channel T to the center $C(\mathcal{A})$, which is isomorphic to $\mathbb{C}^X$, then we obtain a measurement operation whose corresponding POVM is given by the operators $\{V^*\pi(P_x)V|x\in X\}$. To verify this, we evaluate T on a central element $C\in C(\mathcal{A})$,

$$T(C) = T\left(\sum_x C_x P_x\right) = \sum_x V^* \pi(P_x) V C_x, \qquad \text{(A11)}$$

where central elements C are expressed as linear combinations of the projections P_x—i.e., $C=\Sigma_x C_x P_x$ with $C_x \in \mathbb{C}$. This justifies the following interpretation: The quantum system under investigation is described by the observable algebra $\mathcal{A}_x$ if the measurement results in the outcome $x \in X$. In other words, the direct sum operation can be seen as a "logical XOR" composition of quantum systems—in contrast to the tensor product, which corresponds to the "logical AND."

Coming back to the bit commitment protocol, the nodes of the communication tree then in fact have a natural interpretation as outcomes of a measurement process returning a history of communicated decisions, which are given by the unique path in the tree starting at its root and ending at $x \in X$.

Distance measures

In order to evaluate the concealment and bindingness conditions in a quantum bit commitment protocol we need to measure the distance between two quantum channels or two quantum states: Assume two channels T_1 and T_2 with common input and output algebras $\mathcal{A}$ and $\mathcal{B}$, respectively. Since these T_i are (in Heisenberg picture) operators between normed spaces $\mathcal{B}$ and $\mathcal{A}$, the natural choice to quantify their distance is the *operator norm*,

$$\|T_1 - T_2\| := \sup_{B \neq 0} \frac{\|T_1(B) - T_2(B)\|}{\|B\|}. \qquad \text{(A12)}$$

The norm distance, Eq. (A12), has a neat operational characterization: it is twice the largest difference between the overall probabilities in two statistical quantum experiments differing only in replacing one use of T_1 with one use of T_2.

However, we also want to allow for more general experiments, in which the two channels are only applied to a sub system of a larger system. This requires *stabilized* distance measures [70] and naturally leads to the so-called *cb norm* [57]

$$\|T_1 - T_2\|_{\mathrm{cb}} := \sup_{\nu \in \mathbb{N}} \|\mathrm{id}_\nu \otimes (T_1 - T_2)\|, \qquad \text{(A13)}$$

where id_ν again denotes the *ideal* (or *noiseless*) channel on the $(\nu \times \nu)$ matrices. Useful properties of the cb norm include *multiplicativity*, i.e., $\|T_1 \otimes T_2\|_{\mathrm{cb}} = \|T_1\|_{\mathrm{cb}} \|T_2\|_{\mathrm{cb}}$, and *unitality*: $\|T\|_{\mathrm{cb}} = 1$ for any channel T.

Obviously, $\|T\|_{\mathrm{cb}} \geqslant \|T\|$ for every linear map T. If either the input or output space is a classical system, we even have the equality $\|T\|_{\mathrm{cb}} = \|T\|$ (cf. Chap. 3 in [57]). Fully quantum systems generically show a separation between these two norms.

States are channels with one-dimensional input space $\mathbb{C}$. Since this is a classical system, there is no need to distinguish between stabilized and nonstabilized distance measures. The so-called *trace norm* $\|\varrho\|_1 = \mathrm{tr}\sqrt{\varrho^* \varrho}$ is frequently employed to evaluate the distance between two density operators. The trace-norm difference $\|\varrho - \sigma\|_1$ is equivalent to the *fidelity* $F(\varrho, \sigma) := \mathrm{tr}\sqrt{\sqrt{\varrho}\sigma\sqrt{\varrho}}$ (cf. lemma 13).

For any linear operator T the operator norm $\|T\|$ equals the norm of the Schrödinger adjoint T_* on the space of trace-class operators—i.e.,

$$\|T\| = \sup_{\|\varrho\|_1 \leqslant 1} \|T_*(\varrho)\|_1 \qquad \text{(A14)}$$

(cf. Chap. VI of [54] and Sec. 2.4 of [69] for details), which is the usual way to convert norm estimates from the Heisenberg picture into the Schrödinger picture and vice versa. For states $T_* = \varrho$, the operator norm then indeed just coincides with the trace norm: $\|T\| = \|T_*\|_1 = \|\varrho\|_1$.

[1] M. Blum, SIGACT News **15**, 23 (1983).

[2] C. H. Bennett, G. Brassard, C. Crépeau, and M. H. Skubiszewska, in *Advances in Cryptology—Proceedings of CRYPTO'91*, edited by Joan Feigenbaum (Springer, Berlin, 1991), p. 351.

[3] C. Crépeau, J. Mod. Opt. **41**, 2455 (1994).

[4] A. C. C. Yao, in *Proceedings of the 27th ACM Symposium on Theory of Computing*, edited by F. Tom Leighton and Allan Borodin (ACM, New York, 1995), p. 67.

[5] J. Kilian, in *Proceedings of the 20th ACM Symposium on Theory of Computing*, edited by J'anos Simon (ACM, New York, 1988), p. 20.

[6] C. Crépeau, J. van de Graaf, and A. Tapp, in *Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'95)*, edited by Don Coppersmith, *Lecture Notes in Computer Science*, Vol. 963 (Springer, Berlin, 1995), p. 110.

[7] G. Brassard, D. Chaum, and C. Crépeau, J. Comput. Syst. Sci. **37**, 156 (1988).

[8] S. Halevi, in *Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'95)*, edited by Don Coppersmith, *Lecture Notes in Computer Science*, Vol. 963, (Springer, Berlin, 1995), p. 84.

[9] S. Halevi and S. Micali, in *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'96)*, edited by Neal Koblitz, *Lecture Notes in Computer Science*, Vol. 1109, (Springer, Berlin, 1996), p. 201.

[10] M. Naor, J. Cryptology **2**, 151 (1991).

[11] R. Ostrovsky, R. Venkatesan, and M. Yung, in *Proceedings of the 9th Annual Symposium on Theoretical Aspects of Computer Science (STACS'92)*, edited by Alain Finkel and Matthias Jantzen, *Lecture Notes in Computer Science*, Vol. 577, (Springer, Berlin, 1992), p. 439.

[12] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175–179.

[13] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[14] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in *Proceedings of the 34th Annual IEEE Symposium on the Founda-*

tions of Computer Science, edited by Leonidas Guibas (IEEE Computer Society Press, Los Alamitos, 1993), p. 362.
[15] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[16] H. K. Lo and H. F. Chau, Physica D **120**, 177 (1998).
[17] D. Mayers, e-print arXiv:quant-ph/9603015.
[18] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[19] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, e-print arXiv:quant-ph/9712023.
[20] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[21] M. A. Nielsen and I. L. Chuang *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[22] A. Kitaev, D. Mayers, J. Preskill, S. Rules, and Q. Protocols, Phys. Rev. A **69**, 052326 (2004).
[23] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).
[24] C. Cachin, C. Crépeau, and J. Marcil, in *Proceedings of the 39th Annual IEEE Symposium on the Foundations of Computer Science (FOCS 1998)*, edited by Rajeev Motwani (IEEE Computer Society Press, Los Alamitos, 1998), p. 493.
[25] Y. Z. Ding, D. Harnik, A. Rosen, and R. Shaltiel, in *Proceedings of Theory of Cryptography—TCC 2004*, edited by Moni Naor, *Lecture Notes in Computer Science*, Vol. 2951, (Springer, Berlin, 2004), p. 446.
[26] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Proceedings of the 46th IEEE Symposium on the Foundations of Computer Science (FOCS 2005)* (IEEE Computer Society Press, Los Alamitos, 2005).
[27] L. Salvail, in *Proceedings of CRYPTO'98*, edited by Hugo Krawczyk, *Lecture Notes in Computer Science*, Vol. 1462 (Springer, Berlin, 1998), p. 338.
[28] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999).
[29] A. Kent, J. Cryptology **18**, 313 (2005).
[30] L. Hardy and A. Kent, Phys. Rev. Lett. **92**, 157901 (2004).
[31] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao, in *Proceedings of the 32nd ACM Symposium on Theory of Computing*, edited by Frances Yao and Eugene Luks (ACM, New York, 2000), p. 705.
[32] A. Kent, Phys. Rev. Lett. **90**, 237901 (2003).
[33] H. Buhrman, M. Christandl, P. Hayden, H. K. Lo, and S. Wehner, e-print arXiv:quant-ph/0504078.
[34] H. Buhrman, M. Christandl, P. Hayden, H. K. Lo, and S. Wehner, Phys. Rev. Lett. **97**, 250501 (2006).
[35] R. Jain, e-print arXiv:quant-ph/0506001.
[36] H. P. Yuen, e-print arXiv:quant-ph/0006109.
[37] H. P. Yuen, e-print arXiv:quant-ph/0305144.
[38] H. P. Yuen, e-print arXiv:quant-ph/0505132.
[39] H. P. Yuen, e-print arXiv:quant-ph/0702074.
[40] C. Y. Cheung, e-print arXiv:quant-ph/0112120.
[41] G. M. D'Ariano, e-print arXiv:quant-ph/0209149.
[42] G. M. D'Ariano, e-print arXiv:quant-ph/0209150.
[43] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, 2nd ed. (Prentice-Hall, Upper Saddle River, NJ, 2006).
[44] T. Rudolph, e-print arXiv:quant-ph/0202143.
[45] B. Schneier, quoted in C. C. Mann, The Atlantic Monthly , No. 9, 81 (2002).
[46] Cited after N. D. Mermin, Phys Rev. 171, 272 (1968), footnote 2.
[47] D. Kretschmann, D. Schlingemann, and R. F. Werner, e-print arXiv:quant-ph/0605009.
[48] V. P. Belavkin, G. M. D'Ariano, and M. Raginsky, J. Math. Phys. **46**, 062106 (2005).
[49] M. Ozawa, (unpublished).
[50] C. Y. Cheung, e-print arXiv:quant-ph/0508180.
[51] C. Y. Cheung, e-print arXiv:quant-ph/0601206.
[52] R. Canetti, in *Proceedings of the 42nd Annual IEEE Symposium on the Foundations of Computer Science (FOCS2001)* (IEEE Computer Society Press, Los Alamitos, 2001), p. 136; extended updated version available from http://eprint. iacr.org/2000/067.
[53] D. Kretschmann, D. Schlingemann, and R. F. Werner (unpublished).
[54] M. Reed, and B. Simon, *Methods of Modern Mathematical Physics I, Functional Analysis* (Academic, New York, 1980).
[55] A. S. Holevo, Probab. Theory Appli. **48**, 359 (2003).
[56] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).
[57] V. I. Paulsen, *Completely Bounded Maps and Operator Algebras* (Cambridge University Press, Cambridge, England, 2002).
[58] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, in *Proceeding of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 547–553, (IEEE, New York, 2000).
[59] M. Horodecki, P. Shor, and M. B. Ruskai, Rev. Math. Phys. **15**, 1 (2003).
[60] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
[61] M. A. Nielsen, Phys. Lett. A **303**, 249 (2002).
[62] M. Keyl, Phys. Rep. **369**, 431 (2002).
[63] A. Wyner, Bell Syst. Tech. J. **54**, 1355 (1975).
[64] C. Crépeau, and J. Kilian, in *Proceedings of the 29th IEEE Symposium on the Foundations of Computer Science (FOCS 1988)*, edited by Walter Fumy (IEEE Computer Society Press, Los Alamitos, 1988), p. 42.
[65] C. Crépeau, in *Proceedings of EUROCRYPT 1997*, edited by Jacques Stern (Springer, Berlin, 1997), p. 306.
[66] I. Damgård, J. Kilian, and L. Salvail, in *Proceedings of EUROCRYPT 1999*, edited by Kenneth G. Paterson (Springer, Berlin, 1999), p. 56.
[67] A. Winter, A. C. Nascimento, and H. Imai, in *Proceedings of the 9th IMA Conference on Cryptography and Coding*, Lecture Notes in Computer Science, Vol. 2898 (Springer, Berlin, 2003).
[68] A. Harrow, R. Oliveira, and B. M. Terhal, Phys. Rev. A **73**, 032311 (2006).
[69] O. Bratteli and D. W. Robinson, *Operator Algebras and Quantum Statistical Mechanics 1*, 2nd ed. (Springer, Berlin, 1987).
[70] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).