

# Quantum Commitments From Complexity Assumptions

André Chailloux  
LRI, Université Paris-Sud

Iordanis Kerenidis  
LRI, CNRS, Université Paris-Sud

**Bill Rosgen**  
CQT, National U. Singapore

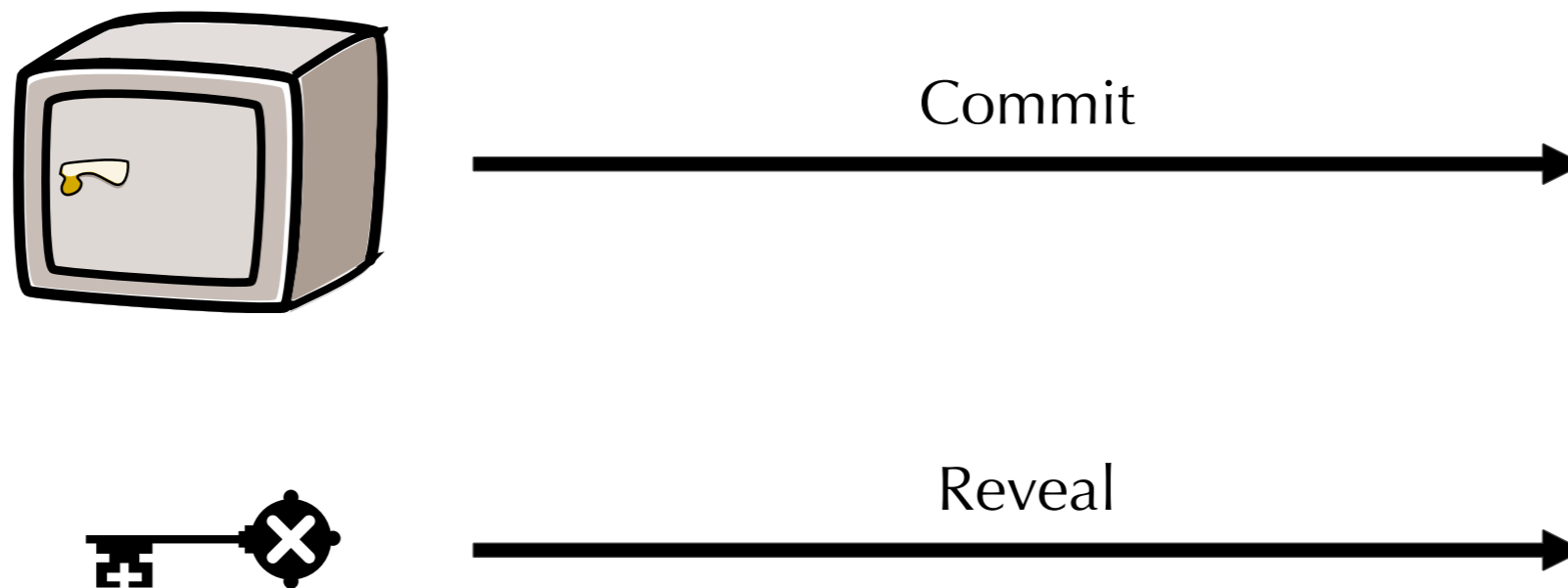
4 July 2011, ICALP



# Bit Commitment

A bit commitment protocol sends one classical bit from Alice to Bob over two phases (*commit* and *reveal*) satisfying two properties:

- ▶ **Hiding:** Bob is unable to learn the bit before the reveal phase
- ▶ **Binding:** Alice is unable to change the bit after the commit phase



We are interested in protocols where the communication between Alice and Bob is quantum, but the goal remains to commit one *classical* bit

# Bit Commitment is Impossible

Even when Alice and Bob use quantum information, no statistically binding and hiding protocol exists. [Mayers 97, Lo and Chau 97]

Assumptions that lead to bit commitment schemes:

- ▶ One way functions [HNORV 09]
- ▶ Pseudorandom generators [Naor 89]
- ▶ Limits on adversary's quantum memory [DFSS05, WST08]
- ▶ Hardness of factoring / discrete log

We consider *worst-case* complexity assumptions

- ▶ These lead to *auxiliary-input* commitment protocols, which are protocols that use quantum or classical advice

If  $\mathbf{ZK} \neq \mathbf{SZK}$  then auxiliary-input one-way functions exist [Vadhan 06]

# Quantum Commitments from Complexity

From complexity assumptions we construct computationally-secure auxiliary-input quantum commitment schemes:

Complexity Assumption	Protocol Requires	Secure Against
$QSZK \not\subseteq QCMA$	classical aux-input	classical advice
$QSZK \not\subseteq QMA$	classical aux-input	quantum advice
$PSPACE \not\subseteq QMA$	quantum aux-input	quantum advice

# Outline of Talk

- 1) Background: Bit Commitment and Quantum Complexity
- 2) Main Idea
- 3) **QSZK** vs **QMA** Protocol
- 4) **PSPACE** vs **QMA** Protocol

# Distance Measures

The *trace norm* provides a natural distance on quantum states.

$$\|X\|_{\text{tr}} = \|X\|_1 = \text{tr}\sqrt{X^*X}$$

Given one copy of a state in  $\{\rho_1, \rho_2\}$ , it can be identified with probability

$$\frac{1}{2} + \frac{1}{4}\|\rho_1 - \rho_2\|_{\text{tr}}$$

The *diamond norm* provides a natural distance on quantum channels

$$\|\Phi\|_{\diamond} = \max_{|\psi\rangle} \|(\Phi \otimes I)(|\psi\rangle\langle\psi|)\|_{\text{tr}}$$

Given one use of a channel in  $\{\Phi_1, \Phi_2\}$ , it can be identified with prob.

$$\frac{1}{2} + \frac{1}{4}\|\Phi_1 - \Phi_2\|_{\diamond}$$

# Bit Commitment Security Definition

The protocols we construct are *non-interactive*.

Basic protocol:

1. Alice constructs one of  $|\psi_0\rangle, |\psi_1\rangle \in \mathcal{A} \otimes \mathcal{B}$ , depending on her bit  $b$
2. *Commit*: Alice sends  $\rho_b = \text{tr}_{\mathcal{B}} |\psi_b\rangle\langle\psi_b|$
3. *Reveal*: Alice sends  $b$  and remaining qubits, Bob measures  $|\psi_b\rangle\langle\psi_b|$

This protocol is *statistically* secure if for some negligible  $\varepsilon$

**Hiding:**  $\|\rho_0 - \rho_1\|_{\text{tr}} \leq \varepsilon$

**Binding:** for any strategies  $S_0$  and  $S_1$  of Alice that both commit to  $\sigma$

$$\frac{1}{2} (\Pr[S_0 \text{ reveals } 0] + \Pr[S_1 \text{ reveals } 1]) \leq \frac{1}{2} + \varepsilon$$

Note: this is a *weak* definition

# Computational Hiding

We do not require that  $\|\rho_0 - \rho_1\|_{\text{tr}} \leq \varepsilon$ : only that the two states are not computationally distinguishable.

**Definition:** [Watrous09]  $\rho_0, \rho_1$  are  $(p, q, r)$ -distinguishable if there is a state  $\sigma$  on  $p$  qubits and a circuit  $D$  of size  $q$  performing a binary measurement s.t.

$$|\Pr[D(\rho_0 \otimes \sigma) = 0] - \Pr[D(\rho_1 \otimes \sigma) = 0]| \geq \frac{1}{r}$$

$\rho_0, \rho_1$  are *computationally indistinguishable* if they are not distinguishable for any polynomials  $p, q, r$  (in the number of qubits of  $\rho_0, \rho_1$ ).

Bit commitment is computationally-binding and statistically-hiding if

**Hiding:**  $\rho_0, \rho_1$  are computationally indistinguishable

**Binding:** for any strategies  $S_0$  and  $S_1$  of Alice that both commit to  $\sigma$

$$\frac{1}{2} (\Pr[S_0 \text{ reveals } 0] + \Pr[S_1 \text{ reveals } 1]) \leq \frac{1}{2} + \varepsilon$$

# Quantum Computational Complexity

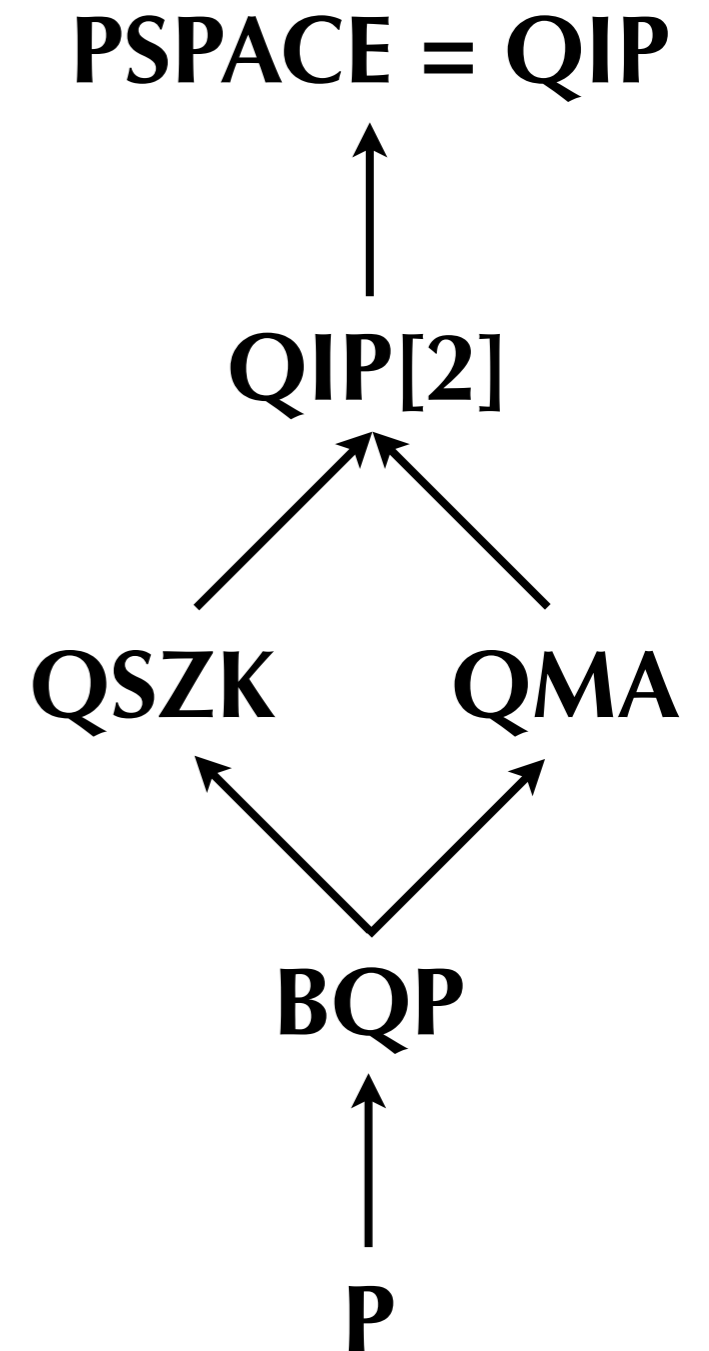
**QMA** is the class of all problems that can be decided with the help of a quantum proof state.

**QSZK** is the class of problems that can be decided when interacting with a prover, where the Verifier learns nothing other than what is being decided.

**QIP** is the class of problems that can be decided when interacting with a quantum prover.

Complexity assumptions that we consider:

- ▶ **QSZK  $\not\subseteq$  QMA**
- ▶ **QIP  $\not\subseteq$  QMA**



# Distinguishing Quantum States

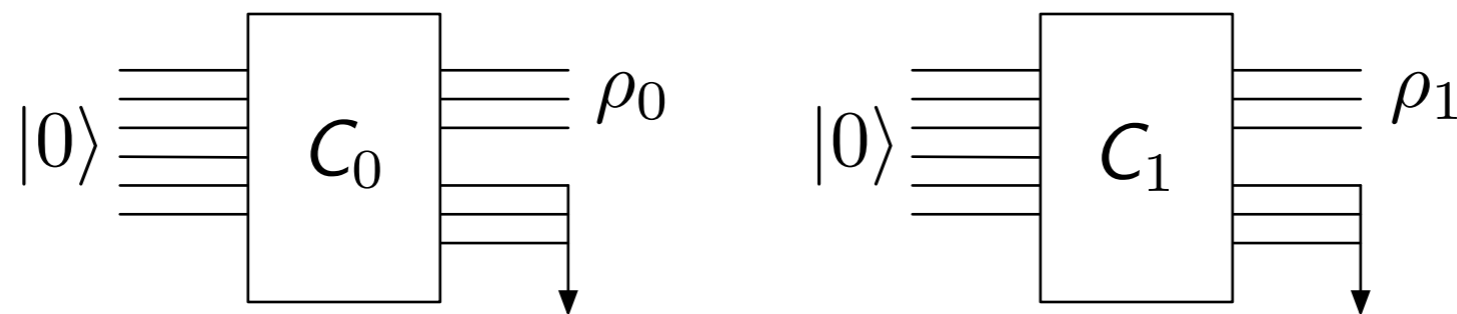
Given two quantum states, how hard to decide if they are close?

## Problem (QSD):

**Input:**  $C_0, C_1$  unitary quantum circuits  $\mathcal{A} \rightarrow \mathcal{O} \otimes \mathcal{G}$  producing states given by  $\rho_i = \text{tr}_{\mathcal{G}} C_i(|0\rangle\langle 0|)$

**Yes:**  $\|\rho_0 - \rho_1\|_{\text{tr}} \geq 2 - \varepsilon$

**No:**  $\|\rho_0 - \rho_1\|_{\text{tr}} \leq \varepsilon$



This problem is complete for **QSZK** [Watrous 02]. We may take  $\varepsilon$  negligible in the size of the circuits  $C_0$  and  $C_1$ .

# Distinguishing Quantum Channels

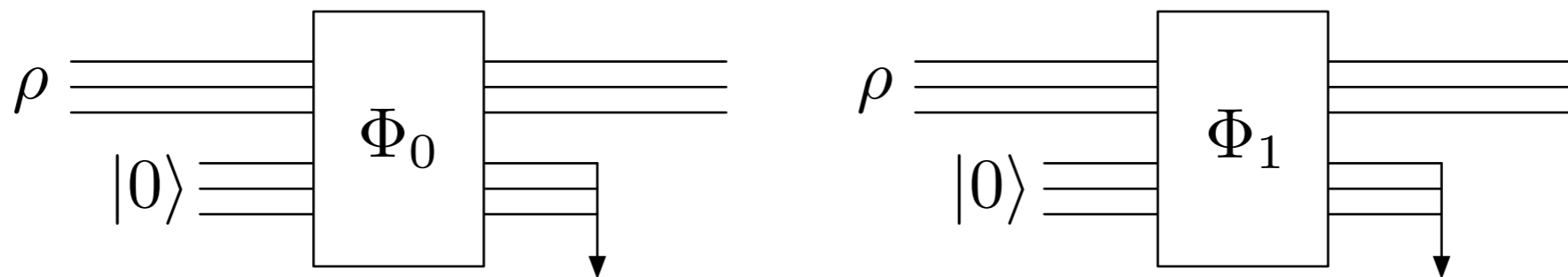
Given two quantum channels, how hard to decide if they are close?  
Channels are only close if they are nearly the same on *all* inputs.

## Problem (QCD):

**Input:**  $\Phi_0, \Phi_1$  quantum circuits  $\mathcal{I} \rightarrow \mathcal{O}$  using aux. spaces  $\mathcal{A}, \mathcal{G}$

**Yes:**  $\|\Phi_0 - \Phi_1\|_{\diamond} \geq 2 - \varepsilon$

**No:**  $\|\Phi_0 - \Phi_1\|_{\diamond} \leq \varepsilon$



This problem is complete for **QIP** [R., Watrous 05]. We may once more take  $\varepsilon$  negligible in the size of the circuits (and **QIP = PSPACE** [JJUW10]).

# Outline of Talk

1) Background: Bit Commitment and Quantum Complexity

2) *Main Idea*

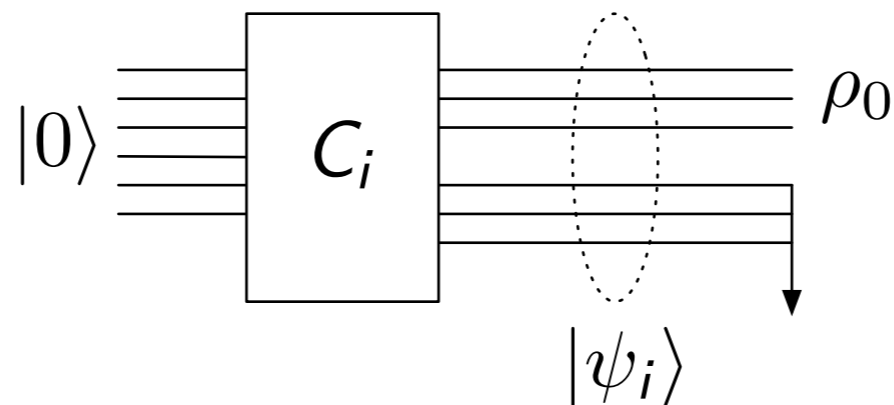
3) **QSZK** vs **QMA** Protocol

4) **PSPACE** vs **QMA** Protocol

# If Distinguishing is Computationally Hard ...

If **QSD** is 'hard', then there exists a 'yes' instance  $(C_0, C_1)$  that results in states  $\rho_0, \rho_1$  that are far apart, but cannot be distinguished computationally.

I.e. there exist states  $|\psi_i\rangle = C_i(|0\rangle)$  whose reduced states  $\rho_i = \text{tr}_{\mathcal{G}} |\psi_i\rangle\langle\psi_i|$  satisfy  $\|\rho_0 - \rho_1\|_{\text{tr}} \geq 2 - \varepsilon$  but cannot be (efficiently) distinguished.



However, the states  $|\psi_0\rangle, |\psi_1\rangle$  can be efficiently distinguished:

▶ Running  $C_j$  in reverse on  $|\psi_i\rangle$  results in the state  $|0\rangle$  with probability:

$$1 \text{ if } i = j$$

$$\varepsilon \text{ if } i \neq j$$

# The Bit Commitment Protocol

## Protocol:

1. **Commit:** Alice uses  $C_b$  to obtain the state  $|\psi_b\rangle$  and sends the portion in the space  $\mathcal{O}$  to Bob (who now holds  $\rho_b$ )
2. **Reveal:** Alice sends  $b$  and the remaining qubits (in space  $\mathcal{G}$ ) to Bob. Bob runs  $C_b$  in reverse and measures, accepting iff result is  $|0\rangle$

## Security (sketch):

**Hiding:** if we assume that our instance of **QSD** is ‘hard’, then by assumption Bob cannot distinguish  $\rho_0, \rho_1$  and so cannot learn  $b$  early.

**Binding:** If Alice commits to a state  $\xi$ , then  $\|\rho_0 - \rho_1\|_{\text{tr}} \geq 2 - \varepsilon$  implies that regardless of what she sends in the reveal phase

$$\frac{1}{2} (\Pr[A \text{ reveals } 0] + \Pr[A \text{ reveals } 1]) \leq \frac{1}{2} + \frac{\sqrt{\varepsilon}}{2}$$

# Outline of Talk

- 1) Background: Bit Commitment and Quantum Complexity
- 2) Main Idea
- 3) **QSZK** vs **QMA** Protocol
- 4) **PSPACE** vs **QMA** Protocol

# Auxiliary-input (In)distinguishability

For this protocol, Alice and Bob need a ‘hard’ instance of **QSD**

We model this as an auxiliary input (i.e. *advice*), and modify our security definitions to account for this.

**Definition:** Given an index set  $\Lambda$ , ensembles  $\{\rho_{0,x}\}$  and  $\{\rho_{1,x}\}$  are computationally indistinguishable if *for all but finitely many*  $x$ , the states  $\rho_{0,x}$  and  $\rho_{1,x}$  are computationally indistinguishable. The ensembles are computationally distinguishable if they are distinguishable *for all*  $x$ .

- ▶ In our case, the input  $x$  will encode a pair of circuits  $(C_0, C_1)$ .
- ▶ The length of  $x$  will be the security parameter.
- ▶ We require indistinguishability only for almost all  $x$  because a polynomial adversary can solve small instances.

# If QSZK is not in QMA ...

**Lemma:** If **QSZK** is not in **QMA**, there exist aux-input ensembles that are computationally indistinguishable on some infinite set  $\Lambda$ .

*Proof Sketch:* Consider **QSD**<sub>Y</sub>, the set of circuits producing distinguishable states, and let  $\{\rho_{0,x}\}$  and  $\{\rho_{1,x}\}$  be the ensembles of states obtained from a pair  $(C_0, C_1) = x$  in **QSD**<sub>Y</sub>. Assume for contradiction that  $\{\rho_{0,x}\}$  and  $\{\rho_{1,x}\}$  are computationally distinguishable.

Then consider the following **QMA** algorithm for **QSD** on input  $x$ :

- ▶ Proof is  $D$ , the distinguishing circuit and  $\sigma$ , the side information.
- ▶ Verifier generates  $\rho_r$  for random  $r$ , applies  $D$ , accepts if output is  $r$

Success probability on **QSD**<sub>Y</sub>:  $1/2 + 1/\text{poly}$ , on **QSD**<sub>N</sub>:  $1/2 + 1/\text{negl}$

Unless **QSZK** is in **QMA**, this algorithm fails infinitely often, i.e. there exists a set  $\Lambda$  of instances that are computationally indistinguishable.

# Bit Commitment from an Ensemble

**Protocol:** Both parties receive aux-input  $x = (C_0, C_1)$

1. **Commit:** Alice uses  $C_b$  to obtain the state  $|\psi_b\rangle$  and sends the portion in the space  $\mathcal{O}$  to Bob (who now holds  $\rho_b$ )
2. **Reveal:** Alice sends  $b$  and the remaining qubits (in space  $\mathcal{G}$ ) to Bob. Bob runs  $C_b$  in reverse and measures, accepting iff result is  $|0\rangle$

**Security (sketch, as before):**

**Hiding:** By assumption,  $\{\rho_{0,x}\}$  and  $\{\rho_{1,x}\}$  are computationally indistinguishable, so Bob cannot learn  $b$  early.

**Binding:** If Alice commits to a state  $\xi$ , then  $\|\rho_0 - \rho_1\|_{\text{tr}} \geq 2 - \varepsilon$  implies that no matter the state she sends in the reveal phase

$$\frac{1}{2} (\Pr[A \text{ reveals } 0] + \Pr[A \text{ reveals } 1]) \leq \frac{1}{2} + \frac{\sqrt{\varepsilon}}{2}$$

# Outline of Talk

- 1) Background: Bit Commitment and Quantum Complexity
- 2) Main Idea
- 3) **QSZK** vs **QMA** Protocol
- 4) **PSPACE** vs **QMA** Protocol

# If PSPACE is not in QMA ...

**Definition:** Two channels  $\Phi_0, \Phi_1$  are comp. distinguishable if there exists a state  $\sigma$  such that  $(\Phi_0 \otimes I)(\sigma), (\Phi_1 \otimes I)(\sigma)$  are comp. distinguishable, and computationally indistinguishable otherwise.

We define aux-input ensembles analogously to the state case.

**Lemma:** If QCD is not in QMA, there exist aux-input channel ensembles that are computationally indistinguishable on some infinite set  $\Lambda$ .

*Proof sketch:* analogous to the state case.

The assumption in this case is much weaker, but we will also require quantum advice to build a protocol (the state  $\sigma$ ).

# Bit Commitment from a Channel Ensemble

Both parties receive aux-input  $(\Phi_0, \Phi_1)$  as well as a quantum state  $\sigma$ . They are promised that:

$$2 - \varepsilon \geq \|\Phi_0 - \Phi_1\|_{\diamond} = \|(\Phi_0 \otimes I)(\sigma) - (\Phi_1 \otimes I)(\sigma)\|_{\text{tr}}$$

**Key fact:** we may assume that such  $\sigma$  exists and is pure [R., Watrous 05]

## Protocol:

1. **Commit:** Alice uses  $\Phi_b$  (and  $\sigma$ ) to obtain the state  $|\psi_b\rangle$  (before tracing out  $\mathcal{G}$ ) and sends the portion in the space  $\mathcal{O}$  to Bob.
2. **Reveal:** Alice sends  $b$  and the remaining qubits (in space  $\mathcal{G}$ ) to Bob. Bob runs  $\Phi_b$  in reverse (to hopefully get  $\sigma$ ). Bob then performs the swap test on this state and his copy of  $\sigma$  accepting iff result is same.

**Security:** Same as in case of states except swap test allows Alice to cheat with probability 1/2. We fix this by proving a parallel repetition result.

# Discussion

We have seen computationally-hiding statistically-binding protocols. Assuming **PSPACE** not in **QMA** we also find statistically-binding computationally-hiding protocols, using a different problem.

We use two complexity assumptions: **QSZK**  $\not\subseteq$  **QMA** and **PSPACE**  $\not\subseteq$  **QMA**

- ▶ The second assumption is reasonable (unless **PSPACE** = **PP**)
- ▶ The first assumption is very strong. In the full version we extend the techniques of [AK 07] to show a (quantum) oracle separation between **QSZK** and **QCMA**. A recent paper shows a stronger result: an oracle relative to which **SZK** is not in **QMA** [Aaronson 11]

Our security definition for bit commitment is quite weak (it is not composable). Can we construct better schemes from these assumptions?

Can we find similar non-interactive schemes for Oblivious Transfer?