# Impossibility of Quantum Bit Commitment, a Categorical Perspective

Feifei He
Institute of Logic and Cognition, Sun Yat-sen University, China

Xin Sun*
Institute of Logic and Cognition, Sun Yat-sen University, China
xin.sun.logic@gmail.com

Quanlong Wang
Department of Computer Science, University of Oxford, United Kingdom

Xishun Zhao
Institute of Logic and Cognition, Sun Yat-sen University, China

Bit commitment is a cryptographic task in which Alice commits a bit to Bob such that she cannot change the value of the bit after her commitment and Bob cannot learn the value of the bit before Alice opens her commitment. According to the MLC no-go theorem, ideal bit commitment is impossible within quantum theory. In the information theoretic-reconstruction of quantum theory, the impossibility of quantum bit commitment is one of the three information-theoretic constrains that characterize quantum theory. In this paper, we first provide a very simple proof of the MLC no-go theorem. Then we formalize bit commitment in the theory of dagger monoidal categories. We show that in the setting of dagger monoidal categories, the impossibility of bit commitment is equivalent to the unitary equivalence of purification.

*Keywords*: bit commitment, categorical quantum mechanics, quantum foundation

## 1 Introduction

Bit commitment, used in a wide range of cryptographic protocols (e.g. zero-knowledge proof, multiparty secure computation, and oblivious transfer), consists of two phases, namely: commit and opening. In the commit phase, Alice the sender chooses a bit $a$ ($a = 0$ or 1) which she wishes to commit to the receiver Bob. Then Alice presents Bob some evidence about the bit. The committed bit cannot be known by Bob prior to the opening phase. Later, in the opening phase, Alice announces some information for reconstructing $a$. Bob then reconstructs a bit $a'$ using Alice's evidence and announcement. A correct bit commitment protocol will ensure that $a' = a$. A bit commitment protocol is concealing if Bob cannot know the bit Alice committed before the opening phase and it is binding if Alice cannot change the bit she committed after the commit phase. It is secure if it is both concealing and binding. It is unconditional secure if it is secure and the security does not rely on any computational assumptions.

Quantum bit commitment (QBC) [4, 19, 7, 36, 25, 26, 29, 20, 27, 2, 30, 40, 38, 32, 22, 45] protocol was first proposed by Bennett and Brassard in 1984 [4]. Later, a number of QBC protocols are designed to achieve unconditional security, such as those of [5, 6]. However, in 1996, Mayers [31] and Lo and

*Corresponding author

Submitted to:
QPL 2019

Chau [28] showed that all previously proposed QBC protocols were vulnerable to an entanglement attack which can be launched by Alice. This result was later referred to as the Mayers-Lo-Chau (MLC) no-go theorem.

This no-go theorem has been continuously challenged in the past two decades. Yuen [43, 44] has repeatedly argued that the no-go proof is not general enough to exhaust all conceivable quantum bit commitment protocols. On the other hand, the no-go theorem has also been extended by several scholars. Spekkens and Rudolph [39] and He [21] extended the no-go theorem with quantitative bounds on the degree of concealment and bindingness. Ariano *et al* [17] provided a strengthened and explicit impossibility proof exhausting all conceivable protocols in which not only quantum information, but also classical information is exchanged between the two parties. However, the considerable length of the proof in [17] makes it still hard to follow. Chiribella *et al* [8] simplifies the proof in [17]. In Cohn-Gordon [16] and Heunen and Kissinger [24], a clear and rigorous formalization of QBC is developed in the setting of categorical quantum mechanics. Cohn-Gordon [16] also provides a proof of the no-go theorem. While this proof is already simpler than all previous proofs, we find there are still rooms of simplification and extension.

In Clifton *et al*'s information theoretic-reconstruction of quantum theory [9], the impossibility of bit commitment is conceived as one of the three fundamental information-theoretic constraints that characterize quantum theory. In [9], the authors partially prove that the impossibility of bit commitment is equivalent to the existence of entangled, or nonlocal, states. This result is questioned by Heunen and Kissinger [24], in which it is demonstrated that in the categorical setting, the impossibility of bit commitment is not equivalent to the existence of entangled states. Which quantum feature is the one that is equivalent to the impossibility of bit commitment is left unanswered in [24].

The contribution of this paper is the following.

1. The length of the proof in Cohn-Gordon [16] is more than two pages. We provide a simpler proof which takes only a few lines.
2. The proof in [16] only concerns the qualitative version of the no-go theorem. We formalize and prove the quantitative version of the no-go theorem.
3. We show that the impossibility of bit commitment is equivalent to the unitary equivalence of purification in the setting of dagger monoidal categories. This provides an answer to the problem left in Heunen and Kissinger [24].

The structure of this paper is the following. We simplify and extend the proof of Cohn-Gordon [16] in Section 2. Then in Section 3 we study the impossibility of bit commitment in the setting of dagger monoidal categories. We conclude this paper with future work in Section 4.

## 2 The no-go theorem of quantum bit commitment

In the literature [31, 28, 39, 16, 24], it is acknowledged that a general model of QBC protocols should at least includes the following ingredients:

1. The Hilbert space required to describe the protocol is the tensor product of the Hilbert spaces that play a role in the protocol.
2. The total system is initially in a pure state.
3. Every action taken by a party corresponds to that party performing a unitary operation on the systems in his/her possession.

4. Every communication corresponds to a party sending a subset of the systems in his/her possession to the other party.

Bearing these common knowledge in mind, we propose a rigorous and simple formalization of quantum bit commitment as follows.

**Definition 1** *A quantum bit commitment protocol consists of the following:*

1. *Two finite dimensional Hiblert spaces A and B.*
2. *Two pure states* $|H\rangle, |T\rangle \in A \otimes B$.
3. *A completely positive map Open on* $A \otimes B$ *such that* $Open(|H\rangle\langle H|)$ *is orthogonal to* $Open(|T\rangle\langle T|)$.[1]

*This QBC protocol is concealing if* $Tr_A|H\rangle = Tr_A|T\rangle$. *It is binding if there is no unitary U on A such that* $(U \otimes I_B)|H\rangle = |T\rangle$.

This formalization provides a high level description of quantum bit commitment. Initially, Alice and Bob jointly prepare a state $|H\rangle$ or $|T\rangle$ of quantum system $A \otimes B$ depending on the value of Alice's bit. (Note that $|H\rangle$ are $|T\rangle$ not the initial state of the QBC protocol, but the final state of the commit phase. Starting from a pure state, a commit phase may involve many rounds of actions and communications.) Alice sends $Tr_A|H\rangle$ or $Tr_A|T\rangle$ to Bob to perform the commitment. At the opening stage, Alice sends the rest sub-state of $|H\rangle$ or $|T\rangle$ to Bob to allow him to verify her commitment. Bob applies the completely positive map *Open* to determine Alice's commitment.

**Example 1** *The QBC protocol due to Bennett and Brassard [4] goes as follows: Alice and Bob first agree on a security parameter, a positive integer s.*

1. *Commit phase:*
   (a) *Alice chooses the value of the committed bit c and the auxiliary bits* $a_1, \ldots, a_s$.
   (b) *If* $c = 0$, *she prepares and sends Bob s qubits which are chosen to be either* $|0\rangle$ *or* $|1\rangle$. *The value of c is kept secret during the commit phase. If* $a_i = 0$, *then Alice sets the i-th qubit to be* $|0\rangle$. *If* $a_i = 1$, *then she sets the i-th qubit to be* $|1\rangle$. *The value of* $a_1, \ldots, a_n$ *are also kept secret during the commit phase.*
   (c) *Similarly, if* $c = 1$, *she prepares and sends Bob s qubits which are chosen to be either* $|+\rangle$ *or* $|-\rangle$. *If* $a_i = 0$, *then Alice sets the i-th qubit to be* $|+\rangle$. *If* $a_i = 1$, *then she sets the i-th qubit to be* $|-\rangle$. *The value of* $c, a_1, \ldots, a_n$ *are kept secret during the commit phase.*
2. *Opening phase:*
   (a) *Bob randomly prepares auxiliary bits* $b_1, \ldots, b_s$. *If* $b_i = 0$, *then Bob measures the i-th qubit in the* $\{|0\rangle, |1\rangle\}$ *basis. If* $b_i = 1$, *then Bob measures the i-th qubit in the* $\{|+\rangle, |-\rangle\}$ *basis.*
   (b) *Alice announcement the value of* $c, a_1, \ldots, a_s$.
   (c) *Bob accepts Alice's commitment if and only if for all indexes* $i \in \{1, \ldots, s\}$ *with* $c = b_i$, *Bob's measurement outcome agrees with Alice's announcement.*

*We can formalize this QBC protocol as follows:*

- *Let* $A = \mathbb{C}^{1+s}$ *and* $B = \mathbb{C}^s$.

[1] A mixed state $\rho$ is orthogonal to another mixed state $\sigma$ if $Tr(\rho^\dagger \sigma) = 0$.

- *Let* $|H\rangle = |0a_1 \ldots a_s\rangle \otimes U_{0,a_1}|0\rangle \ldots U_{0,a_s}|0\rangle$, *where* $U_{0,0}$ *is the identity operator and* $U_{0,1}$ *is the Pauli X operator.*
- *Let* $|T\rangle = |0a_1 \ldots a_s\rangle \otimes U_{1,a_1}|0\rangle \ldots U_{1,a_s}|0\rangle$, *where* $U_{1,0}$ *is the Hadamard operator H and* $U_{1,1}$ *is HX.*
- *Let Open be a completely positive map such that*
  - $Open(|H\rangle\langle H|) = (|0a_1 \ldots a_s\rangle\langle 0a_1 \ldots a_s|) \otimes M_{b_1}(U_{0,a_1}|0\rangle\langle 0|U_{0,a_1}^\dagger) \otimes \ldots \otimes M_{b_s}(U_{0,a_s}|0\rangle\langle 0|U_{0,a_s}^\dagger)$, *where* $M_0$ *is the completely positive map which represents the measurement on the* $\{|0\rangle, |1\rangle\}$ *basis and* $M_1$ *is the completely positive map which represents the measurement on the* $\{|+\rangle, |-\rangle\}$ *basis.*
  - $Open(|T\rangle\langle T|) = (|1a_1 \ldots a_s\rangle\langle 1a_1 \ldots a_s|) \otimes M_{b_1}(U_{1,a_1}|0\rangle\langle 0|U_{1,a_1}^\dagger) \otimes \ldots \otimes M_{b_s}(U_{1,a_s}|0\rangle\langle 0|U_{1,a_s}^\dagger)$.

Note that although our formalization of QBC protocols in Definition 1 looks simple, it is in fact already more general than the formalizations in Lo and Chau [28] and Cohn-Gordon [16]. It is also a proper extension of the purification bit commitment protocol in Spekkens and Rudolph [39].

**Example 2** *A purification bit commitment protocol [39] makes use of two systems, the token system and the proof system. These are associated with Hilbert spaces* $H_t$ *and* $H_p$. *A purification bit commitment protocol also specifies two orthogonal states* $|\phi_0\rangle$ *and* $|\phi_1\rangle$, *which are states of the system* $H_t \otimes H_p$. *At the commit phase, Alice prepares the two systems in the state* $|\phi_b\rangle$ *in order to commit to bit b, and sends the token system to Bob. At the opening phase, Alice sends the proof system to Bob, and Bob performs a measurement of the projector valued measure* $\{P_0, P_1, P_{fail}\}$, *where* $P_b = |\phi_b\rangle\langle\phi_b|$.

## 2.1 The qualitative version of the no-go theorem

Within our formalization, the no-go theorem of quantum bit commitment becomes a precise mathematical statement. To prove this statement, we make use of the unitary equivalence of purification, which can be found in standard textbooks of quantum information [33, 42] .

**Lemma 1 (unitary equivalence of purification)** *Let* $|R_1A\rangle$ *and* $|R_2A\rangle$ *be two purifications of a mixed state* $\rho^A$ *to a composite system RA. There is a unitary transformation U acting on system R such that* $|R_1A\rangle = (U \otimes I_A)|R_2A\rangle$.

**Theorem 1 (no-go theorem, the qualitative version)** *If a quantum bit commitment protocol is concealing, then it is not binding.*

*Proof*: If a QBC is concealing, then $Tr_A(|H\rangle) = Tr_A(|T\rangle)$. Hence $|H\rangle$ and $|T\rangle$ are two purifications of the same mixed state. By Lemma 1 we know there is a unitary operator $U_A$ such that $|H\rangle = (U_A \otimes I_B)|T\rangle$, which means that the QBC is not binding. □

The astonishing simplicity of the above proof suggests a close relationship between the unitary equivalence of purification and the impossibility of quantum bit commitment. In Section 3 we will show that they are actually equivalent in an abstract categorical framework.

## 2.2 The quantitative version of the no-go theorem

The qualitative version of the no-go theorem states that it is impossible for a QBC protocol to be both absolute concealing and absolute binding. However, it does not exclude the possibility of a QBC protocol to be both partially concealing and partially binding. We now formalize and prove the quantitative version of the no-go theorem, which establishes a relation between partially concealing and partially binding. The key notion we are going to use is the fidelity between quantum states.

**Definition 2 (fidelity [33])** *Let $|\phi\rangle$ and $|\psi\rangle$ be two pure states of a Hilbert space. The fidelity of $|\phi\rangle$ and $|\psi\rangle$ is $F(|\phi\rangle,|\psi\rangle) = |\langle\phi|\psi\rangle|^2$. Let $\rho$ and $\sigma$ be two mix states of a Hilbert space. The fidelity of $\rho$ and $\sigma$ is $F(\rho,\sigma) = Tr(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$.*

We define the relation $\overset{\varepsilon}{=}$, where $\varepsilon \in [0,1]$, between quantum states as follows: $\rho \overset{\varepsilon}{=} \sigma$ iff $F(\rho,\sigma) \geq \varepsilon$. Apparently, $\rho = \sigma$ iff $\rho \overset{1}{=} \sigma$.

**Definition 3 ($\varepsilon$-concealing, $\varepsilon$-binding)** *A quantum bit commitment protocol is $\varepsilon$-concealing if $Tr_A|H\rangle \overset{\varepsilon}{=} Tr_A|T\rangle$. It is $\varepsilon$-binding if there is no unitary $U$ on $A$ such that $(U \otimes I_B)|H\rangle \overset{\varepsilon}{=} |T\rangle$.*

The following Uhlmann's theorem will be used in the proof of the quantitative version of the no-go theorem.

**Theorem 2 (Uhlmann's theorem [33])** *$F(\rho,\sigma) = \max\limits_{|\phi\rangle,|\psi\rangle} |\langle\phi|\psi\rangle|$, where $|\phi\rangle$ range over all purifications of $\rho$ and $\psi$ range over range over all purifications of $\sigma$. If $|\phi\rangle$ is a fixed purification of $\rho$, then $F(\rho,\sigma) = \max\limits_{|\psi\rangle} |\langle\phi|\psi\rangle|$, where $\psi$ range over all purifications of $\sigma$.*

**Theorem 3 (no-go theorem, the quantitative version)** *If a quantum bit commitment protocol is $\varepsilon$-concealing, then it is not $\varepsilon^2$-binding.*

*Proof*: If a QBC protocol is $\varepsilon$-concealing, then $Tr_A|H\rangle \overset{\varepsilon}{=} Tr_A|T\rangle$. So we have $F(Tr_A|H\rangle, Tr_A|T\rangle) \geq \varepsilon$. Now by Uhlmann's theorem, we know there exists a purification $|T'\rangle$ of $Tr_A|T\rangle$ such that $|\langle H|T'\rangle| = F(Tr_A|H\rangle, Tr_A|T\rangle) \geq \varepsilon$. Therefore, $F(|H\rangle,|T'\rangle) \geq \varepsilon^2$ and $|H\rangle \overset{\varepsilon^2}{=\!=} |T'\rangle$. Note that by the unitary equivalence of purification, we have $|T'\rangle = (U_A \otimes I_B)|T\rangle$. This means that $(U_A \otimes I_B)|T\rangle \overset{\varepsilon^2}{=\!=} |H\rangle$. Therefore, the QBC protocol is not $\varepsilon^2$-binding. □

## 3 Bit commitment in categorical quantum mechanics

Categorical quantum mechanics [1, 34, 10, 41, 11, 15, 35, 14, 3, 13, 46, 18](CQM) is the study of quantum computation and quantum foundations using category theory, as well as the graphical language closely related to category theory. In CQM, dagger monoidal categories (DMC) are used as an axiomatic basis for quantum mechanics, providing a generalization of the usual axiomatization in terms of Hilbert spaces.

**Definition 4 (strict monoidal category [13])** *A strict monoidal category $\mathscr{C}$ is a category equipped with:*

1. *a parallel composition operation for objects:*

$$\otimes : ob(\mathscr{C}) \times ob(\mathscr{C}) \to ob(\mathscr{C}),$$

2. *a unit object $I \in ob(\mathscr{C})$,*
3. *and a parallel composition operation for morphisms:*

$$\otimes : \mathscr{C}(A,B) \times \mathscr{C}(C,D) \to \mathscr{C}(A \otimes C, B \otimes D)$$

*satisfying the following conditions:*

1. *$\otimes$ is associative and unital on objects:*

$$(A\otimes B)\otimes C = A\otimes(B\otimes C) \qquad A\otimes I = A = I\otimes A,$$

2. *$\otimes$ is associative and unital on morphisms:*

$$(f\otimes g)\otimes h = f\otimes(g\otimes h) \qquad f\otimes 1_I = f = 1_I\otimes f,$$

3. *$\otimes$ and $\circ$ satisfy the interchange law:*

$$(g_1\otimes g_2)\circ(f_1\otimes f_2) = (g_1\circ f_1)\otimes(g_2\circ f_2).$$

**Definition 5 (dagger functor † [13])** *A dagger functor for a strict monoidal category is an operation † that satisfy the following:*

- *identity on objects: $A^\dagger = A$,*
- *reserves morphisms: $(f : A\to B)^\dagger := f^\dagger : B\to A$,*
- *is involutive: $(f^\dagger)^\dagger = f$,*
- *and respects the symmetric monoidal category structure:*

$$(g\circ f)^\dagger = f^\dagger\circ g^\dagger \qquad (f\otimes g)^\dagger = f^\dagger\otimes g^\dagger.$$

A dagger monoidal category is a strict monoidal category equiped with a dagger functor.

**Example 3** *The category of finite dimensional Hilbert spaces **FinHilb** is a DMC. In **FinHilb**, objects are finite dimensional Hilbert spaces over complex numbers, morphisms are linear maps, parallel composition is the tensor product, I is the 1-dimensional Hilbert spaces $\mathbb{C}$, † is the adjoin operator.*

**Example 4** *The category **Dens** of density operators and completely positive maps is a DMC. The objects of **Dens** are the same as the objects of **FinHilb**. A morphism from object $\mathbb{C}^m$ to object $\mathbb{C}^n$ is a completely positive map $f : \mathbb{C}^{m\times m}\to\mathbb{C}^{n\times n}$. Parallel composition is the tensor product, I is the 1-dimensional Hilbert spaces $\mathbb{C}$, † is the adjoin operator.*

**Example 5** *The category of arbitrary dimensional Hilbert spaces **Hilb** is a DMC. In **Hilb**, objects are Hilbert spaces over complex numbers, morphisms are bounded linear maps, parallel composition is the tensor product, I is the 1-dimensional Hilbert spaces $\mathbb{C}$, † is the adjoin operator.*

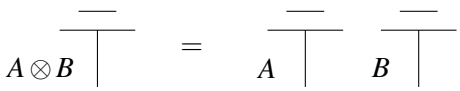
To formalize bit commitment in DMC, we further need concepts such as environment structure and purification.

## 3.1 Environment structure and purification

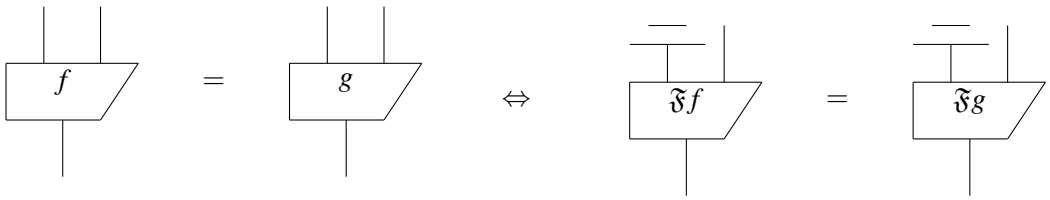
**Definition 6 (environment structure [12])** *Let $\mathscr{C}$ be a dagger monoidal category. An environment structure for $\mathscr{C}$ is a monoidal category $\mathscr{C}^\top$ with the same objects as $\mathscr{C}$, together with a strict monoidal functor $\mathfrak{F} : \mathscr{C}\to\mathscr{C}^\top$ with $\mathfrak{F}(A) = A$, and for each object A a morphism $\top_A : A\to I$ in $\mathscr{C}^\top$, which we depicted as:*


*satisfying:*

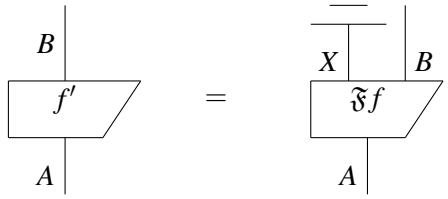
1. *We have $\top_I = 1_I$, and for all objects A and B: $\top_{A\otimes B} = \top_A\otimes\top_B$.*




2. *For morphisms $f : A \to X \otimes B$ and $g : A \to X \otimes B$ in $\mathscr{C}$, they are equivalent if and only if $(\top_X \otimes 1_B) \circ \mathfrak{F}f = (\top_X \otimes 1_B) \circ \mathfrak{F}g$ in $\mathscr{C}^\top$.*



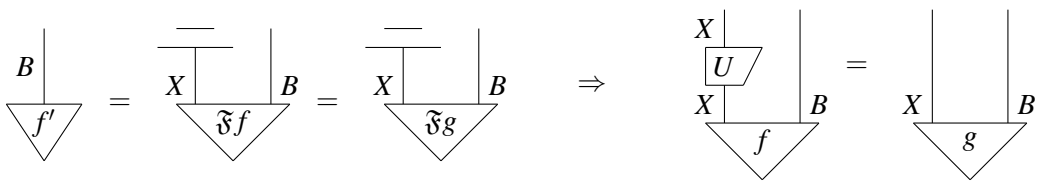

3. *For each $f' \in \mathscr{C}^\top(A,B)$, there is $f \in \mathscr{C}(A, X \otimes B)$ for some object $X$ such that $f' = (\top_X \otimes 1_B) \circ \mathfrak{F}f$ in $\mathscr{C}^\top$. Such an $f$ is called a purification of $f'$.*




Intuitively, if we think of the category $\mathscr{C}$ as consisting of pure states, then the category $\mathscr{C}^\top$ consists of mixed states. The morphisms $\top_A$ can be viewed as to discard system $A$ to the environment, or in other words, trace out $A$.

**Example 6** ***Dens*** *provides an environment structure for* ***FinHilb****, in which $\top_{\mathbb{C}^n}$ is the trace operator $Tr : \mathbb{C}^{n\times n} \to \mathbb{C}$. The functor $\mathfrak{F}$ map a liner map $f \in$ **FinHilb**$(\mathbb{C}^m, \mathbb{C}^n)$ to a completely positive operator $\mathfrak{F}f$ such that $\mathfrak{F}f(\rho) = f\rho f^\dagger$.*

**Definition 7 (unitary equivalence of purification)** *An environment structure $\mathscr{C}^\top$ for $\mathscr{C}$ satisfies the unitary equivalence of purification if the following is satisfied: for all $B \in ob(\mathscr{C}^\top), f' \in \mathscr{C}^\top(I,B)$, if $f, g \in \mathscr{C}(I, X \otimes B)$ are purifications of $f'$, then there exists a unitary morphism $U : X \to X$ such that $(U \otimes 1_B) \circ f = g$.*



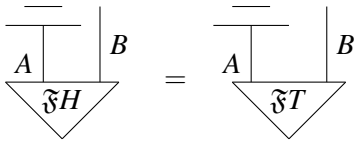

## 3.2 Bit commitment in dagger monoidal category

Now we formalize bit commitment in the setting of dagger monoidal categories. We do not assume compactness in our formalization. This is because assuming compactness will impose finite dimensionality on Hilbert spaces [23]: the DMC **FinHilb** is compact, while **Hilb** is not compact. Assuming no compactness makes our formalization more general than most formalization in the literature, which only formalize bit commitment in finite dimensional Hilbert spaces.

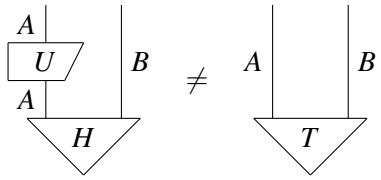
**Definition 8 (bit commitment in DMC)** *Let $\mathscr{C}$ be a dagger monoidal category with an environment structure $\mathscr{C}^{\top}$. A bit commitment protocol on $(\mathscr{C},\mathscr{C}^{\top})$ consists of the following:*

1. *Two objects A and B.*
2. *Two states $H,T : I \to A \otimes B$ in $\mathscr{C}$.*
3. *A morphism Open on $A \otimes B$ in $\mathscr{C}^{\top}$ such that $Open(\mathfrak{F}H) \neq Open(\mathfrak{F}T)$ in $\mathscr{C}^{\top}$.*

A bit commitment protocol on $(\mathscr{C},\mathscr{C}^{\top})$ is concealing if $(\top_A \otimes 1_B) \circ \mathfrak{F}H = (\top_A \otimes 1_B) \circ \mathfrak{F}T$ in $\mathscr{C}^{\top}$.




It is binding if there is no unitary morphism $U : A \to A$ such that $(U \otimes 1_B) \circ H = T$ in $\mathscr{C}$. Equivalently, it is binding if for all unitary morphism $U : A \to A$, it holds that $(U \otimes 1_B) \circ H \neq T$ in $\mathscr{C}$.



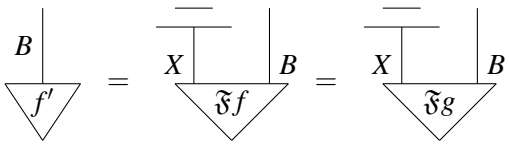

**Theorem 4** *Let $\mathscr{C}$ be a dagger monoidal category with an environment structure $\mathscr{C}^{\top}$. The following are equivalent:*

*(1) The unitary equivalence of purification is satisfied.*

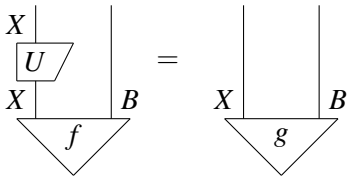
*(2) For all bit commitment protocol on $(\mathscr{C},\mathscr{C}^{\top})$, if it is concealing, then it is not binding.*

Proof: $(1) \Rightarrow (2)$ Assume the unitary equivalence of purification is satisfied. If a bit commitment protocol $(A,B,H,T,Open)$ on $(\mathscr{C},\mathscr{C}^{\top})$ is concealing, then $(\top_A \otimes 1_B) \circ \mathfrak{F}H = (\top_A \otimes 1_B) \circ \mathfrak{F}T$ in $\mathscr{C}^{\top}$. By the third requirement in the definition of environment structure, we know $H$ and $T$ are two purifications of the same state. By the unitary equivalence of purification, we know there is a unitary morphism $U : A \to A$ such that $H = (U \otimes 1_B) \circ T$, which means that the bit commitment protocol is not binding.

$(2) \Rightarrow (1)$ Assume for all bit commitment protocol on $(\mathscr{C},\mathscr{C}^{\top})$, if it is concealing then it is not binding. Let $B$ be an arbitrary object in $\mathscr{C}^{\top}$ and $f' \in \mathscr{C}^{\top}(I,B)$. Assume $f,g \in \mathscr{C}(I,X \otimes B)$ are purifications of $f'$. This means that $f' = (\top_X \otimes 1_B) \circ \mathfrak{F}f = (\top_X \otimes 1_B) \circ \mathfrak{F}g$.




1. If $\mathfrak{F}f = \mathfrak{F}g$, then by the second requirement in the definition of environment structure, we know that $f = g$. Now we let $U = 1_X$. Then it holds that $(U \otimes 1_B) \circ f = g$.
2. If $\mathfrak{F}f \neq \mathfrak{F}g$, then we design a bit commitment protocol $(X,B,f,g,Open)$ in which $Open = 1_{X \otimes B}$. Since $(\top_X \otimes 1_B) \circ \mathfrak{F}f = (\top_X \otimes 1_B) \circ \mathfrak{F}g$, we know this protocol is concealing. Hence it cannot be binding, which means there is a unitary morphism $U : X \to X$ such that $(U \otimes 1_B) \circ f = g$.




To conclude, no matter $\mathfrak{F}f = \mathfrak{F}g$ or $\mathfrak{F}f \neq \mathfrak{F}g$, the unitary equivalence of purification is satisfied. □

## 4 Conclusion and future work

In this paper, we first provide a very simple proof of the no-go theorem of quantum bit commitment. Then we generalize the no-go theorem to the theory of dagger monoidal categories. We show that in the setting of dagger monoidal categories, the impossibility of bit commitment is equivalent to the unitary equivalence of purification.

The presented material also indicates some directions for future research:

1. In Sikora and Selby [37], the authors formalize bit commitment in generalized probabilistic theories and show that the no-go theorem holds by presenting a quantitative trade-off between Alice's and Bob's cheating probabilities. A comparison between our formalization and theirs will be carried out in the future.
2. We also plan to apply the axiomatic and graphical language of categorical quantum mechanics in the formal verification of concrete QBC protocols in the future.

## References


[1] Samson Abramsky & Bob Coecke (2004): *A Categorical Semantics of Quantum Protocols*. In: *19th IEEE Symposium on Logic in Computer Science (LICS 2004), 14-17 July 2004, Turku, Finland, Proceedings*, IEEE Computer Society, pp. 415–425, doi:10.1109/LICS.2004.1319636. Available at https://doi.org/10.1109/LICS.2004.1319636.

[2] Emily Adlam & Adrian Kent (2015): *Device-independent relativistic quantum bit commitment*. *Physical Review A* 92(022315), pp. 1–9.

[3] Miriam Backens (2014): *The ZX-calculus is complete for stabilizer quantum mechanics*. *New Journal of Physics* 16(9), p. 093021, doi:10.1088/1367-2630/16/9/093021. Available at https://doi.org/10.1088%2F1367-2630%2F16%2F9%2F093021.

[4] Charles Bennetta & GillesBrassard (1984): *Quantum cryptography: Public key distribution and coin tossing*. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179.

[5] Gilles Brassard & Claude Crépeau (1990): *Quantum Bit Commitment and Coin Tossing Protocols*. In Alfred Menezes & Scott A. Vanstone, editors: *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference*, Springer, pp. 49–61.

[6] Gilles Brassard, Claude Crépeau, Richard Jozsa & Denis Langlois (1993): *A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties*. In: *34th Annual Symposium on Foundations of Computer Science, Palo Alto, California, USA, 3-5 November 1993*, IEEE Computer Society, pp. 362–371, doi:10.1109/SFCS.1993.366851. Available at https://doi.org/10.1109/SFCS.1993.366851.

[7] Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo & Stephanie Wehner (2008): *Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment*. *Physical Review A* 78(022316), pp. 1–10.

[8] Giulio Chiribella, Giacomo Mauro DAriano, Paolo Perinotti, Dirk Schlingemann & Reinhard Werner (2013): *A short impossibility proof of quantum bit commitment*. *Physics Letters A* 377(15), pp. 1076 – 1087, doi:https://doi.org/10.1016/j.physleta.2013.02.045. Available at http://www.sciencedirect.com/science/article/pii/S0375960113002326.

[9] Rob Clifton, Jeffrey Bub & Hans Halvorson (2003): *Characterizing Quantum Theory in Terms of Information-Theoretic Constraints*. *Foundations of Physics* 33(11), p. 15611591.

[10] Bob Coecke & Ross Duncan (2008): *Interacting Quantum Observables*. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir & Igor Walukiewicz, editors: *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II - Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations*, *Lecture Notes in Computer Science* 5126, Springer, pp. 298–310, doi:10.1007/978-3-540-70583-3_25. Available at https://doi.org/10.1007/978-3-540-70583-3_25.

[11] Bob Coecke & Ross Duncan (2011): *Interacting quantum observables: categorical algebra and diagrammatics*. *New Journal of Physics* 13(043016), pp. 1–85.

[12] Bob Coecke & Chris Heunen (2016): *Pictures of complete positivity in arbitrary dimension*. *Inf. Comput.* 250, pp. 50–58, doi:10.1016/j.ic.2016.02.007. Available at https://doi.org/10.1016/j.ic.2016.02.007.

[13] Bob Coecke & Aleks Kissinger (2017): *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press.

[14] Bob Coecke & Simon Perdrix (2012): *Environment and classical channels in categorical quantum mechanics*. *Logical Methods in Computer Science* 8(4:14), pp. 1–24.

[15] Bob Coecke, Quanlong Wang, Baoshan Wang, Yongjun Wang & Qiye Zhang (2011): *Graphical Calculus for Quantum Key Distribution (Extended Abstract)*. *Electr. Notes Theor. Comput. Sci.* 270(2), pp. 231–249, doi:10.1016/j.entcs.2011.01.034. Available at https://doi.org/10.1016/j.entcs.2011.01.034.

[16] Katriel Cohn-Gordon (2012): *Commitment Algorithms*. Master's thesis, University of Oxford.

[17] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann & Reinhard F. Werner (2007): *Reexamination of quantum bit commitment: The possible and the impossible*. *Phys. Rev. A* 76, p. 032328, doi:10.1103/PhysRevA.76.032328. Available at `https://link.aps.org/doi/10.1103/PhysRevA.76.032328`.

[18] Amar Hadzihasanovic, Kang Feng Ng & Quanlong Wang (2018): *Two complete axiomatisations of pure-state qubit quantum computing*. In Anuj Dawar & Erich Grädel, editors: *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, ACM, pp. 502–511, doi:10.1145/3209108.3209128. Available at `https://doi.org/10.1145/3209108.3209128`.

[19] Lucien Hardy & Adrian Kent (2004): *Cheat Sensitive Quantum Bit Commitment*. *Physical Review Letters* 92(15), pp. 1–4.

[20] Guang Ping He (2014): *Simplified quantum bit commitment using single photon nonlocality*. *Quantum Information Processing* 13(10), pp. 2195–2211, doi:10.1007/s11128-014-0728-8. Available at `https://doi.org/10.1007/s11128-014-0728-8`.

[21] Guang Ping He (2015): *Security bound of cheat sensitive quantum bit commitment*. *Scientific Reports* 5, p. 9398.

[22] Guang Ping He (2019): *Unconditionally secure quantum bit commitment based on the uncertainty principle*. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 475(2222), p. 20180543.

[23] Chris Heunen (2008): *Compactly Accessible Categories and Quantum Key Distribution*. *Logical Methods in Computer Science* 4(4), doi:10.2168/LMCS-4(4:9)2008. Available at `https://doi.org/10.2168/LMCS-4(4:9)2008`.

[24] Chris Heunen & Aleks Kissinger (2016): *Can quantum theory be characterized in terms of information-theoretic constraints?* Http://homepages.inf.ed.ac.uk/cheunen/publications/2016/cbh/cbh.pdf.

[25] Adrian Kent (2011): *Unconditionally secure bit commitment with flying qudits*. *New Journal of Physics* 13(113015), pp. 1–16.

[26] Adrian Kent (2012): *Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes*. *Phys. Rev. Lett.* 109, p. 130501.

[27] Yan-Bing Li, Qiaoyan Wen, Zi-Chen Li, Su-Juan Qin & Ya-Tao Yang (2014): *Cheat sensitive quantum bit commitment via pre- and post-selected quantum states*. *Quantum Information Processing* 13(1), pp. 141–149.

[28] Hoi-Kwong Lo & H. F. Chau (1997): *Is Quantum Bit Commitment Really Possible?* *Physical Review Letters* 78(17), pp. 3410–3413.

[29] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner & H. Zbinden (2013): *Experimental Bit Commitment Based on Quantum Communication and Special Relativity*. *Phys. Rev. Lett.* 111, p. 180504.

[30] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner & H. Zbinden (2015): *Practical Relativistic Bit Commitment*. *Phys. Rev. Lett.* 115, p. 030502.

[31] Dominic Mayers (1997): *Unconditionally secure quantum bit commitment is impossible*. *Physical Review Letters* 78(17), pp. 3414–3417.

[32] Marius Nagy & Naya Nagy (2018): *An Information-Theoretic Perspective on the Quantum Bit Commitment Impossibility Theorem*. *Entropy* 20(3), p. 193, doi:10.3390/e20030193. Available at `https://doi.org/10.3390/e20030193`.

[33] Michael Nielsen & Isaac Chuang (2011): *Quantum Computation and Quantum Information*. Cambridge University Press.

[34] Peter Selinger (2007): *Dagger Compact Closed Categories and Completely Positive Maps: (Extended Abstract)*. *Electr. Notes Theor. Comput. Sci.* 170, pp. 139–163, doi:10.1016/j.entcs.2006.12.018. Available at https://doi.org/10.1016/j.entcs.2006.12.018.

[35] Peter Selinger (2011): *Finite Dimensional Hilbert Spaces are Complete for Dagger Compact Closed Categories (Extended Abstract)*. *Electr. Notes Theor. Comput. Sci.* 270(1), pp. 113–119, doi:10.1016/j.entcs.2011.01.010. Available at https://doi.org/10.1016/j.entcs.2011.01.010.

[36] Kaoru Shimizu, Hiroyuki Fukasaka, Kiyoshi Tamaki & Nobuyuki Imoto (2011): *Cheat-sensitive commitment of a classical bit coded in a block of $m \times n$ round-trip qubits*. *Physical Review A* 84(022308), pp. 1–14.

[37] Jamie Sikora & John Selby (2018): *Simple proof of the impossibility of bit commitment in generalized probabilistic theories using cone programming*. *Physical review A* 97(042302), pp. 1–5.

[38] Yaqi Song & Li Yang (2018): *Practical Quantum Bit Commitment Protocol Based on Quantum Oblivious Transfer*. *Applied Sciences* 8(10), doi:10.3390/app8101990. Available at http://www.mdpi.com/2076-3417/8/10/1990.

[39] R. W. Spekkens & T. Rudolph (2001): *Degrees of concealment and bindingness in quantum bit commitment protocols*. *Phys. Rev. A* 65, p. 012310, doi:10.1103/PhysRevA.65.012310. Available at https://link.aps.org/doi/10.1103/PhysRevA.65.012310.

[40] Ephanielle Verbanis, Anthony Martin, Raphaël Houlmann, Gianluca Boso, Félix Bussières & Hugo Zbinden (2016): *24-Hour Relativistic Bit Commitment*. *Phys. Rev. Lett.* 117, p. 140506.

[41] Jamie Vicary (2011): *Categorical Formulation of Finite-dimensional C*-algebras*. *Electr. Notes Theor. Comput. Sci.* 270(1), pp. 129–145, doi:10.1016/j.entcs.2011.01.012. Available at https://doi.org/10.1016/j.entcs.2011.01.012.

[42] John Watrous (2018): *The Theory of Quantum Information*. Cambridge University Press.

[43] Horace Yuen (2000): *Unconditionally Secure Quantum Bit Commitment Is Possible*. Https://arxiv.org/abs/quant-ph/0006109.

[44] Horace Yuen (2005): *Unconditionally Secure Quantum Bit Commitment*. Https://arxiv.org/abs/quant-ph/0505132.

[45] Lu Zhou, Xin Sun, Chunhua Su, Zhe Liu & Kim-Kwang Raymond Choo (2019): *Game theoretic security of quantum bit commitment*. *Inf. Sci.* 479, pp. 503–514, doi:10.1016/j.ins.2018.03.046. Available at https://doi.org/10.1016/j.ins.2018.03.046.

[46] Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki & Arcangelo Castiglione (2018): *Quantum technique for access control in cloud computing II: Encryption and key distribution*. *J. Network and Computer Applications* 103, pp. 178–184, doi:10.1016/j.jnca.2017.11.012. Available at https://doi.org/10.1016/j.jnca.2017.11.012.