

Quantum Commitments from Complexity Assumptions

André Chailloux¹, Iordanis Kerenidis^{1,2,3}, Bill Rosgen³

arXiv:1010.2793

1) LRI, Université Paris-Sud 2) CNRS 3) CQT, National University of Singapore



Centre for
Quantum
Technologies

National University of Singapore

Overview

We construct two types of noninteractive auxiliary-input bit commitment schemes from worst-case complexity assumptions. We show:

- QSZK $\not\subseteq$ QMA implies quantum commitment with classical advice
- PSPACE $\not\subseteq$ QMA implies quantum commitment with quantum advice

We also provide evidence for the first assumption in the form of a quantum oracle relative to which QSZK $\not\subseteq$ QCMA.

Auxiliary-input commitment schemes

Definition. A quantum commitment scheme is a two-party protocol such that:

- The sender S and the receiver R have a common security parameter 1^n , S has a bit b to be committed, and Both S and R are quantum algorithms that run in time $\text{poly}(n)$.
- In the *commit* phase, the S interacts with the receiver R in order to commit to b .
- In the *reveal* phase, S interacts with the receiver R to reveal b . R accepts or rejects depending on the revealed value of b and his final state. If S is honest R always accepts.

Definition. A *non-interactive* quantum commitment scheme is *secure* if it satisfies:

Hiding: ρ_0 and ρ_1 sent by the honest sender in the commit phase are indistinguishable.

Binding: For any senders S_0^*, S_1^* who commit to the same state and any $p \in \text{poly}$

$$\frac{1}{2} (\Pr[S_0^* \text{ reveals } b = 0] + \Pr[S_1^* \text{ reveals } b = 1]) \leq \frac{1}{2} + \frac{1}{p(n)}$$

These security properties can hold in one of two ways:

Statistically: against computationally unbounded adversaries

Computationally: against quantum polynomial-time adversaries with quantum advice

Both properties cannot hold statistically without further restrictions on cheating parties.

Definition. An *auxiliary-input* commitment scheme takes an extra parameter $x \in I$ (the security parameter is $n = |x|$). Such a protocol must be secure for *some* infinite set I . We also require that the protocol can be (constructed and) performed efficiently in $|x|$.

Complexity assumptions

We use two complexity assumptions:

QSZK $\not\subseteq$ QMA: This assumption is strong, but it would be a surprise if we could replace the entanglement between the parties in QSZK proof systems with a single message. As further evidence, we extend the techniques in [1] to show:

Theorem. There exists a quantum oracle A such that $\text{QSZK}_{\text{HV}}^A \not\subseteq \text{QCMA}^A$.

PSPACE $\not\subseteq$ QMA: This assumption is much weaker

$$\text{QMA} \subseteq \text{PP} \subseteq \text{PSPACE},$$

and so if false, implies that $\text{PP} = \text{PSPACE}$. The ‘classical’ version of our assumption is $\text{AM} \not\subseteq \text{MA}$, which is false under derandomization assumptions.

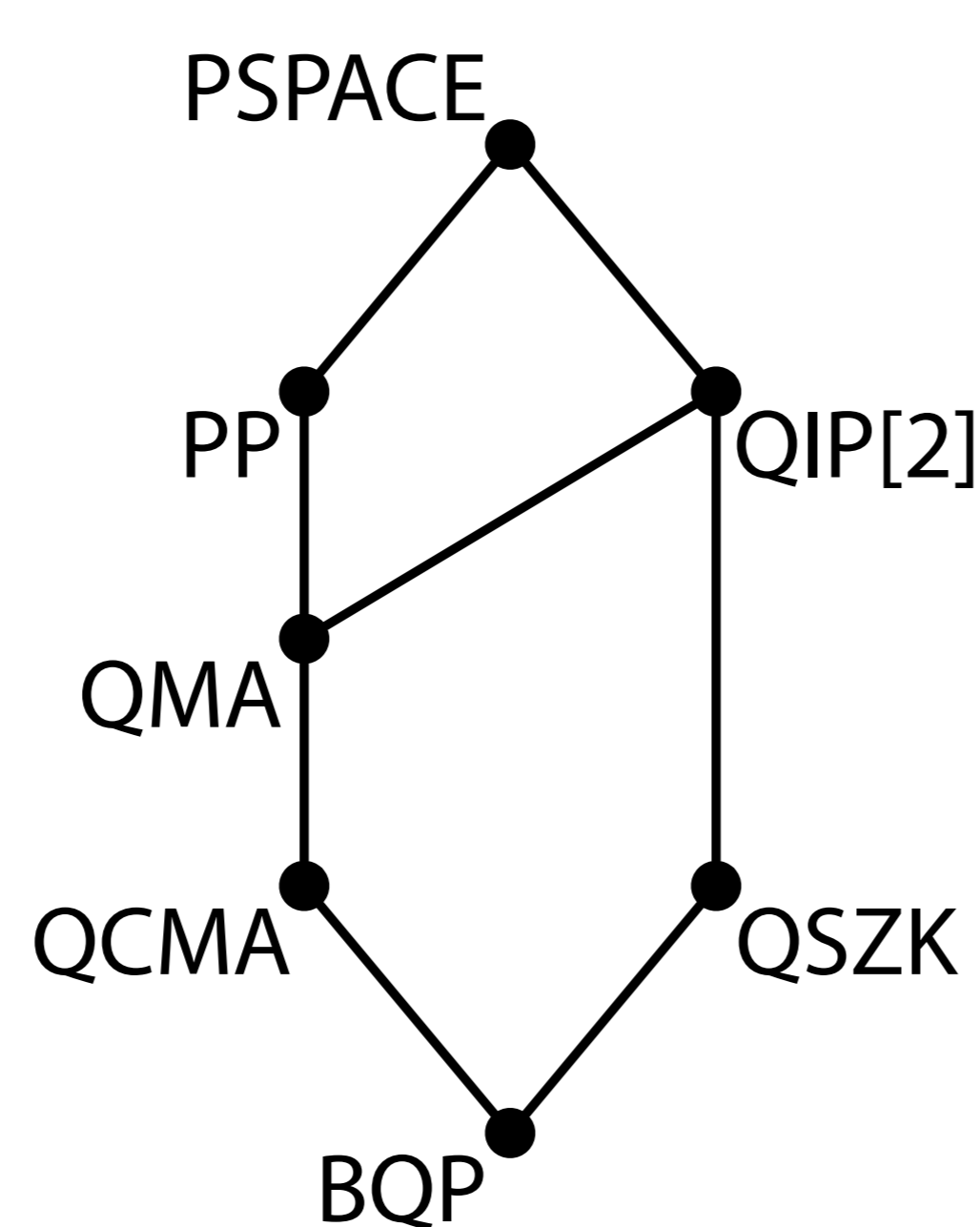


Figure 1: Known relationships between complexity classes.

Complete problems for quantum classes

We use two distinguishability problems: the idea is to use hard instances to build commitment schemes. If no such instances exist, then we can put these problems into QMA.

Definition (QSD Problem). For μ a negligible function, the promise problem QSD = $\{\text{QSD}_Y, \text{QSD}_N\}$ takes as input two quantum circuits C_0, C_1 with $\rho_i = \text{tr}_2 C_i|0\rangle$ such that

$$\begin{aligned} (C_0, C_1) \in \text{QSD}_Y &\Leftrightarrow \|\rho_0 - \rho_1\|_{\text{tr}} \geq 2 - \mu(n) \\ (C_0, C_1) \in \text{QSD}_N &\Leftrightarrow \|\rho_0 - \rho_1\|_{\text{tr}} \leq \mu(n) \end{aligned}$$

This problem is complete for QSZK [3].

Definition (QCD Problem). For μ a negligible function, the promise problem QCD = $\{\text{QCD}_Y, \text{QCD}_N\}$ takes as input two quantum circuits C_0, C_1 such that

$$\begin{aligned} (C_0, C_1) \in \text{QCD}_Y &\Leftrightarrow \|C_0 - C_1\|_{\diamond} \geq 2 - \mu(n) \\ (C_0, C_1) \in \text{QCD}_N &\Leftrightarrow \|C_0 - C_1\|_{\diamond} \leq \mu(n). \end{aligned}$$

This problem is complete for QIP = PSPACE [2].

Commitments if QSZK is not in QMA

The auxiliary-input to the protocol is any instance $(C_0, C_1) \in \text{QSD}_Y$. This is a pair of circuits whose output states $\rho_i = \text{tr}_2 C_i|0\rangle$ are statistically distinguishable. Given these circuits, the protocol is:

Commit: The sender commits to i by computing $C_i|0\rangle$ and sending the first system.

Reveal: The sender sends the second system as well as i . The receiver checks by running C_i in reverse and measuring the output, accepting only if it is $|0\rangle$.

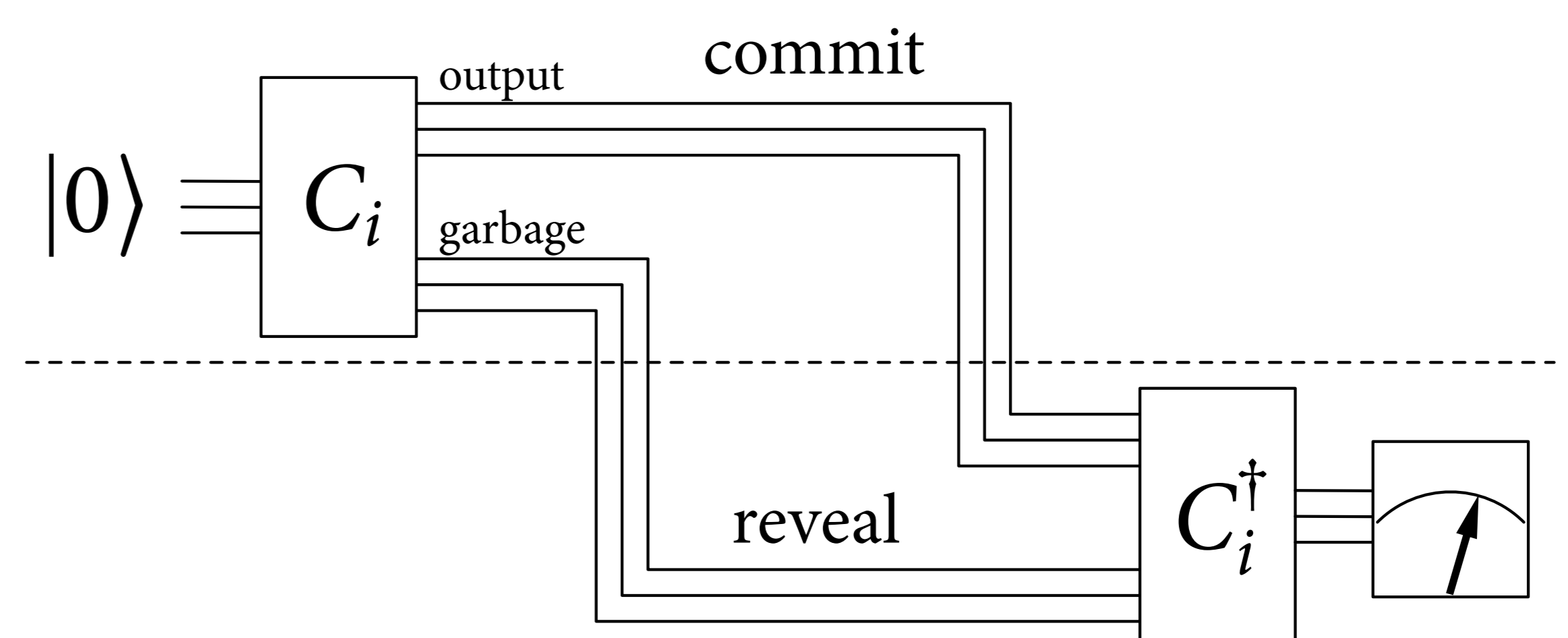


Figure 2: The sender commits by sending the first system. The receiver checks by receiving the second system and uncomputing C_i to verify that the result is the initial state.

Theorem. If QSZK $\not\subseteq$ QMA, then the auxiliary-input protocol in Figure 2 is both statistically-binding and computationally-hiding.

Idea. We argue that subject to our complexity assumption, there are infinitely many pairs of circuits whose outputs are not *computationally* distinguishable, i.e. unless the protocol is computationally-hiding for infinitely many $(C_0, C_1) \in \text{QSD}_Y$ then there exists a QMA protocol for the QSD problem.

If the protocol is not computationally-hiding, then the states ρ_i can be distinguished efficiently (with quantum advice). A QMA protocol to distinguish them has the prover sending a description of an efficient distinguishing circuit along with any quantum advice state needed. This implies that unless the protocol is hiding for infinitely many auxiliary inputs (C_0, C_1) , then all but a finite number of QSD instances can be solved in QMA. Since this finite number can be hardcoded, either the protocol is hiding or QSZK \subseteq QMA. \square

If we weaken our security requirement to demand hiding against adversaries with classical (and not quantum) advice, we can weaken the assumption to QSZK $\not\subseteq$ QCMA.

Commitments if PSPACE is not in QMA

Given any instance $(C_0, C_1) \in \text{QCD}_Y$ and as quantum advice (to both parties) the input state $|\psi\rangle$ that maximizes the distinguishability of the output, we find a similar protocol.

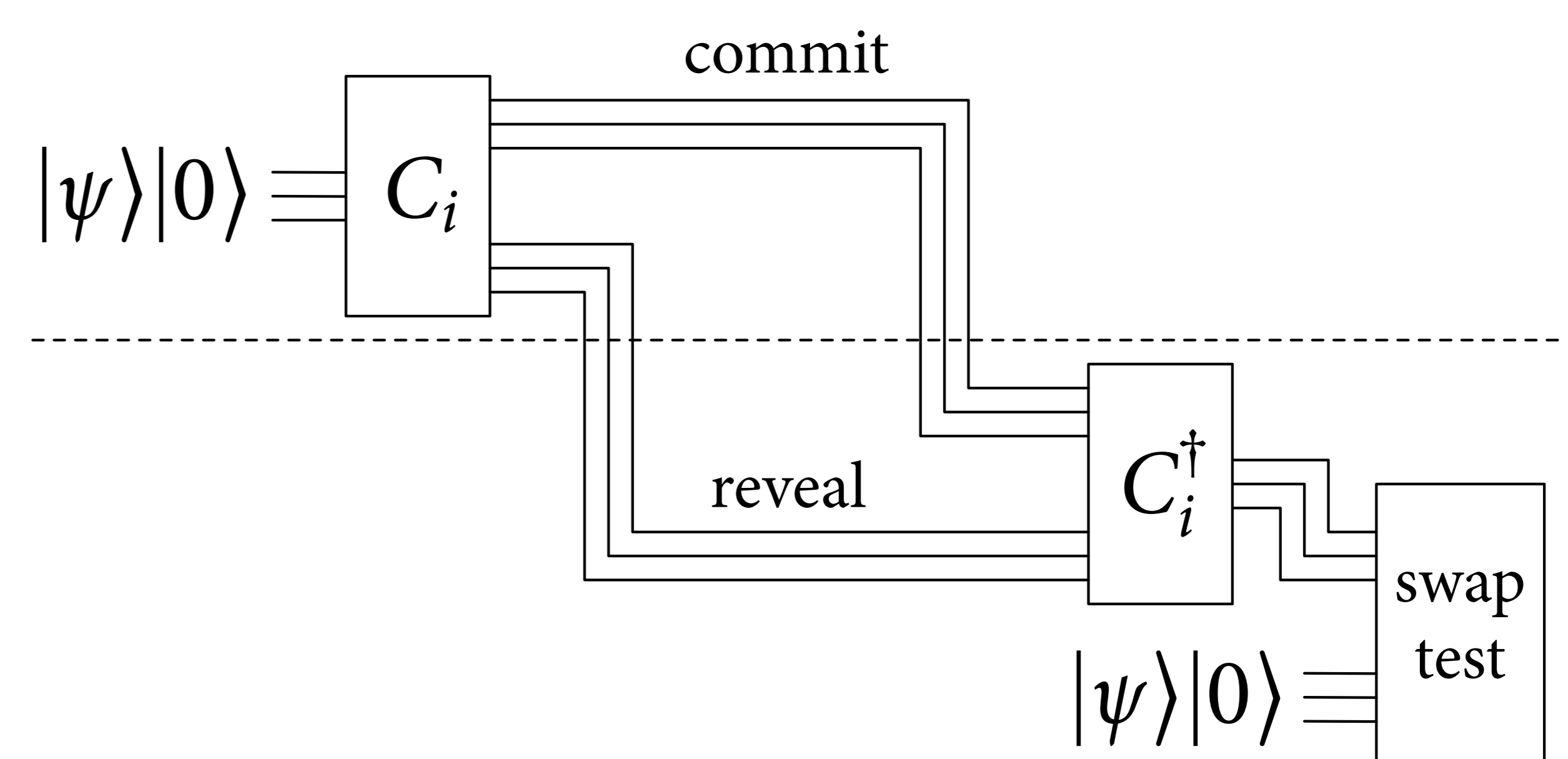


Figure 3: This protocol is the same as the previous one, with the exception that after the receiver uncomputes C_i the swap test is used to check that the result is the initial state.

This protocol achieved only constant binding error (from the swap test). We prove an amplification result for protocols based on the swap test to obtain:

Theorem. If PSPACE $\not\subseteq$ QMA then a k -fold parallel-repetition of the protocol in Figure 3 is an auxiliary-input quantum commitment scheme with quantum advice that is statistically-binding and computationally-hiding.

We also use a different PSPACE-complete problem to construct a commitment protocol with quantum advice that is computationally-binding and statistically-hiding, under the assumption that PSPACE $\not\subseteq$ QMA.

References

- [1] S. Aaronson and G. Kuperberg. *Theory of Computing*, 3(7):129–157, 2007.
- [2] B. Rosgen and J. Watrous. In *Proc. CCC*, 344–354, 2005.
- [3] J. Watrous. In *Proc. FOCS*, 459–468, 2002.