Quantum computational indistinguishability and zero-knowledge

John Watrous

School of Compupter Science
and
Institute for Quantum Computing

University of Waterloo

October 2, 2006

Topic of talk

The notion of **indistinguishability** is important in the theory of cryptography.

This talk will focus on two instances that arise in the quantum setting:

- Indistinguishability of two or more **quantum states**.
- Indistinguishability of two or more **quantum operations**.

Two natural notions of indistinguishability:

- **Information-theoretic** indistinguishability.
- **Computational** indistinguishability.

The purpose of the talk will be to discuss important issues regarding these notions.

Principal motivation: **zero-knowledge**.

Information-theoretic indistinguishability of states

Suppose two mixed states are fixed in advance: ρ and ξ.

One of the two states is selected uniformly at random, and given to an adversary whose goal is: determine which states was selected.

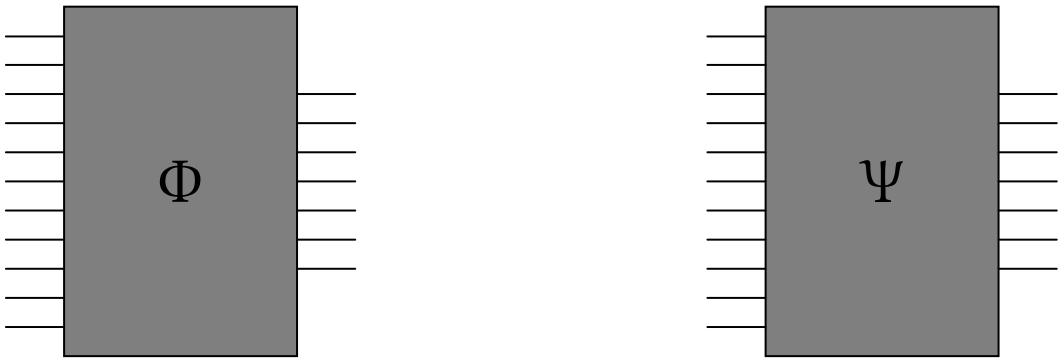
- There is a measurement that correctly identifies whether the state was ρ or ξ with probability

$$\frac{1}{2} + \frac{1}{4} \|\rho - \xi\|_{\mathsf{tr}} .$$

- This is optimal.

Distinguishing between operations

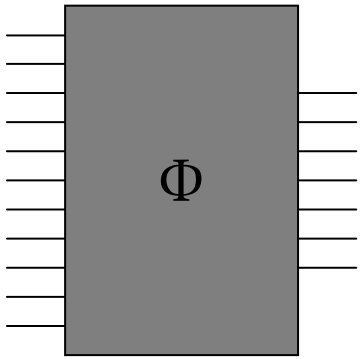
Consider a similar question for **operations** rather than states:



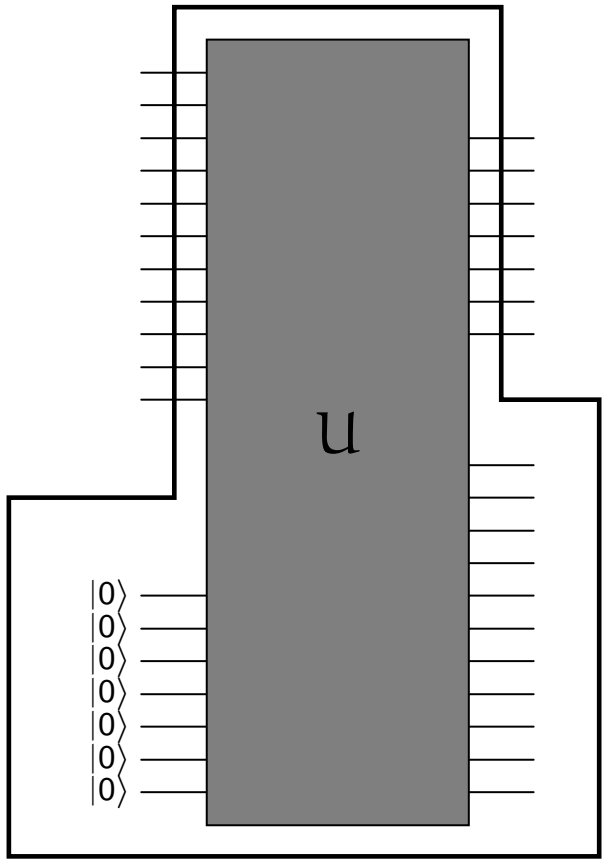
Assume that **only a single evaluation** of the given operation is permitted.

Distinguishing between operations

Note: it may not be the case that the operations are unitary. They might, for example, arise as follows:



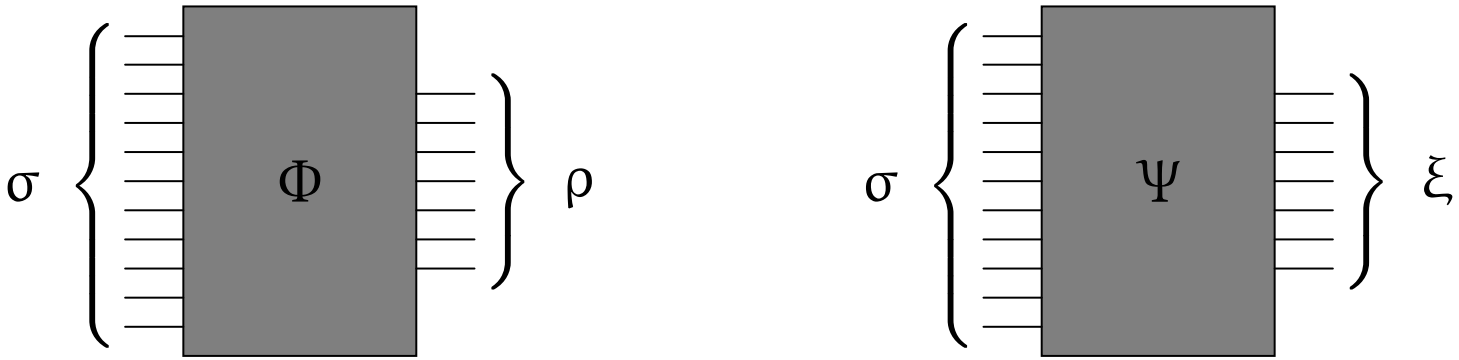
is given by



We are working with **general quantum operations** (also called admissible operations, CPSO's, etc.).

Distinguishing between operations

Given two such operations:



What is the best way to distinguish between them?

One possibility:

Try to optimally choose an input state σ so that the output states ρ and ξ have large trace distance.

Bad choice. . .

So close and yet so far...

Let Φ and Ψ be mappings from n qubits to n qubits defined as follows:

$$\Phi(X) = \frac{1}{2^n + 1}\left((\operatorname{tr} X)I + X^T\right), \; \Psi(X) = \frac{1}{2^n - 1}\left((\operatorname{tr} X)I - X^T\right).$$

These are both valid quantum operations.

- For every mixed state σ it holds that $\left\|\Phi(\sigma) - \Psi(\sigma)\right\|_{tr} \leqslant \frac{4}{2^n+1}$. The outcomes are **exponentially close** in trace distance.
- Take a maximally entangled state on $2n$ qubits

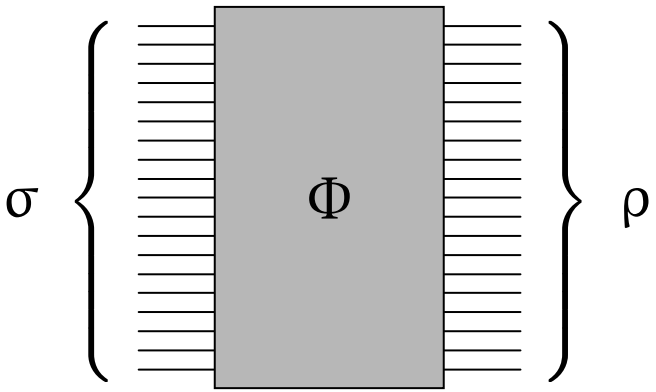
$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle\,|i\rangle\,.$$

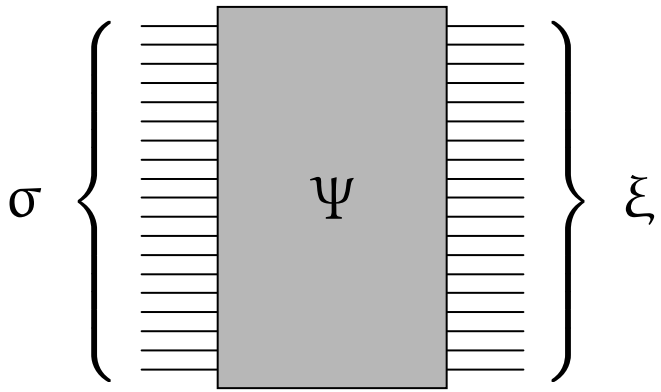
Then

$$\left\|(\Phi \otimes I)(|\psi\rangle\langle\psi|) - (\Psi \otimes I)(|\psi\rangle\langle\psi|)\right\|_{tr} = 2.$$

The two outcomes are **perfectly distinguishable**.

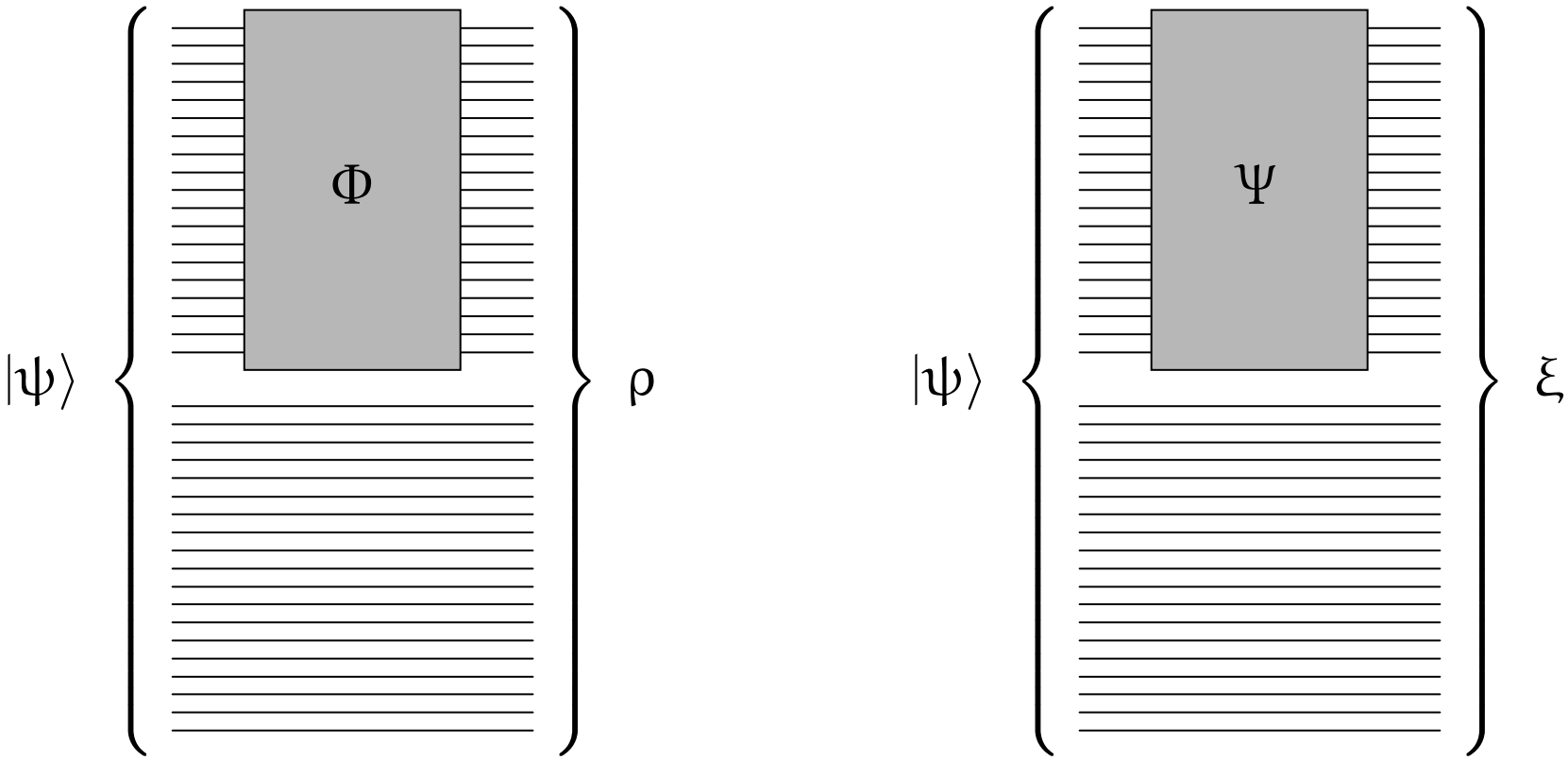
So close and yet so far…





$\rho \approx \xi$ (for any choice of σ)

So close and yet so far…



$\|\rho - \xi\|_{\mathsf{tr}} = 2$ (i.e., they are **perfectly** distinguishable)

Kitaev's "diamond" norm

There is a norm defined on super-operators that perfectly handles this situation: Kitaev's "diamond" norm.

Simplified definition:

$$\|\Phi - \Psi\|_\diamond = \max_\sigma \|(\Phi \otimes \mathrm{I})(\sigma) - (\Psi \otimes \mathrm{I})(\sigma)\|_{\mathsf{tr}} .$$

The **optimal probability** of correctly identifying which of the two operations Φ and Ψ was given, allowing for a single evaluation on a state of arbitrary size, is

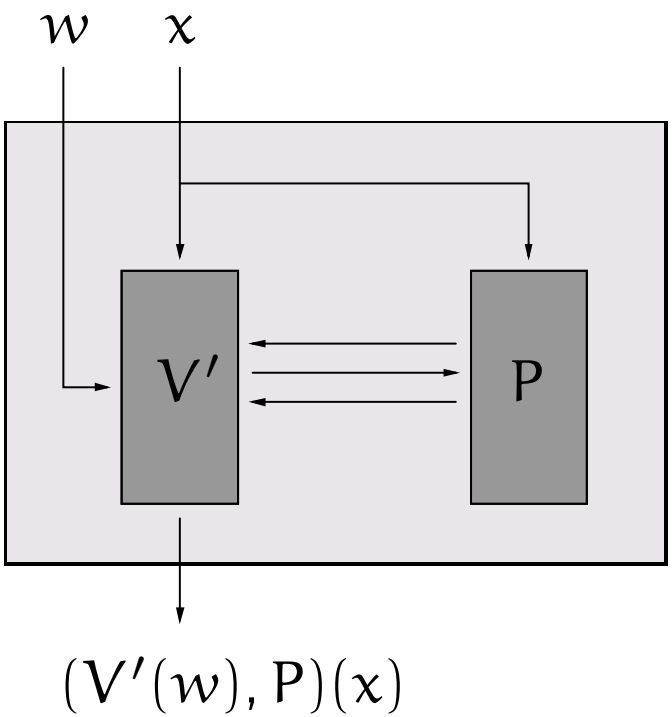
$$\Pr[\text{correct identification}] = \frac{1}{2} + \frac{1}{4}\|\Phi - \Psi\|_\diamond .$$

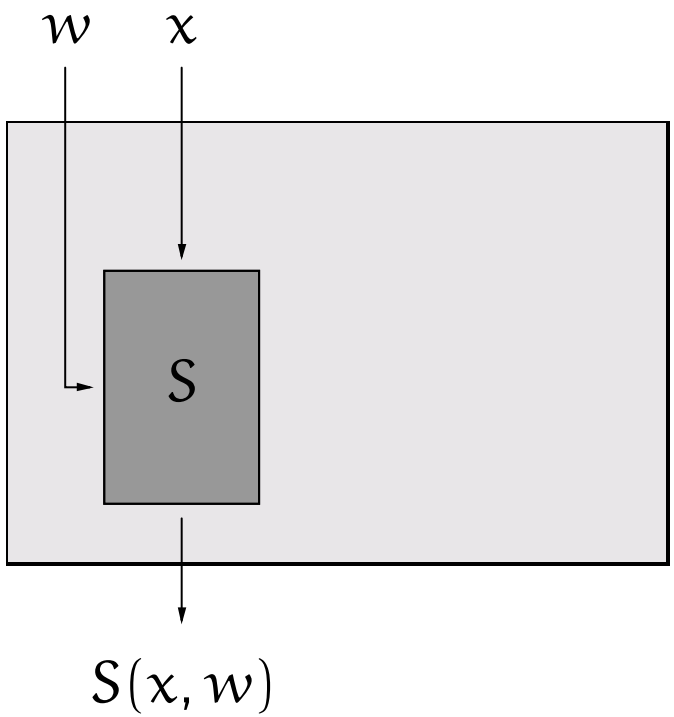
Note: the existence of the external space gives the diamond norm nice properties and makes it well-suited for various applications.

Classical zero-knowledge

Suppose (V, P) is an interactive proof system for some problem A.

Then (V, P) is (classical) **zero-knowledge** if, for every poly-time V' there exists a poly-time simulator S so that these two processes are indistinguishable when $x \in A$:

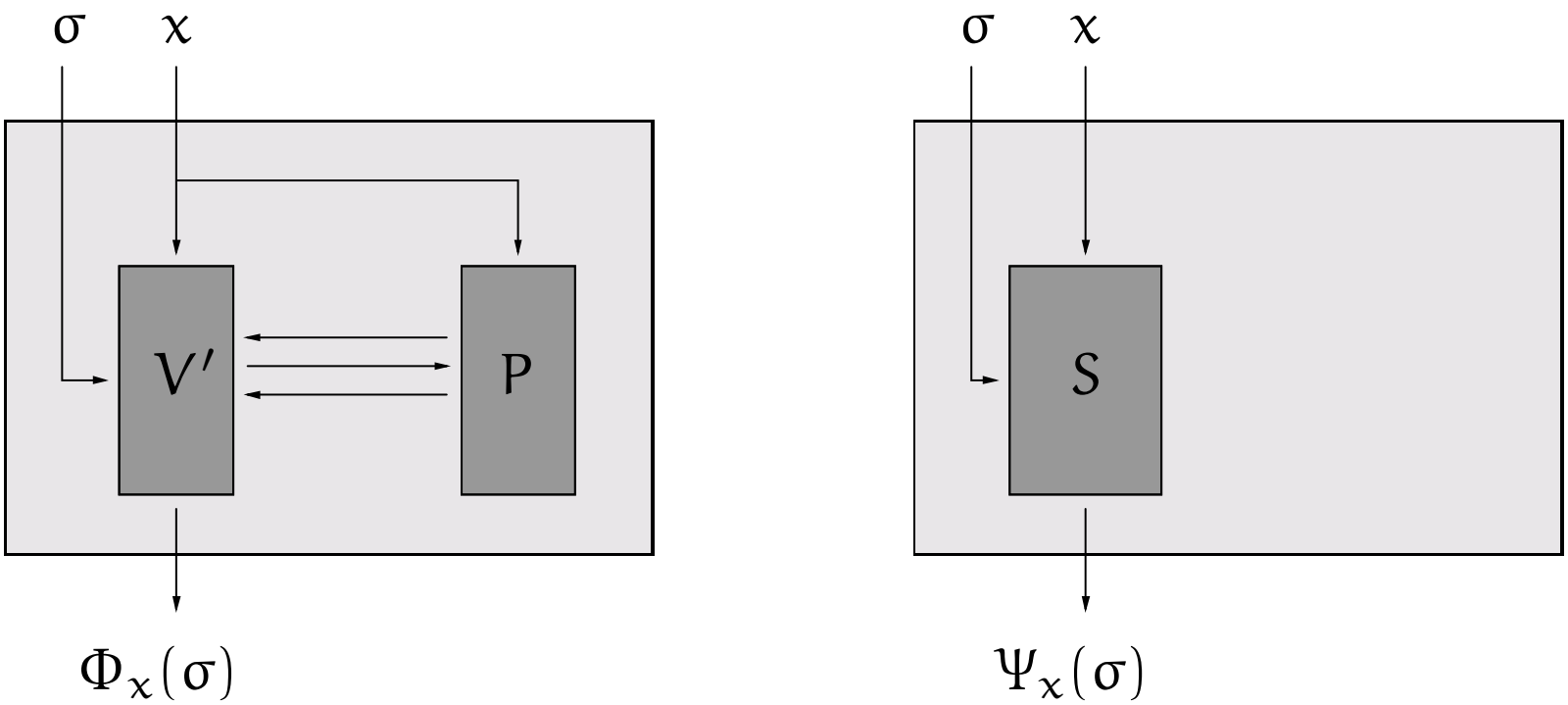




The input w represents the **auxiliary input**.

Quantum statistical zero-knowledge

We have a similar picture where the cheating verifier V' may be **quantum**:



We say that (V, P) is **quantum <u>statistical</u> zero-knowledge** if, for every poly-time V', there exists a poly-time S, such that

$$\| \Phi_x - \Psi_x \|_\diamond$$

is negligible whenever $x \in A$.

Comments on this definition

- Captures the following notion: if you have a quantum computer, you cannot **increase** your knowledge by interacting with a quantum statistical zero-knowledge prover a polynomial number of times.
- The resulting class of proof systems have good closure properties: closure under **sequential composition** and **Karp reductions**.
- **Opinion:** this is the “correct” quantum analogue to the standard classical definition of statistical zero-knowledge from an **operational** viewpoint. . .

  . . . removing the auxiliary quantum input or changing the norm, for instance, represents a compromise or one sort or another.

Quantum statistical zero-knowledge protocols

Some interactive proof systems can be proved to be zero-knowledge with respect to the previous definition:

1. The Goldreich-Micali-Wigderson Graph Isomorphism protocol.
2. A few other protocols with a similar form: prover sends a message, verifier flips a single coin, prover responds with a second message.
3. A universal protocol for $\mathrm{QSZK}_{\mathrm{HV}}$.

The construction of simulators for cheating verifiers substitutes an *Amplification Lemma* for the usual notion of "rewinding" [W., 2006].

Computational indistinguishability of states

We have already considered the optimal probability with which two states can be distinguished by **unrestricted** measurements.

Now let us consider the case where the measurements are **computationally** restricted.

Let us restate the problem in a way that makes sense for computational restrictions:

Given two sets of states:

$$\{\rho_n : n \in \mathbb{N}\} \quad \text{and} \quad \{\xi_n : n \in \mathbb{N}\}.$$

The states ρ_n and ξ_n are n-qubit states for each n.

What does it mean for the two sets to be **quantum computationally indistinguishable**?

Example: bit commitment

For example, the two sets $\{\rho_n : n \in \mathbb{N}\}$ and $\{\xi_n : n \in \mathbb{N}\}$ might represent Bob's view of Alice's commitment to a bit...

In other words, let n be a security parameter, and consider the situation that Alice commits to a bit b using some **unconditionally binding** and **computationally concealing** commitment scheme.

After the commitment phase:

$$b = 0 \quad \Rightarrow \text{ Bob's state is } \rho_n.$$
$$b = 1 \quad \Rightarrow \text{ Bob's state is } \xi_n.$$

GMW 3-coloring protocol

The GRAPH 3-COLORING Problem is to determine whether or not a given n-vertex undirected graph G has a valid coloring with 3 colors.

The Goldreich-Micali-Wigderson protocol for Graph 3-Coloring relies on computationally concealing bit commitments. . . it is as follows:

Prover: Let $\phi : \{1, \ldots, n\} \to \{1, 2, 3\}$ be a valid coloring of G if one exists, and uniformly choose $\pi \in S_3$. Send the verifier commitments to the colors $\pi(\phi(1)), \ldots, \pi(\phi(n))$.

Verifier: Choose an edge $\{i, j\}$ of G uniformly at random.

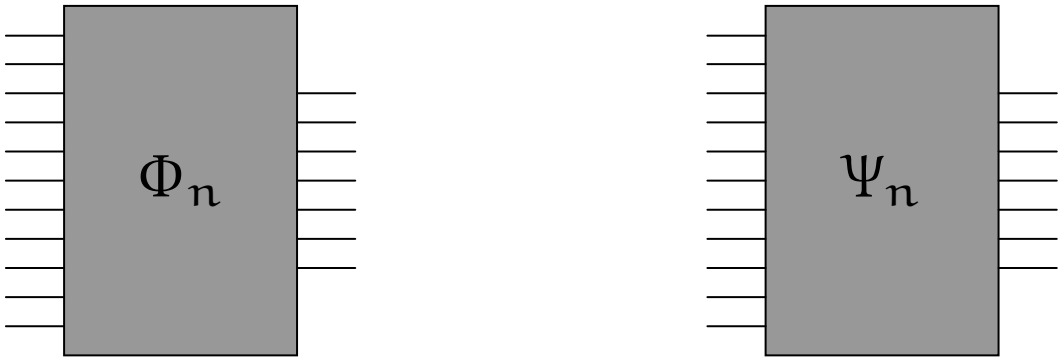
Prover: Reveal the colors $a_i = \pi(\phi(i))$ and $a_j = \pi(\phi(j))$.

Verifier: If $a_i \neq a_j$ then accept, else reject.

Sequential repetition followed by unanimous vote gives exponentially small soundness error.

Computational distinguishability of operations

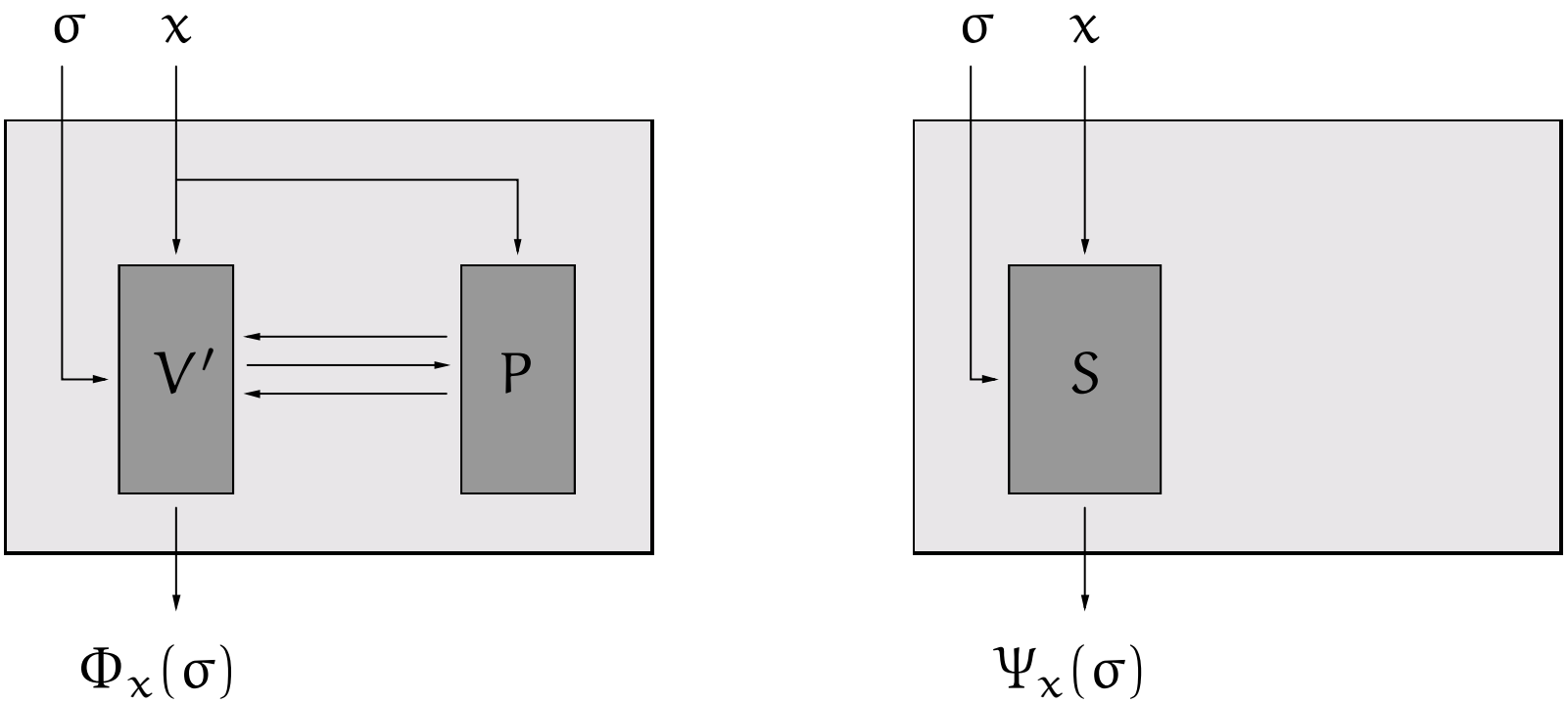
Similar to before, we may also consider what it means for two **operations** to be **quantum computationally indistinguishable**:



Again, only a single evaluation (possibly on just a part of a larger system) of the given operation is permitted.

Quantum computational zero-knowledge

A protocol (V, P) for problem A is quantum computational zero-knowledge if these two processes are **computationally** indistinguishable for $x \in A$:



They should be quantum computationally indistinguishable **for every choice of the auxiliary input state**.

Non-uniformity in the classical definition

Classically, the definition of computational indistinguishability that is used in the context of zero-knowledge is a **non-uniform** one...

We would say that two collections of probability distributions

$$\{u_n : n \in \mathbb{N}\} \quad \text{and} \quad \{v_n : n \in \mathbb{N}\}$$

are computationally indistinguishable if every family $\{C_n\}$ of polynomial-size circuits fails to distinguish u_n and v_n with non-negligible probability.

Similar definition for processes...

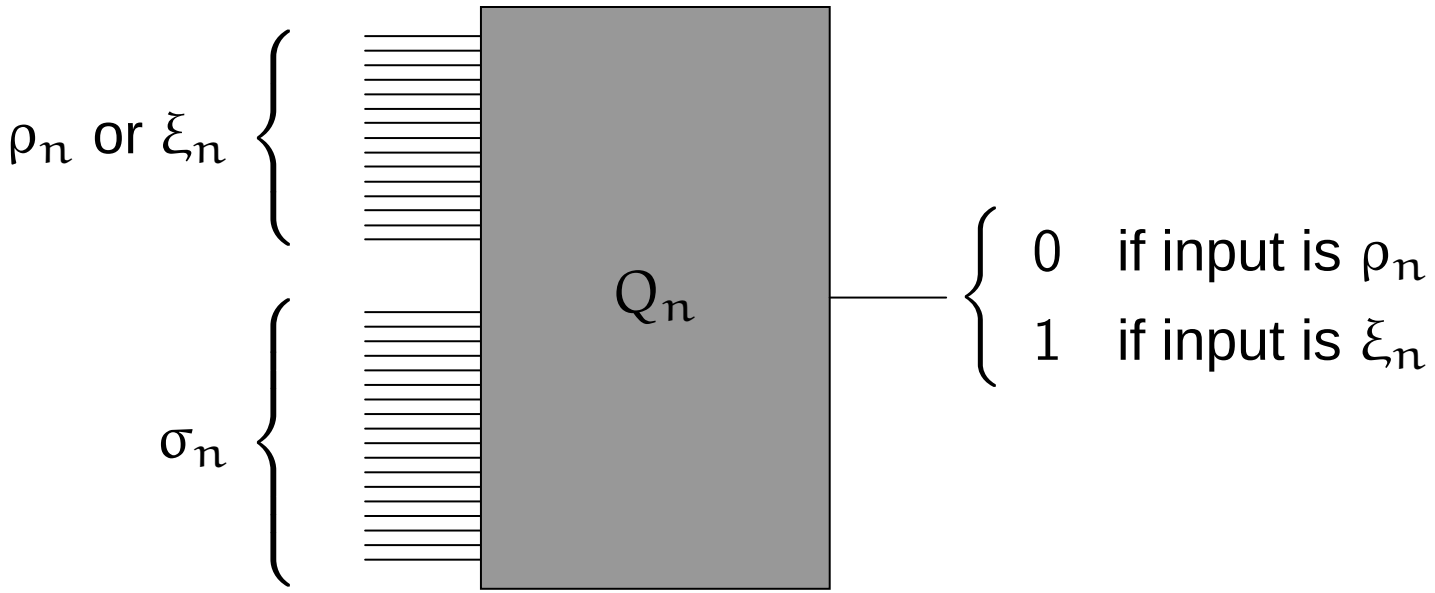
This notion of indistinguishability is perfect for classical zero-knowledge, because it translates to making no assumptions on the auxiliary input...

...we can view that the optimal input for distinguishing two classical processes can be hard-coded into a given poly-size circuit.

Quantum case: a stronger notion of non-uniformity

We need a stronger notion of non-uniformity in the quantum case. . . we must allow quantum circuits to take an **arbitrary quantum input**.

Definition: The sets $\{\rho_n\}$ and $\{\xi_n\}$ are quantum computationally indistinguishable if for every poly-size family $\{Q_n\}$ and every set $\{\sigma_n\}$ of states fails to distinguish ρ_n and ξ_n with non-negligible bias:



Similar definition for operations. . .

Application to 3-Coloring

Suppose that we have a **bit commitment** protocol that is unconditionally binding and quantum computationally concealing with respect to the strong non-uniform definition.

Then the Goldreich-Micali-Wigderson 3-Coloring protocol is **quantum computational zero-knowledge**.

- Proof is based on the same Amplification Lemma that is used in the statistical zero-knowledge protocols mentioned before.
- It is doubtful that bit commitment protocols with weaker notions of the quantum computational concealing property could be used instead (without different proof methods).

Conclusion

Suggestion:

Whenever possible, allow for auxiliary quantum inputs in definitions of quantum cryptographic primitives.

Direction for further work:

Find good candidates for quantum one-way functions, and the connection to bit commitment.

Wish-list:

1. Honest players should **not** require quantum computers.
2. Security should hold against poly-size quantum adversaries with **arbitrary auxiliary quantum inputs**.