On Quantum Indifferentiability

Tore Vincent Carstens , Ehsan Ebrahimi, Gelo Noel Tabia, and Dominique Unruh

University of Tartu, Estonia

March 8, 2018

Abstract

We study the indifferentiability of classical constructions in the quantum setting, such as the Sponge construction or Feistel networks. (But the approach easily generalizes to other constructions, too.) We give evidence that, while those constructions are known to be indifferentiable in the classical setting, they are not indifferentiable in the quantum setting. Our approach is based on an quantum-information-theoreoretical conjecture.

1 Introduction

Indifferentiability [MRH04] is a security notion that allows us to compare the implementation of a cryptosystem (called a "construction" in the following) to an ideal representation. For example, the indifferentiability framework allows us to say that a certain hash function is indifferentiable from a random oracle. This means that we can use this hash function in any setting in which a random oracle can be used, without loss of security.[1] In particular, showing indifferentiability of a specific construction immediately implies a number of other security properties. (For example, if a hash function is indifferentiable from a random oracle, we immediately get that it is one-way, collision-resistant, a pseudo-random-function, etc.) Indifferentiability is most often applied in settings where a larger primitive (say a hash function) is constructed from a smaller idealized primitive (say a random oracle with short input/output as a block function).

Many classical constructions have been revisited based on the indifferentiability framework. To name a few, the Luby-Rackoff construction (Feistel network) [LR88] that constructs a pseudo-random permutation from pseudo-random functions has been studied based on the indifferentiability framework in multiple research works [CHK+16, DKT16, DS16]. In [CDMP05], they revisited the Merkle-Damgård construction based on indifferentiability framework. They show that the plain Merkle-Damgård construction is differentiable from a random oracle, however, they modify the MD construction to successfully obtain a positive result. The indifferentiability of the Sponge construction, that is used in the SHA-3 hash function [NIS14], has been shown in [BDPA08].

It is worth mentioning that at least in the case of SHA-3/the Sponge construction, all security properties were derived from its indifferentiability. For example, we are not aware of any proof of the collision-resistance of the Sponge construction that does not rely on first showing indifferentiability.[2]

[1] Within limitations. There are certain settings in which indifferentiability is not enough for this purpose. See [RSS11]. In most settings, however, a construction that is indifferentiable from a random oracle is as good as a random oracle.

[2] [CBH+17] shows the (quantum) collision-resistance of the Sponge construction in the case where the underlying block function is a random function, but this does not apply to SHA-3 which uses an invertible random permutation instead.

However, all of these results are in the classical setting. To the best of our knowledge, no results are known in the quantum setting. Especially in the case of the Sponge construction, this is quite problematic since no direct proofs of the security properties of the Sponge construction are known (in the case of a random permutation as block function). That means, we do not even know whether SHA-3 is post-quantum secure.

In this paper, we give some evidence why there is a lack of proofs of quantum indifferentiability. Precisely, we show that under a certain quantum-information-theoreoretical assumption, perfectly secure quantum indifferentiability is impossible in a wide variety of cases (including the Sponge construction and Feistel networks). This holds even in the weaker setting where the construction is accessed classically, and the adversary merely has superposition access to the underlying primitive (e.g., the random oracle).

While our proofs are, at this point, still conditional on a conjecture, and limited to the case of perfect indifferentiability, we conjecture that the indifferentiability will not hold generally. And even if not, our results indicate that (and why!) it would be very difficult to build a quantum indifferentiable construction, or to prove the post-quantum security of existing cryptosystems such as SHA-3 using the indifferentiability framework.

Organization. In Section 2, we revisit the indifferentiability framework, introduce the quantum indifferentiability framework (to the best of our knowledge, it has not been defined before), and introduce our conjectures and theorems (with informal arguments why we believe in them). In Section 4 we show our main (conditional) impossibility result. And in Section 5, we show how our general result is applied concretely to the Sponge construction and Feistel networks (via a simple counting argument).

2 Indifferentiability

Classical indifferentiability. We first revisit the classical indifferentiability framework [MRH04]. The purpose of that framework is to compare constructions $\mathcal{T}_1$ with idealized counterparts $\mathcal{T}_2$. In [MRH04], constructions can be arbitrary interacting systems. For the purpose of this paper, it will be easiest to consider a special case, namely where constructions are (stateful) oracles.[3] We then say that $\mathcal{T}_1$ is quantum indifferentiable from $\mathcal{T}_2$ iff – roughly – any attack that is possible on $\mathcal{T}_1$ is also possible on $\mathcal{T}_2$. This then implies that, if $\mathcal{T}_2$ is ideal and thus without relevant attacks by assumptions, also $\mathcal{T}_1$ is without relevant attacks.

To make this more formal, we need to first introduce two types of "interfaces" to a construction, the private and the public interface. In our view (where constructions are oracles), these simply represent two types of queries, and we write $\mathcal{T}_1^{priv}$ for $\mathcal{T}_1$ restricted to its private interface (i.e., ignoring all queries that are not of the private type), and $\mathcal{T}_1^{pub}$ for $\mathcal{T}_1$ restricted to its public interface. The idea behind private and public interfaces is that private interfaces model the access the user of a construction has (e.g., input/output via an API), while the public interface represents what access an adversary has (e.g., network communication, or, in our case, publicly available random oracles).

Then, to the intuitive requirement that all attacks on $\mathcal{T}_1$ are also possible on $\mathcal{T}_2$, we require that there is a simulator that mimics whatever happens in an attack on $\mathcal{T}_1$. Here the simulator is allows to access and modify interaction over the public interface, but not over the private interface. This leads to the following definitions:

[3] That is, whenever a construction is queried with some value x, it returns some value y to the invoking party and possibly updates its internal state.

Definition 1 (Classical indifferentiability) *$\mathcal{T}_1$ is classically indifferentiable from $\mathcal{T}_2$ iff for any polynomial-time distinguisher $\mathcal{D}$, there exists a polynomial-time simulator Sim such that*

$$|\Pr[\mathcal{D}(\mathcal{T}_1^{priv}, \mathcal{T}_1^{pub}) = 1] - \Pr[\mathcal{D}(\mathcal{T}_2^{priv}, \mathsf{Sim}(\mathcal{T}_2^{pub})) = 1]|$$

is negligible.

Here $\mathcal{D}(\mathcal{T}_1^{priv}, \mathcal{T}_1^{pub})$ means an invocation of $\mathcal{D}$ with oracle access to $\mathcal{T}_1^{priv}$ and $\mathcal{T}_1^{pub}$. (Note: $\mathcal{T}_1^{priv}$ and $\mathcal{T}_1^{pub}$ are restrictions of the same $\mathcal{T}_1$, thus they share the same internal state.) Similarly, $\mathsf{Sim}(\mathcal{T}_2^{pub})$ is the simulator Sim with oracle access to $\mathcal{T}_2^{pub}$. (And $\mathsf{Sim}()$ is itself used as an oracle for $\mathcal{D}$.)

Indifferentiability has the useful property that most security properties carry over from $\mathcal{T}_2$ to $\mathcal{T}_1$. For example, if $\mathcal{T}_2$ is a random function, then we know that $\mathcal{T}_2$ is collision-resistant. Then, if $\mathcal{T}_1$ is indifferentiable from $\mathcal{T}_2$, we know that $\mathcal{T}_2$ is collision-resistant as well. (This is, for example, how collision-resistance of the Sponge construction is proven in [BDPA08]: first the indifferentiability of the Sponge construction is shown, and collision-resistance and many other properties follow for free.)

One of the most common use cases for the indifferentiability framework is when the constructions are stateless deterministic functions. For example, in the indifferentiabiltiy result for the Sponge construction [BDPA08], we have: $f : \{0,1\}^{r+c} \to \{0,1\}^{r+c}$ is a random permutation. $\mathcal{T}_1 : \{0,1\}^* \to \{0,1\}^*$ is the Sponge construction itself, that is, when queried with m over the private interface, it computes the hash of m using the Sponge construction based on the block function f (which is given as an oracle), and returns the hash. When queried on the public interface, $\mathcal{T}_1$ forwards its query to f. (This models the fact that the block function is publicly known.) $\mathcal{T}_2 : \{0,1\}^* \to \{0,1\}^*$ is a uniformly random function (the same function both on the private and public interface). [BDPA08] then shows that $\mathcal{T}_1$ is indifferentiable from $\mathcal{T}_2$. In other words, the Sponge construction behaves like a random oracle if the round function f is a random permutation.

Throughout this paper, we will only consider settings of this structure. That is, we always assume:

Conditions 1.

- f represents some random function. We call f the *primitive*. (That is, f is chosen according to some distribution, but after that initial sampling, f is stateless and deterministic. Typically, f is a uniformly random function, uniformly random permutation, or ideal cipher.)
- $\mathcal{T}_1$ depends deterministically on f. Namely, the interface $\mathcal{T}_1^{priv}$ implements some function $\mathcal{C}[f]$ that depends only on f. (Typically, $\mathcal{C}[f]$ can be implemented efficiently given oracle access to f but we do not require this. $\mathcal{C}[f]$ is the actual construction that we analyse, e.g., the Sponge construction.) The interface $\mathcal{T}_1^{pub}$ implements f itself.
- $\mathcal{T}_2$ is a random function. (In the same sense as f but typically with a different distribution.) That is, both $\mathcal{T}_2^{priv}$ and $\mathcal{T}_2^{pub}$ give access to the same random function. ($\mathcal{T}_2$ might be, e.g., a uniformly random function when we are trying to implement a random oracle. Or it might be, e.g., an ideal cipher.)

Quantum indifferentiability. It is immediate how to translate the indifferentiability framework to the quantum case. Instead of saying that constructions are classical oracles, they are quantum oracles. (Formally, quantum oracles are superoperators with an input and a state register as input, and an output and a state register as output. For stateless oracles, the state register is not used.) Then, the definition is almost verbatim the same:

Definition 2 (Quantum indifferentiability) *$\mathcal{T}_1$ is quantum indifferentiable from $\mathcal{T}_2$ iff for any quantum-polynomial-time distinguisher $\mathcal{D}$, there exists a quantum-polynomial-time simulator* Sim *such that*

$$|\Pr[\mathcal{D}(\mathcal{T}_1^{priv}, \mathcal{T}_1^{pub}) = 1] - \Pr[\mathcal{D}(\mathcal{T}_2^{priv}, \mathsf{Sim}(\mathcal{T}_2^{pub})) = 1]| \tag{1}$$

is negligible.

We say $\mathcal{T}_1$ is perfectly quantum indifferentiable from $\mathcal{T}_2$ if that difference is 0.

However, more interesting is the question what oracles the constructions $\mathcal{T}_1$ and $\mathcal{T}_2$ implement. As before, we will look at the most common case where $\mathcal{T}_1$ and $\mathcal{T}_2$ are deterministic and stateless, and $\mathcal{T}_1$ is based on some primitive f, as in Conditions 1. But there are two possibilities how to implement a function as a quantum oracle: We can allow classical queries, or superposition access.[4] So, for each of the oracles in Conditions 1, we need to decide whether they can be queried classically or in superposition. First, consider the primitive f. Since f represents a globally known function (e.g., the block function of a hash function construction modeled as a random oracle), we have to model the fact that an adversary can evaluate that function in superposition. (See [BDF+11] for additional discussion on why random oracles should be modeled with superposition queries.) That is, the interface $\mathcal{T}_1^{pub}$ should be f with superposition access. How about $\mathcal{T}_1^{priv} = \mathcal{C}[f]$? This is what the user accesses, i.e., queries to $\mathcal{T}_1^{priv} = \mathcal{C}[f]$ are the queries that would be performed by protocols that use $\mathcal{C}[f]$ (e.g., some protocol that uses the Sponge construction to implement a MAC). So, if we allow superposition queries here, indifferentiability will imply that $\mathcal{T}_1$ is as secure as the ideal construction $\mathcal{T}_2$ even when used in protocols that evaluate $\mathcal{C}[f]$ in superposition. If we allow only classical queries here, we get the weaker result that indifferentiability will imply that $\mathcal{T}_1$ is as secure as the ideal construction $\mathcal{T}_2$ only when used in protocols that evaluate $\mathcal{C}[f]$ classically. It depends on the intended use case which is preferred. Since we will give evidence that indifferentiability is not achievable in many cases, we will use the weaker variable (with classical queries) as this yields a stronger claim. Summarizing, we will assume the following throughout this paper:

Conditions 2.

- f represents some random function. We call f the *primitive*.
- The interface $\mathcal{T}_1^{priv}$ answers classical queries to some function $\mathcal{C}[f]$ that depends only on f. The interface $\mathcal{T}_1^{pub}$ answers superposition queries to f.
- $\mathcal{T}_2$ implements a random function H. That is, $\mathcal{T}_2^{priv}$ answers classical queries to H, and $\mathcal{T}_2^{pub}$ answers superposition queries to H.[5]

Then, if we say, e.g., the Sponge construction implements a random oracle, we mean that f is a uniformly random permutation, $\mathcal{C}[f]$ is the sponge construction, and H is a uniformly random function.

In the following, for added clarity, we will always write an overline over constructions that are classical oracles, and no overline over constructions that allow superposition access. E.g., (1) would be

$$|\Pr[\mathcal{D}(\overline{\mathcal{T}_1^{priv}}, \mathcal{T}_1^{pub}) = 1] - \Pr[\mathcal{D}(\overline{\mathcal{T}_2^{priv}}, \mathsf{Sim}(\mathcal{T}_2^{pub})) = 1]|.$$

[4] An oracle implementing f with classical queries will measure its input register in the computational basis, resulting in a value x, and then prepare its output register in the state $|f(x)\rangle$. An oracle implementing f with superposition queries will apply the unitary U_f to a pair of registers, where U_f is defined by $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$.

[5] Why does $\mathcal{T}_2^{pub}$ answer superposition queries? This is another design choice but if $\mathcal{T}_2^{pub}$ would answer only classical queries, we would get a trivial impossibility even for simple cases like "f is indifferentiable from f" because the simulator would only get classical access but has to use it to answer superposition queries.

3 On the impossibility of quantum indifferentiability

In the previous section, we described the notion quantum indifferentiability. We will now explain why quantum indifferentiability is probably impossible to achieve in many situations.

To explain this, assume $\mathcal{T}_1$ is quantum indifferentiable from $\mathcal{T}_2$. That means, for any distinguisher $\mathcal{D}$, there is a simulator Sim such that:

$$\Pr[\mathcal{D}(\overline{\mathcal{T}_1^{priv}}, \mathcal{T}_1^{pub}) = 1] \approx \Pr[\mathcal{D}(\overline{\mathcal{T}_2^{priv}}, \mathsf{Sim}(\mathcal{T}_2^{pub})) = 1]. \tag{2}$$

($\approx$ means negligible distance here.) Since $\mathcal{T}_1^{pub}$ is an oracle with superposition access, $\mathsf{Sim}(\mathcal{T}_2^{pub})$ must be an oracle with superposition access, too. Now consider any query the distinguisher $\mathcal{D}$ makes. That query can be a superposition between different queries, and $\mathcal{T}_1^{pub}$ will respond to that query in superposition. In particular, $\mathcal{T}_1^{pub}$ will not collapse the superposition by entangling it with its internal state (since $\mathcal{T}_1^{pub}$ is stateless). Since such a collapse of the superposition could be detected by $\mathcal{D}$, $\mathsf{Sim}(\mathcal{T}_2^{pub})$ also must not collapse the superposition. Thus $\mathsf{Sim}(\mathcal{T}_2^{pub})$ must not entangle the query register with its internal state. But that means that $\mathsf{Sim}(\mathcal{T}_2^{pub})$ cannot keep any information about the query (because that would entangle it with the query input if the query is a superposition between different inputs). So, $\mathsf{Sim}(\mathcal{T}_2^{pub})$ will have a state that is independent of the queries. That means that for any distinguisher, there is a *stateless* simulator $\mathsf{Sim}(\mathcal{T}_2^{pub})$ that satisfies (2).

Now consider a classical distinguisher $\mathcal{D}$, i.e., $\mathcal{D}$ makes only classical queries. Then we can take the stateless simulator $\mathsf{Sim}(\mathcal{T}_2^{pub})$ and make it classical in the sense that $\mathsf{Sim}(\mathcal{T}_2^{pub})$ now measures all queries before answering. Since $\mathcal{D}$ is classical, $\mathcal{D}$ cannot tell the difference, and (2) still holds. A stateless simulator $\mathsf{Sim}(\mathcal{T}_2^{pub})$ that measures all its queries before answering is just a classical oracle, thus $\mathsf{Sim}(\mathcal{T}_2^{pub})$ can be replaced by a classical stateless simulator $\mathsf{Sim}'(\mathcal{T}_2^{pub})$. (This classical simulator will not necessarily be efficient since it has to simulate a quantum algorithm. But if we do not require $\mathsf{Sim}'(\mathcal{T}_2^{pub})$ to be efficient, then $\mathsf{Sim}'(\mathcal{T}_2^{pub})$ can simply learn the function H by performing exponentially many queries to $\mathcal{T}_2^{pub}$, and then $\mathsf{Sim}'(\mathcal{T}_2^{pub})$ has a complete description of $\mathsf{Sim}(\mathcal{T}_2^{pub})$ which allows $\mathsf{Sim}'(\mathcal{T}_2^{pub})$ to perform a simulation in exponential time.)

Summarizing, this argument indicates that the following conjecture holds:

Conjecture 1 *If $\mathcal{T}_1$ is quantum indifferentiable from $\mathcal{T}_2$, then $\mathcal{T}_1$ is classically indifferentiable from $\mathcal{T}_2$ with respect to stateless simulators in the following sense:*

For any classical polynomial-time distinguisher $\mathcal{D}$, there is a classical (not necessarily polynomial-time!) stateless simulator Sim such that

$$\left|\Pr[\mathcal{D}(\overline{\mathcal{T}_1^{priv}}, \overline{T_1^{pub}}) = 1] - \Pr[\mathcal{D}(\overline{\mathcal{T}_2^{priv}}, \overline{\mathsf{Sim}}(\overline{\mathcal{T}_2^{pub}})) = 1]\right|$$

is negligible.

Why is this conjecture important? Because it is in many cases quite simple to show the impossibility of classical indifferentiability with respect to stateless simulators. Namely, assume some construction $\mathcal{T}_1 = \mathcal{C}[f]$ such that f is picked from a set $\mathbf{F}$ of functions while $\mathcal{C}[f]$ (and thus also H) is chosen from some other set $\mathbf{H}$ of functions. (E.g., in the case of the Sponge construction, $\mathbf{F}$ is the set of functions $\{0,1\}^{r+c} \to \{0,1\}^{r+c}$ where r, c are two security parameters of the Sponge, and $\mathbf{H}$ is the set of all functions $\{0,1\}^* \to \{0,1\}^*$.) Assume further that $|\mathbf{F}| \ll |\mathbf{H}|$. (This is clearly the case for the Sponge construction.)

Assume that $\mathcal{T}_1$ is classically indifferentiable from $\mathcal{T}_2$ with respect to classical stateless simulators. Consider a distinguisher $\mathcal{D}$ that simply queries $\mathcal{T}_1^{priv}$ at a random input x. This will return

$y = \mathcal{C}[f](x)$. Then the distinguisher performs a number of additional queries to $T_1^{priv} = f$ to compute $\mathcal{C}[f](x)$. If this yields the same value y, the distinguisher $\mathcal{D}$ outputs 1. In the real case (i.e., interacting with $\mathcal{T}_1^{priv}$ and $\mathcal{T}_1^{pub}$), the distinguisher always outputs 1. Now consider the stateless simulator Sim. Since Sim is stateless, Sim will implement some function $f' \in \mathbf{F}$. (That is determined after choosing the initial randomness of Sim.) Thus, when interacting with $\mathcal{T}_2^{priv} = H$ and $\mathsf{Sim}(\mathcal{T}_2^{pub}) = f'$, the distinguisher $\mathcal{D}$ outputs 1 only if $H(x) = \mathcal{C}[f'](x)$. But $\mathcal{D}$ has to output 1 with overwhelming probability, so $H(x)$ and $\mathcal{C}[f']$ must be equal almost everywhere. But if $|\mathbf{F}| \ll |\mathbf{H}|$, then there are not enough functions f' so that $\mathcal{C}[f']$ can cover (up to a negligible number of errors) most of $\mathbf{H}$. Thus, for many choices of $\mathbf{H}$, the simulator will be caught by $\mathcal{D}$. That means, there is no successful simulator for $\mathcal{D}$. Hence $\mathcal{T}_1$ is not classically indifferentiable from $\mathcal{T}_2$ with respect to classical stateless simulators, and hence, by Conjecture 1, $\mathcal{T}_1$ is not quantumly indifferentiable from $\mathcal{T}_2$.

Notice that this argument was independent of how $\mathcal{C}[]$ was actually defined, so it means that there is no $\mathcal{C}[]$ such that $\mathcal{T}_1$ is quantum indifferentiable from T_2. In the case of the Sponge construction, not only does it show (conditional on Conjecture 1) that there the Sponge construction itself is not indifferentiable from a random oracle, but that there is no other hash function construction that is indifferentiable from a random oracle, either (assuming a small block function).

Of course, this was only a sketch illustrating the reasoning. In Section 5, we make this reasoning precise for the Sponge construction and Feistel networks.

Unfortunately, while we believe that Conjecture 1 is very realistic given the argument we gave before Conjecture 1, we were not able to prove this.

Instead, we present progress towards the goal of proving Conjecture 1: First, we show it only for perfect indifferentiability. And second, our proof is still based on a (more elementary) quantum-information-theoretical conjecture. Specifically, we show:

Theorem 1 *Assume that Conjecture 2 holds.*

If $\mathcal{T}_1$ is perfectly quantum indifferentiable from $\mathcal{T}_2$, then $\mathcal{T}_1$ is classically indifferentiable from $\mathcal{T}_2$ with respect to stateless simulators (in the sense of Conjecture 1).

And we use the following conjecture in this theorem:

Conjecture 2 *Consider N binary measurements described by projectors $P_1, \ldots, P_N$, and a quantum state $|\Psi\rangle$.*

Assume that any t out of the N measurements commute on state $|\Psi\rangle$. That is, for any I with $|I| = t$, if $P'_1, \ldots, P'_t$ and $P''_1, \ldots, P''_t$ are the projectors $\{P_i\}_{i\in I}$ (possibly in different order), then $P'_t \ldots P'_1|\Psi\rangle = P''_t \ldots P''_1|\Psi\rangle$.

Then there exist random variables $X_1, \ldots, X_N$ with a distribution D such that for any $I = \{i_1, \ldots, i_t\}$, the joint distribution of the $X_{i_1}, \ldots, X_{i_t}$ is the distribution of the outcomes when we measure $|\Psi\rangle$ with measurements $P_{i_1}, \ldots, P_{i_t}$.

What does this conjecture mean, and why do we believe it? It says that whenever we have a state where any t of out of a set of N measurements commute, then there is a joint classical distribution that explains any t of those N measurements (a hidden variable theory).

In fact, a small variation of this conjecture is easy to prove: If we require that $P'_t \ldots P'_1|\Psi\rangle = P''_t \ldots P''_1|\Psi\rangle$ for all $|\Psi\rangle$ (not just one fixed $|\Psi\rangle$), then we know that the P_i commute pairwise and thus jointly diagonalize. And then the joint distribution trivially exists.[6]

[6]Namely, the N-tuple $(x_1, \ldots, x_N)$ has probability $\|P_N^{(x_N)} \ldots P_1^{(x_1)}|\Psi\rangle\|^2$ where $P_i^{(x_i)} := P_i$ if $x_i = 1$, else $P_i^{(x_i)} := 1 - P_i$.

The difference to our conjecture is that in our conjecture, we only assume that the P_i commute *on a specific state* $|\Psi\rangle$, there might be other states where they do not commute.

In Section 4 we will show Theorem 1 for the special case where the primitive f is a function with one-bit output.

Then, in subsection 4.1, we generalize this to arbitrary f by a simple reduction to the 1-bit case.

Finally, in Section 5, we show how Conjecture 1 implies the impossibility of showing the indifferentiability of the Sponge construction and Feistel networks. (We stress that these impossibilities are based on the input/output sizes of the construction and the primitive. Thus, they also imply an analogous impossibility for any other construction that uses the a primitive of the same size.) The counting technique we use is quite general and is likely to apply to any construction that is length-extending. (In particular, this means that it is unlikely that we can use indifferentiability for analyzing hash functions based on random block functions.)

4 Transforming indifferentiability simulator into a stateless one

Throughout this section, $\mathcal{T}_1$ is a construction $\mathcal{C}[f]$ that uses a primitive function $f : X \to \{0,1\}$ as a building block. We consider $\mathcal{T}_2$ to be a random oracle H (or ideal cipher H) with the same domain and co-domain size as $\mathcal{T}_1$. We refer to $\mathcal{T}_1$ as "real case" and $\mathcal{T}_2$ as "ideal case" in the following. A quantum distinguisher $\mathcal{D}$, that tries to differentiate $\mathcal{C}[f]$ from H, has classical access to $\mathcal{C}[f]$ (private interface) and superposition access to f (public interface). The simulator that simulates f in the ideal case, has a superposition access to H.

We show that there exists a class of quantum distinguishers that can force any quantum simulator to fulfil some properties by applying some tests. At the end, we prove that perfect quantum indifferentiability implies classical indifferentiability with a stateless classical simulator. Recall that by a stateless classical simulator we mean a classical simulator that chooses a function $f : X \to \{0,1\}$ before receiving any query from the distinguisher. Then, it answers to a query on input x by $f(x)$.

By a "one-sided" distinguisher, we mean a distinguisher that outputs 1 with probability 1 while interacting with $\mathcal{C}[f]$ and f (the real case). The following lemma shows that for the finite class of distinguishers, the perfect quantum indifferentiability implies the existence of a simulator that is perfect for any distinguisher inside the class.

Lemma 1 *Let $\mathbb{D}$ be a finite class of "one-sided" distinguisher that make a polynomial number of queries. If the construction $\mathcal{T}_1$ is perfectly quantum indifferentiable from the construction $\mathcal{T}_2$, then there exists a simulator* Sim *such that for any $\mathcal{D} \in \mathbb{D}$,*

$$|\Pr[\mathcal{D}(\overline{\mathcal{T}_1^{priv}}, \mathcal{T}_1^{pub}) = 1] - \Pr[\mathcal{D}(\overline{\mathcal{T}_2^{priv}}, \mathsf{Sim}(\mathcal{T}_2^{pub})) = 1]| = 0.$$

Proof. Let $\mathcal{D}^*$ be a distinguisher that picks an uniformly random element from $\mathbb{D}$ and runs it. Considering $\mathcal{T}_1$ is perfectly quantum indifferentiable from $\mathcal{T}_2$, there exists Sim^* such that $|\Pr[\mathcal{D}^*(\overline{\mathcal{T}_1^{priv}}, \mathcal{T}_1^{pub}) = 1] - \Pr[\mathcal{D}^*(\overline{\mathcal{T}_2^{priv}}, \mathsf{Sim}^*(\mathcal{T}_2^{pub})) = 1]| = 0$. Assume that there exists $\mathcal{D} \in \mathbb{D}$ such that

$$|\Pr[\mathcal{D}(\overline{\mathcal{T}_1^{priv}}, \mathcal{T}_1^{pub}) = 1] - \Pr[\mathcal{D}(\overline{\mathcal{T}_2^{priv}}, \mathsf{Sim}^*(\mathcal{T}_2^{pub})) = 1]| > 0.$$

Since $\mathbb{D}$ is a class of one-sided distinguishers, we can conclude

$$|\Pr[\mathcal{D}^*(\overline{\mathcal{T}_1^{priv}}, \mathcal{T}_1^{pub}) = 1] - \Pr[\mathcal{D}^*(\overline{\mathcal{T}_2^{priv}}, \mathsf{Sim}^*(\mathcal{T}_2^{pub})) = 1]| > 0,$$

which is a contradiction. □

This section is dedicated to the proof the following theorem. In our proof, we assume that the implemented primitive f has a one-bit output and then afterwards we generalize the result to a construction $\mathcal{C}[f]$ that uses a primitive with n-bit output.

Theorem 2 *If two construction $\mathcal{C}[f]$ and H are **perfectly quantum** indifferentiable then for any classical "one-sided" distinguisher $\mathcal{D}_{cl}$ (cl stands for classical), there exists a stateless simulator Sim_{sl} (sl stands for stateless) such that*

$$|\Pr[\mathcal{D}_{cl}(\overline{\mathcal{C}[f]}, \overline{f}) = 1] - \Pr[\mathcal{D}_{cl}(\overline{H}, \overline{\mathsf{Sim}_{sl}(H)}) = 1]|$$

is negligible.

The remainder of this section is dedicated to the proof of Theorem 2.

Notations. S is the internal register (state) of the simulator, X,Y are input/output registers for querying the simulator (that are provided by the distinguishers), A is an ancillary wire and $|\Phi\rangle$ is the initial state of the simulator. The notation $[q]$ denotes the set $\{1, \ldots, q\}$.

Definition 3 *For a given simulator Sim, and for a given algorithm $\mathcal{D}$ querying the simulator, let $\rho_S^{\mathsf{Sim},\mathcal{D}} := \sum_j \lambda_j |\Psi_j\rangle\langle\Psi_j|$, where $\lambda_i > 0$ and $\{|\Psi_j\rangle\}_j$ is an orthonormal set of vectors, denotes the state of the S-register of Sim after running D. Let $V^{\mathcal{D},\mathsf{Sim}} := \{|\Psi_j\rangle\}_j$ (i.e., $V^{\mathcal{D},\mathsf{Sim}}$ is defined such that the state of Sim after running $\mathcal{D}$ is a mixture of pure states in $V^{\mathcal{D},\mathsf{Sim}}$).*

Definition 4 *We define $\mathbb{D}$ to be a specific finite class of "one-sided" distinguishers such that any distinguisher in $\mathbb{D}$ makes at most $q+2$ queries to the public interface of the construction. For readability, we specify the distinguishers in the class (members of $\mathbb{D}$) throughout the proof wherever we need them. We prefix each such declaration with "Distinguisher in $\mathbb{D}$:". Note that all the distinguishers are independent of the simulator, so $\mathbb{D}$ could in principle be defined at this point.*

Definition 5 *Let $V_i^{\mathsf{Sim}} := \bigcup_{\mathcal{D}} V^{\mathcal{D},\mathsf{Sim}}$ where the union ranges over all $\mathcal{D} \in \mathbb{D}$ that makes i queries (i.e., V_i^{Sim} is defined such that the state of Sim after i queries is a mixture of pure states in V_i^{Sim}). We omit Sim from V_q^{Sim} wherever Sim is clear. Note that $V_0 = \{|\Phi\rangle\}$ where $|\Phi\rangle$ is the initial state of the simulator.*

We start with a classical one-sided distinguisher $\mathcal{D}_{cl}$ that makes at most $q-1$ queries.

Distinguishers in $\mathbb{D}$: $\mathcal{D}_{cl} \in \mathbb{D}$.

Property 1 *The simulator is perfect for the class of distinguishers $\mathbb{D}$, that is, the simulator is a perfect simulator for any $\mathcal{D} \in \mathbb{D}$.*

Claim 1 *There exists a simulator Sim_1 that has Property 1.*

Proof. Since $\mathbb{D}$ is a finite class of one-sided distinguishers, the existence of Sim_1 follows from Lemma 1. □

Property 2 *The simulator is an unitary transformation, i.e., its operation in the i-th query is given by an unitary $U^{(i)}$ that may depend on the primitive that is queried by the simulator and it is applied to the registers X, Y, S.*

Claim 2 *There exists a simulator Sim_2 that has the properties 1 and 2.*

Proof. Let Sim_2 be a purification of Sim_1. It is clear that it fulfils the properties 1 and 2. □

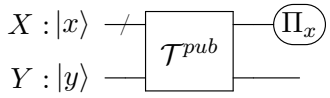
Property 3 *For any $i \in [q]$ and $x \in X$, there exists an unitary $U_x^{(i)}$ such that for any $|\Psi\rangle \in V_{i-1}$, $y \in Y$:*

$$U^{(i)}|x, y, \Psi\rangle = |x\rangle \otimes U_x^{(i)}|y, \Psi\rangle,$$

where $U^{(i)}$ is the unitary from Property 2.

Claim 3 Sim_2 *fulfils Property 3.*

Proof. Fix some $i \in [q]$. By definition of $V_{i-1}^{\mathsf{Sim}_2}$ for any $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_2}$, there exists an $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ such that $|\Psi\rangle \in V^{\mathsf{Sim}_2, \mathcal{D}^{(i-1)}}$. Let $\mathcal{D}_1^{(i)}(\mathcal{D}^{(i-1)})$ be an i-query distinguisher that runs $\mathcal{D}^{(i-1)}$, queries the public interface of the construction $\mathcal{T}$ for uniformly random inputs x, y, and measures the wire X by the projective measurement $\Pi_x = \{P_{yes}, I - P_{yes}\}$ in which $P_{yes} := |x\rangle\langle x|$ as follows:

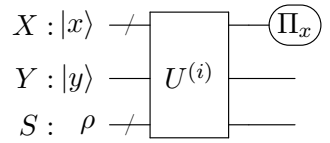


Finally, $\mathcal{D}_1^{(i)}(\mathcal{D}^{(i-1)})$ outputs 1 if the measurement result is "yes", otherwise it outputs 0.

Note that in the real case the output of the circuit above is $|x, y \oplus f(x)\rangle_{XY}$ for any x, y. Then the projective measurement Π_x on the register A will output "yes" with probability 1. Thus, $\mathcal{D}_1^{(i)}(\mathcal{D}^{(i-1)})$ is a one-sided distinguisher.

Distinguishers in $\mathbb{D}$: *For any $i \in [q]$ and any $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$, $\mathcal{D}_1^{(i)}(\mathcal{D}^{(i-1)}) \in \mathbb{D}$. (It may seem this rule (and others below) may make $\mathbb{D}$ infinite. However,it will be clear at the end of the proof that $\mathbb{D}$ is finite.)*

We depict the circuit in the ideal case where the state of the simulator is $\rho_S^{\mathsf{Sim}_2, \mathcal{D}^{(i-1)}} := \sum_j \lambda_j |\Psi_j\rangle\langle\Psi_j|$ where $\lambda_j > 0$ and $|\Psi_1\rangle := |\Psi\rangle$ after running $D^{(i-1)}$. (For simplicity we omit $\mathsf{Sim}_2, \mathcal{D}^{(i-1)}$ and S from $\rho_S^{\mathsf{Sim}_2, \mathcal{D}^{(i-1)}}$.)



Since the simulator Sim_2 is perfect for $\mathbb{D}$, the output of the measurement has to be "yes" with probability 1 in the ideal case, too. We show that the measurement Π_x outputs "no" (or "yes") with probability 0 (or 1) even if the inner state of the simulator is $|\Psi\rangle$ in the circuit above:

$$0 = \Pr[\text{"no"} \leftarrow \Pi : \text{state } \rho] = \sum_j \lambda_j \Pr[\text{"no"} \leftarrow \Pi : \text{state } |\Psi_j\rangle],$$

and since for any j, $\lambda_j > 0$ then $\Pr[\text{"no"} \leftarrow \Pi : \text{state } |\Psi\rangle] = 0$. So far we have proven that for any input $x \in X$, $y \in Y$ and $|\Psi\rangle \in V_{i-1}$, the measurement Π_x in the circuit above returns "yes" with probability 1. Now we prove the existence of the unitary $U_x^{(i)}$ for any x. Fix an arbitrary $x \in X$. Let us assume that $B := \{|b, \Psi_j\rangle\}_{b,j}$ is an orthonormal basis for $Y \otimes \operatorname{span} V_{i-1}$. Since $U^{(i)}$ is an unitary operation, then it transforms the orthonormal set $\{|x, y_b, \Psi_j\rangle\}_{b,j}$ to an orthonormal set $\{|x, y'_b, \Psi'_j\rangle\}_{b,j}$ (i.e, we assume that for any b and j, $U^{(i)}|x, y_b, \Psi_j\rangle = |x, y'_b, \Psi'_j\rangle$). We define $U_x^{(i)}$

to be the unitary that for any j and b, it maps $|y_b, \Psi_j\rangle$ to $|y'_b, \Psi'_j\rangle$ and it is arbitrary for the vectors that are not in $Y \otimes \operatorname{span} V_{i-1}$. Since $Y \otimes V_{i-1} \subseteq Y \otimes \operatorname{span} V_{i-1}$, then there exists an unitary $U_x^{(i)}$ such that for any $y \in Y$ and $|\Psi\rangle \in V_{i-1}$, $U^{(i)}(|x, y, \Psi\rangle_{XYS}) = |x\rangle \otimes U_x^{(i)}|y, \Psi\rangle$. Because x was chosen arbitrarily, we can conclude for any $x \in X$, there exists an unitary $U_x^{(i)}$ such that for any $y \in Y$ and $|\Psi\rangle \in V_{i-1}$, $U^{(i)}(|x, y, \Psi\rangle_{XYS}) = |x\rangle \otimes U_x^{(i)}|y, \Psi\rangle$.

□

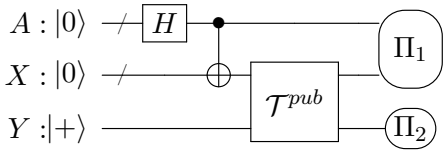
Property 4 *For any $i \in [q]$ and $|\Psi\rangle \in V_{i-1}$, there exists $|\Psi'\rangle$ such that*

$$\forall x: \; U_x^{(i)}(|+\rangle_Y \otimes |\Psi\rangle_S) = |+\rangle_Y \otimes |\Psi'\rangle_S,$$

where $U_x^{(i)}$ is the unitary from Property 3.

Claim 4 Sim_2 *fulfils Property 4.*

Proof. Fix some $i \in [q]$. By definition of $V_{(i-1)}^{\mathsf{Sim}_2}$ for any $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_2}$, there exists an $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ such that $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_2, \mathcal{D}^{(i-1)}}$. Let $\mathcal{D}_2^{(i)}(\mathcal{D}^{(i-1)})$ be an i-query distinguisher that runs $\mathcal{D}^{(i-1)}$, then it prepares an ancillary wire A and queries the public interface of the construction $\mathcal{T}$, and measures the A, X wires by the projective measurement $\Pi_1 = \{P_{yes}, I - P_{yes}\}$ in which $P_{yes} := |\Phi^+\rangle\langle\Phi^+|$ (where $|\Phi^+\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle\langle x|$) and the Y wire by the projective measurement $\Pi_2 = \{P_{yes}, I - P_{yes}\}$ in which $P_{yes} := |+\rangle\langle +|$ is as follows:

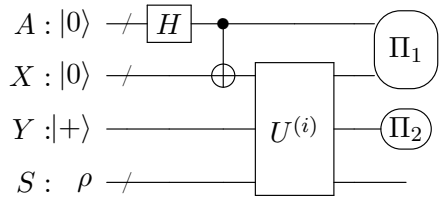


(In the circuit above, the Hadamard operation H is applied to each wire.) Finally, it outputs 1, if both measurements return "yes", otherwise, it outputs 0.

It is easy to see that in the real case the output of the circuit is $|\Phi^+\rangle_{AX} \otimes |+\rangle_Y$ and therefore both measurements return "yes" with probability 1. Thus, $\mathcal{D}_2^{(i)}(\mathcal{D}^{(i-1)})$ is a one-sided distinguisher.

Distinguishers in $\mathbb{D}$: *For any $i \in [q]$ and any $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$, $\mathcal{D}_2^{(i)}(\mathcal{D}^{(i-1)}) \in \mathbb{D}$.*

We depict the circuit above in the ideal case with Sim_2. The state of the simulator is $\rho = \sum_i \lambda_i |\Psi_i\rangle\langle\Psi_i|$ where $|\Psi_1\rangle = |\Psi\rangle$ and $\lambda_i > 0$.



Since the simulator Sim_2 is perfect for the class $\mathbb{D}$, both measurements return "yes" with probability 1 in the ideal case as well. We show that both measurements return "yes" even if the state of the simulator is $|\Psi\rangle$:

$$0 = \Pr[\text{"no"} \leftarrow \Pi_1 \vee \text{"no"} \leftarrow \Pi_2 : \text{state } \rho] = \sum_i \lambda_i \Pr[\text{"no"} \leftarrow \Pi_1 \vee \text{"no"} \leftarrow \Pi_2 : \text{state } |\Psi_i\rangle],$$

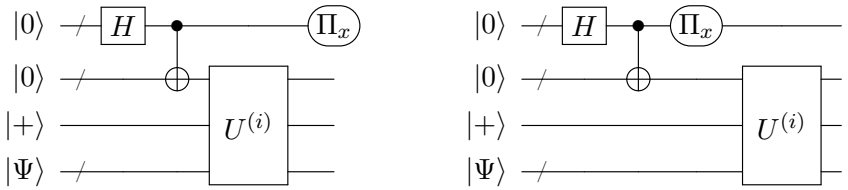
and since $\lambda_i > 0$ for any i, then

$$\forall i,\ \Pr[\text{“no”} \leftarrow \Pi_1 \vee \text{“no”} \leftarrow \Pi_2 : \text{state } |\Psi_i\rangle] = 0.$$

This proves that

$$\Pr[\text{“yes”} \leftarrow \Pi_1 \wedge \text{“yes”} \leftarrow \Pi_2 : \text{state } |\Psi\rangle] = 1.$$

Since the operation is unitary there exists a pure state $|\Psi'\rangle$ such that the circuit above, when the inner state of the simulator is $|\Psi\rangle$, outputs $|\Phi^+\rangle_{AX} \otimes |+\rangle_Y \otimes |\Psi'\rangle_S$ in the ideal case. Let for any $x \in X$, $\Pi_x := \{P_{yes}, I - P_{yes}\}$ be a projective measurement where $P_{yes} = |x\rangle\langle x|$. It is clear that the output of the following two circuits are the same for any Π_x.



Considering the right circuit, we can write:

$$2^{-n/2}|x\rangle_A|x\rangle_X|+\rangle_Y|\Psi'\rangle_S = 2^{-n/2}|x\rangle U^{(i)}|x,+,\Psi\rangle = 2^{-n/2}|x\rangle|x\rangle \otimes U_x^{(i)}|+\rangle|\Psi\rangle,$$

where the second equality holds because of the *Claim* 3 and therefore $U_x^{(i)}|+\rangle|\Psi\rangle = |+\rangle_Y|\Psi'\rangle_S$. □

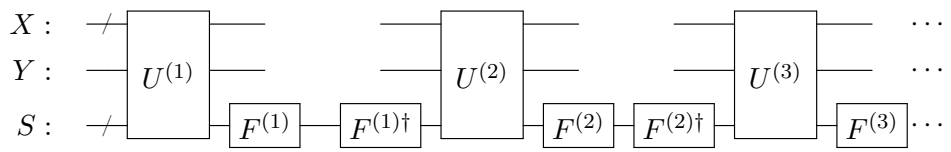
Property 5 *For any $i \in [q]$ and $|\Psi\rangle \in V_{i-1}$, $\forall x:\ U_x^{(i)}(|+\rangle_Y|\Psi\rangle_S) = |+\rangle \otimes |\Psi\rangle$.*

Claim 5 *There exists a simulator Sim_3 that has properties 1, 2, 3, and 5.*

Proof. Fix an $i \in [q]$. From Claim 4 and the linearity of $U_x^{(i)}$, it follows that for any $|\alpha\rangle \in \operatorname{span} V_{i-1}^{\mathsf{Sim}_2}$, there exists $|\Psi'\rangle$ such that for any x, $U_x^{(i)}|+\rangle|\alpha\rangle = |+\rangle|\Psi'\rangle$. Let $\{|e_j\rangle^{(i-1)}\}_j$ be an orthonormal basis of $\operatorname{span} V_{i-1}^{\mathsf{Sim}_2}$. Then for any x and j we can write $U_x^{(i)}|+\rangle|e_j\rangle^{(i-1)} = |+\rangle|e'_j\rangle^{(i)}$, where $\{|e'_j\rangle^{(i)}\}_j$ is some other orthonormal set (since $U_x^{(i)}$ is an unitary operation and preserves the orthogonality). Let $E^{(i)}$ be a unitary such that maps $|e'_j\rangle^{(i)}$ to $|e_j\rangle^{(i-1)}$ for any j (if $\operatorname{span}\{|e'_j\rangle^{(i)}\}_j$ is not the whole space, then $E^{(i)}$ can be defined arbitrarily for the rest of the vectors). For any $i \in [q]$, we define $F^{(i)} := E^{(1)} \dots E^{(i)}$ and let $F^{(0)} := I$. Let Sim_3 be a simulator that answers to the i-th query with the unitary:

$$U_{new}^{(i)}|x,y,\Psi\rangle := (I \otimes I \otimes F^{(i)})U^{(i)}(I \otimes I \otimes F^{(i-1)\dagger})|x,y,\Psi\rangle.$$

The following circuit depicts Sim_3.



Note that Sim_3 is a perfect simulator for the class of $\mathbb{D}$ (fulfils Property 1), because the Sim_3's answers to the distinguishers queries are indistinguishable from the Sim_2's answers (because the only difference between Sim_3 and Sim_2 is the application of an unitary transformation to the inner state register followed by its inverse). It is clear that Sim_3 fulfils Property 2 by its construction.

By definition of Sim_3, for any $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$ we can write $|\Psi\rangle = F^{(i-1)}|\Phi\rangle$ for some $|\Phi\rangle \in V_{i-1}^{\mathsf{Sim}_2}$. Let $|\Phi\rangle = \sum_j \alpha_j |e_j\rangle^{(i-1)}$. We show that Sim_3 has Property 3. We claim that for any $i \in [q]$ and $x \in X$, there exists a unitary $U_{x,new}^{(i)}$ such that for any $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$, $y \in Y$:

$$U_{new}^{(i)}|x, y, \Psi\rangle = |x\rangle \otimes U_{x,new}^{(i)}|y, \Psi\rangle.$$

$$\begin{aligned}
U_{new}^{(i)}|x, y, \Psi\rangle &= (I \otimes I \otimes F^{(i)})U^{(i)}(I \otimes I \otimes F^{(i-1)\dagger})|x, y, \Psi\rangle \\
&= (I \otimes I \otimes F^{(i)})U^{(i)}(I \otimes I \otimes F^{(i-1)\dagger})|x\rangle|y\rangle F^{(i-1)}|\Phi\rangle \\
&= (I \otimes I \otimes F^{(i)})U^{(i)}|x\rangle|y\rangle|\Phi\rangle \\
(Claim\ 3) &= (I \otimes I \otimes F^{(i)})(|x\rangle \otimes U_x^{(i)}|y\rangle|\Phi\rangle) \\
&= |x\rangle \otimes (I \otimes F^{(i)})U_x^{(i)}|y\rangle|\Phi\rangle \\
&= |x\rangle \otimes (I \otimes F^{(i)})U_x^{(i)}(I \otimes F^{(i-1)\dagger})|y\rangle|\Psi\rangle.
\end{aligned}$$

We define $U_{x,new}^{(i)} := (I \otimes F^{(i)})U_x^{(i)}(I \otimes F^{(i-1)\dagger})$ and this finishes the proof of our claim. Finally, we show that Sim_3 fulfils *Property* 5. We claim that for any $i \in [q]$, $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$, and $x \in X$: $U_{x,new}^{(i)}(|+\rangle|\Psi\rangle) = |+\rangle|\Psi\rangle$.

$$\begin{aligned}
U_{x,new}^{(i)}(|+\rangle|\Psi\rangle) &= (I \otimes F^{(i)})U_x^{(i)}(I \otimes F^{(i-1)\dagger})(|+\rangle|\Psi\rangle) \\
&= (I \otimes F^{(i)})U_x^{(i)}(I \otimes F^{(i-1)\dagger})(|+\rangle F^{(i-1)}|\Phi\rangle) \\
&= (I \otimes F^{(i)})U_x^{(i)}(|+\rangle|\Phi\rangle) \\
&= (I \otimes F^{(i)})U_x^{(i)}(|+\rangle \sum_j \alpha_j |e_j\rangle^{(i-1)}) \\
&= (I \otimes F^{(i)}) \sum_j \alpha_j U_x^{(i)}|+\rangle|e_j\rangle^{(i-1)} \\
&= (I \otimes F^{(i)}) \sum_j \alpha_j |+\rangle|e_j'\rangle^{(i)} \\
&= \sum_j \alpha_j (I \otimes F^{(i-1)}E^{(i)})|+\rangle|e_j'\rangle^{(i)} \\
&= \sum_j \alpha_j (I \otimes F^{(i-1)})|+\rangle|e_j\rangle^{(i-1)} \\
&= |+\rangle F^{(i-1)} \sum_j \alpha_j |e_j\rangle^{(i-1)} = |+\rangle F^{(i-1)}|\Phi\rangle = |+\rangle|\Psi\rangle.
\end{aligned}$$

□

For simplicity, we omit "*new*" from $U_{new}^{(i)}$ and $U_{x,new}^{(i)}$ for the rest of the paper.

Claim 6 *For any $i \in [q]$, $V_{i-1}^{\mathsf{Sim}_3} \subseteq V_i^{\mathsf{Sim}_3}$.*

Proof. Since Sim_3 has Property 5, $U^{(i)}|0\rangle_X|+\rangle_Y|\Psi\rangle$ is the identity for all $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$. Let $\mathcal{D}^{(i-1)} \in \mathbb{D}$ be a distinguisher that makes $i-1$ queries. Thus, we get every state in $V_i^{\mathsf{Sim}_3}$ using an i-query distinguisher $\mathcal{D}_3^{(i)}(\mathcal{D}^{(i-1)})$ that runs the distinguisher $\mathcal{D}^{(i-1)}$ and then additionally queries with $X, Y = |0\rangle|+\rangle$. Finally, the distinguisher outputs 1. Thus, it is a one-sided distinguisher.

Distinguishers in $\mathbb{D}$: *For any $i \in [q]$ and any $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$, the distinguisher $\mathcal{D}_3^{(i)}(\mathcal{D}^{(i-1)})$ (described above) is in $\mathbb{D}$.*

For all $(i-1)$-query distinguishers $\mathcal{D}^{(i-1)} \in \mathbb{D}$, we can write $V^{\mathsf{Sim}_3,\mathcal{D}^{(i-1)}} = V^{\mathsf{Sim}_3,\mathcal{D}_3^{(i)}(\mathcal{D}^{(i-1)})}$ and hence:

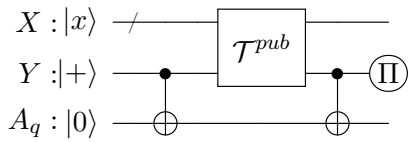
$$V_{i-1}^{\mathsf{Sim}_3} = \bigcup_{\mathcal{D}^{(i-1)} \in \mathbb{D}} V^{\mathsf{Sim}_3,\mathcal{D}^{(i-1)}} = \bigcup_{\mathcal{D}^{(i-1)} \in \mathbb{D}} V^{\mathsf{Sim}_3,\mathcal{D}_3^{(i)}(\mathcal{D}^{(i-1)})} \subseteq V_i^{\mathsf{Sim}_3}.$$

□

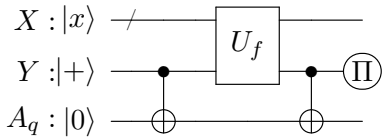
Property 6 *For any $i \in [q]$ and $|\Psi\rangle \in V_{i-1}$, and any x, $U_x^{(i)}|1\rangle_Y|\Psi\rangle = (X \otimes I_S)U_x^{(i)}|0\rangle_Y|\Psi\rangle$. Here X is the bit-flip operator (Pauli X matrix).*

Claim 7 Sim_3 *fulfils Property 6.*

Proof. Fix some $i \in [q]$. By definition of $V_{i-1}^{\mathsf{Sim}_3}$, for any $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$ there exists an $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ such that $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3,\mathcal{D}^{(i-1)}}$. Let $\mathcal{D}_4^{(i)}(\mathcal{D}^{(i-1)})$ be an i-query distinguisher that runs $\mathcal{D}^{(i-1)}$, prepares an ancillary wire A_q, queries the public interface of the construction for uniformly random x, and measures the outputs wire Y by the projective measurement $\Pi := \{P_{yes}, I - P_{yes}\}$ where $P_{yes} = |+\rangle\langle+|$ as follows:



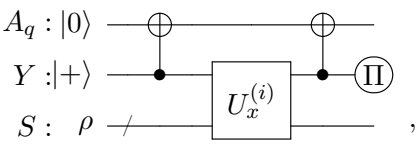
Finally, it outputs 1 if the measurement returns "yes", otherwise it outputs 0. We depict the circuit in the real case.



A simple calculation shows that the output of the circuit above is $|x, f(x)\rangle_{XA_q} \otimes |+\rangle_Y$ (before the measurement) for any x and the measurement returns "yes" on the wire A_q with probability 1. Thus, $\mathcal{D}_4^{(i)}(\mathcal{D}^{(i-1)})$ is a one-sided distinguisher.

Distinguishers in $\mathbb{D}$: *For any $i \in [q]$ and any $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$, the distinguisher $\mathcal{D}_4^{(i)}(\mathcal{D}^{(i-1)})$ (described above) is in $\mathbb{D}$.*

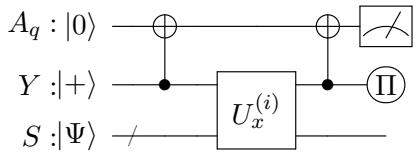
Since the simulator is perfect for the class $\mathbb{D}$, the measurement will output "yes" with probability 1 in the ideal case as well. We depict the circuit in the ideal case where $\rho := \sum_j \lambda_j |\Psi_j\rangle\langle\Psi_j|$ is the inner state of Sim_3 after running the distinguisher $\mathcal{D}^{(i-1)}$.



,

Similar to Claim 3, we can conclude that the measurement returns "yes" even if the state of the simulator is $|\Psi\rangle$.

To prove the claim, we analyse the output of the following circuit.



where the measurement on the wire A_q is the computational basis measurement. We write $U_x^{(i)}|0\rangle|\Psi\rangle = |0\rangle|\Psi_{00}\rangle + |1\rangle|\Psi_{01}\rangle$ and $U_x^{(i)}|1\rangle|\Psi\rangle = |0\rangle|\Psi_{10}\rangle + |1\rangle|\Psi_{11}\rangle$ for some non-normalized states $|\Psi_{bb'}\rangle$. Then, the output of the circuit before the measurements is

$$\frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle|\Psi_{00}\rangle + |1\rangle|1\rangle|\Psi_{01}\rangle + |1\rangle|0\rangle|\Psi_{10}\rangle + |0\rangle|1\rangle|\Psi_{11}\rangle\big).$$

We show that $|\Psi_{00}\rangle = |\Psi_{11}\rangle$ and $|\Psi_{10}\rangle = |\Psi_{01}\rangle$. The measurement on the wire Y returns $|+\rangle$ with probability 1. If the computational basis measurement never outputs 0 or 1, then we can conclude $|\Psi_{00}\rangle = |\Psi_{11}\rangle = 0$ or $|\Psi_{10}\rangle = |\Psi_{01}\rangle = 1$, respectively. Otherwise, we would get the equations

$$|0\rangle|\Psi_{00}\rangle + |1\rangle|\Psi_{11}\rangle = |+\rangle|\Psi'\rangle \text{ and } |1\rangle|\Psi_{01}\rangle + |0\rangle|\Psi_{10}\rangle = |+\rangle|\Psi''\rangle,$$

for some states $|\Psi'\rangle$ and $|\Psi''\rangle$. We apply the operations $\langle 0| \otimes I$ and $\langle 1| \otimes I$ to the two sides of the equations above to conclude $|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}|\Psi'\rangle = |\Psi_{11}\rangle$ and $|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}|\Psi''\rangle = |\Psi_{01}\rangle$. Therefore,

$$\begin{aligned} U_x^{(i)}|0\rangle|\Psi\rangle &= |0\rangle|\Psi_{00}\rangle + |1\rangle|\Psi_{01}\rangle \\ &= |0\rangle|\Psi_{11}\rangle + |1\rangle|\Psi_{10}\rangle \\ &= (X \otimes I)U_x^{(i)}|1\rangle|\Psi\rangle. \end{aligned}$$

□

Property 7 *For any $i \in [q]$, $|\Psi\rangle \in V_{i-1}$ and x, there are non-normalized $|\Psi_{x0}\rangle, |\Psi_{x1}\rangle$ such that:*

$$U_x^{(i)}|b\rangle|\Psi\rangle = |b\rangle|\Psi_{x0}\rangle + |\bar{b}\rangle|\Psi_{x1}\rangle \text{ and } |\Psi_{x0}\rangle + |\Psi_{x1}\rangle = |\Psi\rangle.$$

Claim 8 Sim_3 *has Property 7.*

Proof. It is clear that we can write $U_x^{(i)}|0\rangle|\Psi\rangle = |0\rangle|\Psi_{x0}\rangle + |1\rangle|\Psi_{x1}\rangle$ for some non-normalized $|\Psi_{x0}\rangle, |\Psi_{x1}\rangle$. Since Sim_3 has Property 6, we can write $U_x^{(i)}|1\rangle|\Psi\rangle = |1\rangle|\Psi_{x0}\rangle + |0\rangle|\Psi_{x1}\rangle$. We prove that $|\Psi_{x0}\rangle + |\Psi_{x1}\rangle = |\Psi\rangle$.

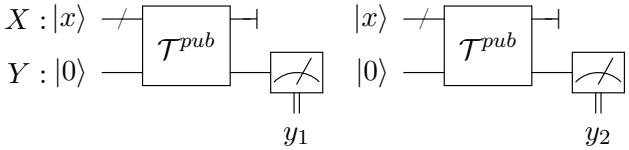
$$\begin{aligned} U_x^{(i)}|+\rangle|\Psi\rangle &= \frac{1}{\sqrt{2}}\big(U_x^{(i)}|0\rangle|\Psi\rangle + U_x^{(i)}|1\rangle|\Psi\rangle\big) \\ &= \frac{1}{\sqrt{2}}\big(|0\rangle|\Psi_{x0}\rangle + |1\rangle|\Psi_{x1}\rangle + |1\rangle|\Psi_{x0}\rangle + |0\rangle|\Psi_{x1}\rangle\big) \\ &= |+\rangle\big(|\Psi_{x0}\rangle + |\Psi_{x1}\rangle\big) \end{aligned}$$

On the other hand, by Property 5 $U_x^{(i)}|+\rangle|\Psi\rangle = |+\rangle|\Psi\rangle$ and therefore $|\Psi_{x0}\rangle + |\Psi_{x1}\rangle = |\Psi\rangle$. □

Property 8 *For any $i \in [q]$, $x \in X$, and $|\Psi\rangle \in V_{i-1}$, the states $|\Psi_{x0}\rangle$ and $|\Psi_{x1}\rangle$ from Property 7 are orthogonal. In addition, for any x there exists a projector $P_x^{(i)}$ such that for any $|\Psi\rangle \in \operatorname{span} V_{i-1}$, we can write $U_x^{(i)} : |b\rangle|\Psi\rangle \mapsto |b\rangle P_x^{(i)}|\Psi\rangle + |1-b\rangle\overline{P_x^{(i)}}|\Psi\rangle$ where $\overline{P_x^{(i)}} := I - P_x^{(i)}$.*

Claim 9 Sim_3 *has Property 8.*

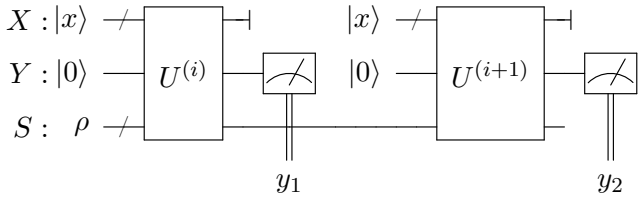
Proof. Fix $i \in [q]$ and $|\Psi\rangle \in V_{i-1}$. By the definition of V_{i-1}, there exists an $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ such that $|\Psi\rangle \in V^{\mathcal{D}^{(i-1)}}$. Let the state of the simulator after running $\mathcal{D}^{(i-1)}$ be $\rho := \sum_i \lambda_i |\Psi_i\rangle\langle\Psi_i|$ where $|\Psi_1\rangle := |\Psi\rangle$ and $\lambda_i > 0$ (this is possible by the definition of $V^{\mathcal{D}^{(i-1)}}$). Let $\mathcal{D}_5^{(i+1)}(\mathcal{D}^{(i-1)})$ be a distinguisher that runs $\mathcal{D}^{(i-1)}$ and queries the public interface of the construction on the same uniformly random input x in the i-th and $(i+1)$-th query, and then measures the output wire Y as depicted in the following circuit.



Finally, the distinguisher outputs 1 if $y_1 = y_2$ and 0 otherwise. It is clear that in the real case, the distinguisher returns 1 with probability 1. Thus, $\mathcal{D}_5^{(i+1)}(\mathcal{D}^{(i-1)})$ is a one-sided distinguisher.

Distinguishers in $\mathbb{D}$: *For any $i \in [q]$ and any $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$, the distinguisher $\mathcal{D}_5^{(i+1)}(\mathcal{D}^{(i-1)})$ (described above) is in $\mathbb{D}$.*

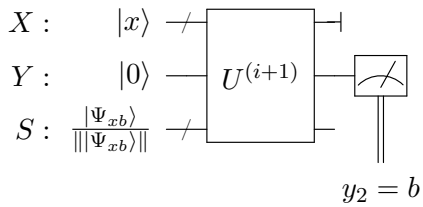
We depict the circuit above in the ideal case:



Since Sim_3 is a perfect simulator for the class $\mathbb{D}$, then in the circuit above $y_1 = y_2$ with probability 1. We show that $\Pr[y_1 = y_2] = 1$ even if the inner state of the simulator is $|\Psi\rangle$:

$$0 = \Pr[y_1 \neq y_2 : \text{state } \rho] = \sum_i \lambda_i \Pr[y_1 \neq y_2 : \text{state } |\Psi_i\rangle]. \tag{3}$$

Since $\forall i,\ \lambda_i > 0$ and $|\Psi_1\rangle = |\Psi\rangle$, then we can conclude $\Pr[y_1 \neq y_2 : |\Psi\rangle] = 0$. We analyse the circuit above assuming the inner state of the simulator is $|\Psi\rangle$. Notice that if y_1 is measured to be some $b \in \{0,1\}$ then the inner state after running the first part of the circuit is $\frac{|\Psi_{xb}\rangle}{\||\Psi_{xb}\rangle\|}$ by Property 7. If $\Pr[y_1 = 0] = 0$ or $\Pr[y_1 = 1] = 0$, then $|\Psi_{x0}\rangle = 0$ or $|\Psi_{x1}\rangle = 0$, respectively, and $|\Psi_{x0}\rangle$, $|\Psi_{x1}\rangle$ are orthogonal. So let us assume that $\Pr[y_1 = 0] > 0$ and $\Pr[y_1 = 1] > 0$. We claim that the second part of the circuit can distinguish the states $\frac{|\Psi_{x0}\rangle}{\||\Psi_{x0}\rangle\|}$ and $\frac{|\Psi_{x1}\rangle}{\||\Psi_{x1}\rangle\|}$ perfectly and therefore they are orthogonal. (Note that when y_1 is not known, the state of the simulator after the first query can be either one of $\frac{|\Psi_{x0}\rangle}{\||\Psi_{x0}\rangle\|}$ or $\frac{|\Psi_{x1}\rangle}{\||\Psi_{x1}\rangle\|}$.) So we need to show, that for each $b \in \{0,1\}$ in the case of the input $\frac{|\Psi_{xb}\rangle}{\||\Psi_{xb}\rangle\|}$ to the second part of the circuit the result of the y_2-measurement will always be b.



In other words, we show that the probability of measuring b in the circuit above is 1. Suppose for a contradiction this was not the case, and it was possible to measure $1-b$ with some probability ϵ, then

$$\Pr[y_1 = b \wedge y_2 = 1-b] = \Pr[y_1 = b] \cdot \Pr[y_2 = 1-b | y_1 = b] > 0.$$

Here the first factor is > 0 by assumption, and the second factor is precisely $= \epsilon$. By (3), it cannot happen that different values b and $1-b$ are measured for y_1 and y_2. Therefore, the second part of the circuit can distinguish the states $\frac{|\Psi_{x0}\rangle}{\||\Psi_{x0}\rangle\|}$ and $\frac{|\Psi_{x1}\rangle}{\||\Psi_{x1}\rangle\|}$ perfectly and therefore they are orthogonal.

Finally, we prove the existence of the projector $P_x^{(i)}$. We define $V_{xb} := \operatorname{span}\{|\Psi_{xb}\rangle\}_{|\Psi\rangle \in V_{i-1}}$. We show that for any $|\Psi\rangle$, $|\Psi'\rangle \in V_{i-1}$ with $|\Psi\rangle \neq |\Psi'\rangle$, $\langle \Psi_{xb}, \Psi'_{x\bar{b}} \rangle = 0$ ($|\Psi_{xb}\rangle$ and $|\Psi'_{x\bar{b}}\rangle$ are orthogonal). Since for any $|\Psi\rangle \in V_{i-1}$ the measurement in the circuit above returns b with probability 1 and using Property 3, we can write

$$\frac{U^{(i+1)}|x, 0, \Psi_{xb}\rangle}{\||\Psi_{xb}\rangle\|} = |x\rangle|b\rangle|\Phi\rangle \quad \text{and} \quad \frac{U^{(i+1)}|x, 0, \Psi'_{x\bar{b}}\rangle}{\||\Psi'_{x\bar{b}}\rangle\|} = |x\rangle|\bar{b}\rangle|\Phi'\rangle,$$

for some states $|\Phi\rangle$ and $|\Phi'\rangle$. Now it is clear that $\langle \Psi_{xb}, \Psi'_{x\bar{b}} \rangle = 0$ since a unitary transformation preserves the Hilbert space inner product. We define $P_x^{(i)}$ to be the projector onto the Hilbert space V_{x0}. Note that the definition of $P_x^{(i)}$ does not depend on the choice of $|\Psi\rangle \in V_{i-1}$. Since for any x and $|\Psi\rangle \in V_{i-1}$, $P_x^{(i)}|\Psi_{x0}\rangle = |\Psi_{x0}\rangle$ and $\overline{P_x^{(i)}}|\Psi_{x1}\rangle = |\Psi_{x1}\rangle$, we can write

$$U_x^{(i)}|b\rangle|\Psi\rangle = |b\rangle|\Psi_{x0}\rangle + |\bar{b}\rangle|\Psi_{x1}\rangle = |b\rangle P_x^{(i)}|\Psi\rangle + |\bar{b}\rangle\overline{P_x^{(i)}}|\Psi\rangle. \tag{4}$$

And finally, the result holds for any $|\Psi\rangle \in \operatorname{span} V_{i-1}$ by the linearity of $U_x^{(i)}$ and $P_x^{(i)}$. □

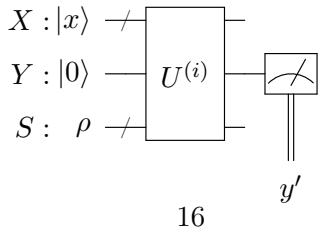
Property 9 *For any $i \in [q]$, $|\Psi\rangle \in \operatorname{span} V_{i-1}$, and $x \in X$, $P_x^{(i)}|\Psi\rangle = P_x^{(i+1)}|\Psi\rangle$, where $P_x^{(i)}$ and $P_x^{(i+1)}$ are the projectors from Property 8.*

Claim 10 Sim_3 *fulfils Property 9.*

Proof. Fix some $i \in [q]$ and $|\Psi\rangle \in V_{i-1}$(not $\operatorname{span} V_{i-1}$). By definition of $V_{i-1}^{\mathsf{Sim}_3}$, for any $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$ there exists an $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ such that $|\Psi\rangle \in V^{\mathsf{Sim}_3, \mathcal{D}^{(i-1)}}$. Let the state of the simulator after running $\mathcal{D}^{(i-1)}$ be $\rho := \sum_j \lambda_j |\Psi_j\rangle\langle\Psi_j|$ where $|\Psi_1\rangle := |\Psi\rangle$ and $\lambda_j > 0$ (this is possible by the definition of $V^{\mathcal{D}^{(i-1)}}$). Let $\mathcal{D}_6^{(i)}(\mathcal{D}^{(i-1)})$ be a distinguisher that runs the distinguisher $\mathcal{D}^{(i-1)}$, then queries the public interface of the construction (the i-th query) for uniformly random input x, then measures the output register in the computational basis, and finally it outputs 1. It is clear that $\mathcal{D}_6^{(i)}(\mathcal{D}^{(i-1)})$ is a one-sided distinguisher.

Distinguishers in $\mathbb{D}$: *For any $i \in [q]$ and any $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$, the distinguisher $\mathcal{D}_6^{(i)}(\mathcal{D}^{(i-1)})$ (described above) is in $\mathbb{D}$.*

Note that we need the distinguisher $\mathcal{D}_6^{(i)}(\mathcal{D}^{i-1})$ to show that for any $x \in X$ and $|\Psi\rangle \in V_{i-1}$, $P_x^{(i)}|\Psi\rangle$ and $\overline{P_x^{(i)}}|\Psi\rangle \in V_i$ where $P_x^{(i)}$ is defined in Claim 9. We depict the circuit corresponding to i-th query of $\mathcal{D}_6^{(i)}(\mathcal{D}^{i-1})$ in the ideal case.



Let $M_y := I \otimes |y\rangle\langle y| \otimes I$ and $Pro(|\Phi\rangle) := |\Phi\rangle\langle\Phi|$. We can calculate the inner state of the simulator after running $\mathcal{D}_6^{(i)}(\mathcal{D}^{i-1})$:

$$\begin{aligned}
\rho^{\mathsf{Sim}_3,\mathcal{D}_6^{(i)}(\mathcal{D}^{i-1})} &= \mathrm{tr}_{X,Y} \sum_{x,y,j} \frac{\lambda_j}{|X|} M_y U^{(i)} \Big(|x\rangle\langle x| \otimes |0\rangle\langle 0| \otimes |\Psi_j\rangle\langle\Psi_j| \Big) U^{(i)\dagger} M_y^\dagger \\
(Claim\ 9) &= \mathrm{tr}_{X,Y} \sum_{x,y,j} \frac{\lambda_j}{|X|} M_y Pro\big(|x,0\rangle \otimes P_x^{(i)}|\Psi_j\rangle + |x,1\rangle \otimes \overline{P_x^{(i)}}|\Psi_j\rangle\big) M_y^\dagger \\
&= \mathrm{tr}_{X,Y} \sum_{x,j} \frac{\lambda_j}{|X|} \Big(Pro\big(|x,0\rangle \otimes P_x^{(i)}|\Psi_j\rangle\big) + Pro\big(|x,1\rangle \otimes \overline{P_x^{(i)}}|\Psi_j\rangle\big) \Big) \\
&= \sum_{x,j} \frac{\lambda_j}{|X|} \Big(Pro\big(P_x^{(i)}|\Psi_j\rangle\big) + Pro\big(\overline{P_x^{(i)}}|\Psi_j\rangle\big) \Big)
\end{aligned}$$

Therefore,

$$\overline{P_x^{(i)}}|\Psi\rangle, P_x^{(i)}|\Psi\rangle \in \sup \rho^{\mathsf{Sim}_3,\mathcal{D}_6^{(i)}(\mathcal{D}^{i-1})} = \mathrm{span}\, V_i^{\mathsf{Sim}_3,\mathcal{D}_6^{(i)}(\mathcal{D}^{i-1})} \subseteq \mathrm{span}\, V_i^{\mathsf{Sim}_3}. \tag{5}$$

We use the distinguisher $\mathcal{D}_5^{(i+1)}(\mathcal{D}^{(i-1)})$ described in the proof of Claim 9. Recall that the outputs of the measurements of $\mathcal{D}_5^{(i+1)}(\mathcal{D}^{(i-1)})$ are the same with probability 1 even if the inner state of the simulator is $|\Psi\rangle$ (i.e., $\Pr[y_1 = y_2] = 1$). We analyse the measurement outputs of the distinguisher $\mathcal{D}_5^{(i+1)}(\mathcal{D}^{(i-1)})$. We have the following three cases for the first measurement outcome:

1. $0 < \Pr[y_1 = 0] < 1$. Recall that $\Pr[y_2 = 0|y_1 = 0] = 1$ and $\Pr[y_2 = 1|y_1 = 1] = 1$. The state just before measuring y_1 is $U^{(i)}|x\rangle|0\rangle|\Psi\rangle$. We can write $U^{(i)}|x\rangle|0\rangle|\Psi\rangle = |x\rangle \otimes \big(|0\rangle P_x^{(i)}|\Psi\rangle + |1\rangle\overline{P_x^{(i)}}|\Psi\rangle\big)$ by *Claim* 9. When the first measurement output is 0 ($y_1 = 0$), the input to the $(i+1)$-query will be $|x\rangle|0\rangle P_x^{(i)}|\Psi\rangle$. And since $P_x^{(i)}|\Psi\rangle \in \mathrm{span}\, V_i$ and Sim_3 has Property 8, the state before measuring y_2 is (in the $y_1 = 0$ case):

$$U^{(i+1)}|x\rangle|0\rangle P_x^{(i)}|\Psi\rangle = |x\rangle \otimes \big(|0\rangle P_x^{(i+1)} P_x^{(i)}|\Psi\rangle + |1\rangle\overline{P_x^{(i+1)}} P_x^{(i)}|\Psi\rangle\big).$$

   Since in this case $\Pr[y_2 = 0] = 1$, then we can conclude $\overline{P_x^{(i+1)}} P_x^{(i)}|\Psi\rangle = 0$ and hence $P_x^{(i+1)} P_x^{(i)}|\Psi\rangle = P_x^{(i)}|\Psi\rangle$. Similarly, we can show $P_x^{(i+1)}\ \overline{P_x^{(i)}}|\Psi\rangle = 0$, when $y_1 = 1$. Therefore, we can conclude

$$P_x^{(i+1)}|\Psi\rangle = P_x^{(i+1)} P_x^{(i)}|\Psi\rangle + P_x^{(i+1)}\overline{P_x^{(i)}}|\Psi\rangle = P_x^{(i)}|\Psi\rangle. \tag{6}$$

2. If $\Pr[y_1 = 0] = 1$ then $\overline{P_x^{(i)}}|\Psi\rangle = 0 = P_x^{(i+1)}\overline{P_x^{(i)}}|\Psi\rangle$ and since $\Pr[y_2 = 1] = 1$ and similar to the previous case, we can deduce 6.

3. If $\Pr[y_1 = 1] = 0$ then $P_x^{(i)}|\Psi\rangle = 0 = P_x^{(i+1)} P_x^{(i)}|\Psi\rangle$ and since $\Pr[y_2 = 1] = 1$ and similar to the first case, we can deduce 6.

Thus we have shown that Property 9 holds for any $|\Psi\rangle \in V_{i-1}$. And finally, the result holds for any $|\Psi\rangle \in \mathrm{span}\, V_{i-1}$ by the linearity of $P_x^{(i)}$ and $P_x^{(i+1)}$. □

Property 10 *For any* $i \in [q-2]$, $|\Psi\rangle \in V_{i-1}$ *and* x, x', $\overline{P_x^{(i+2)}} P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle = 0$ *and* $P_x^{(i+2)} P_{x'}^{(i+1)} \overline{P_x^{(i)}} |\Psi\rangle = 0$.

Claim 11 Sim_3 *fulfils Property 10.*

Proof. Fix some $i \in [q-2]$. By definition of $V_{i-1}^{\mathsf{Sim}_3}$, for any $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$ there exists an $(i-1)$-query distinguisher $\mathcal{D}^{(i-1)} \in \mathbb{D}$ such that $|\Psi\rangle \in V^{\mathsf{Sim}_3, \mathcal{D}^{(i-1)}}$. Let the state of the simulator after running $\mathcal{D}^{(i-1)}$ be $\rho = \sum_i \lambda_i |\Psi_i\rangle\langle\Psi_i|$ with $|\Psi\rangle = |\Psi_1\rangle$ and $\lambda_1 > 0$. Let $\mathcal{D}_7^{(i+2)}(\mathcal{D}^{i-1})$ be a distinguisher that runs $\mathcal{D}^{(i-1)}$ and does the following steps, respectively:

1. Run $\mathcal{D}^{(i-1)}$
2. Pick uniformly at random x, x' from X. Query $|x\rangle_X |0\rangle_Y$ to the public interface of the construction (i-th query). Then measures the output register and gets some bit b.
3. Query $|x'\rangle_X |0\rangle_Y$ to the public interface of the construction ($(i+1)$-th query). Measure the output register and gets some bit b'.
4. Query $|x\rangle_X |0\rangle_Y$ to the public interface of the construction ($(i+2)$-th query) and measure the output register to get some bit b''.
5. It outputs 1 if $b = b''$, and 0 otherwise.

In the real case, $b = b''$ with probability 1. Thus, $\mathcal{D}_7^{(i+2)}(\mathcal{D}^{i-1})$ is a one-sided distinguisher.

Distinguishers in $\mathbb{D}$: *For any* $i \in [q-2]$ *and any* $(i-1)$*-query distinguisher* $\mathcal{D}^{(i-1)} \in \mathbb{D}$*, the distinguisher* $\mathcal{D}_7^{i+2}(\mathcal{D}^{i-1})$ *(described above) is in* $\mathbb{D}$.

We analyse the test in the ideal case. Since Sim_3 is a perfect simulator for $\mathbb{D}$, then $b = b''$ with probability 1 in the ideal case as well when the state of the simulator is ρ after running $\mathcal{D}^{i-1}$. Using similar argument as in Claim 9, we can conclude that $\Pr[b = b''] = 1$ even if the state of the simulator is $|\Psi\rangle$. Therefore, we assume that the inner state of the simulator is $|\Psi\rangle$ in the following analyses. Since Sim_3 has Property 8, the output state of the i-th query is $|x\rangle_X |0\rangle_Y P_x^{(i)} |\Psi\rangle_S + |x\rangle_X |1\rangle_Y \overline{P_x^{(i)}} |\Psi\rangle_S$. Depending on the distribution of the result of the measurements, there are the following cases.

Case 1. If $0 < \Pr[b = 0] < 1$. Now if $b = 0$ then the input to the $(i+1)$-th query is $|x'\rangle \otimes |0\rangle \otimes P_x^{(i)} |\Psi\rangle$ and since $P_x^{(i)} |\Psi\rangle \in \operatorname{span} V_i^{\mathsf{Sim}_3}$ (this is shown using the distinguisher D_6 in Claim 10) and the linearity of $U^{(i+1)}$, the output of the $(i+1)$-th query is

$$|x'\rangle_X |0\rangle_Y P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle_S + |x'\rangle_X |1\rangle_Y \overline{P_{x'}^{(i+1)}} P_x^{(i)} |\Psi\rangle_S.$$

Now we write two cases based on the distribution of the bit b':

- If $\Pr[b' = 0] = 0$, we can deduce $P_x^{(i+1)} P_{x'}^{(i)} |\Psi\rangle_S = 0$ and consequently $\overline{P_x^{(i+2)}} P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle = 0$.
- Otherwise, with non-zero probability the input to the $(i+1)$-th query is $|x'\rangle |0\rangle P_x^{(i+1)} P_{x'}^{(i)} |\Psi\rangle_S$. Since $P_x^{(i+1)} P_{x'}^{(i)} |\Psi\rangle_S \in \operatorname{span} V_{i+1}$ (it is shown using the distinguisher $\mathcal{D}_6^{(i+1)}$ in Claim 10) the linearity of $U^{(i+2)}$ and Property 8, the output of the $(i+2)$-th query is

  $$|x'\rangle_X |0\rangle_Y P_x^{(i+2)} P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle_S + |x'\rangle_X |1\rangle_Y \overline{P_x^{(i+2)}} P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle_S.$$

  Since $b = b''$ with probability 1, then $\overline{P_x^{(i+2)}} P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle = 0$.

Now if $b = 1$ then the input to the $(i+1)$-th query is $|x'\rangle \otimes |0\rangle \otimes \overline{P_x^{(i)}}|\Psi\rangle$ and since $\overline{P_x^{(i)}}|\Psi\rangle \in \operatorname{span} V_i^{\mathsf{Sim}_3}$ (this is shown using the distinguisher $D_6^{(i)}$ in Claim 10) the output of the $(i+1)$-th query is

$$|x'\rangle_X |0\rangle_Y P_{x'}^{(i+1)} \overline{P_x^{(i)}}|\Psi\rangle_S + |x'\rangle_X |1\rangle_Y \overline{P_{x'}^{(i+1)}}\ \overline{P_x^{(i)}}|\Psi\rangle_S.$$

Now there are two cases based on the distribution of the bit b':

- If $\Pr[b' = 0] = 0$, then we can deduce $P_x^{(i+1)} \overline{P_{x'}^{(i)}}|\Psi\rangle_S = 0$ and consequently $\overline{P_x^{(i+2)}} P_{x'}^{(i+1)} \overline{P_x^{(i)}}|\Psi\rangle = 0$.
- Otherwise, with non-zero probability the input to the $(i+2)$-th query is $|x\rangle|0\rangle P_{x'}^{(i+1)} \overline{P_x^{(i)}}|\Psi\rangle_S$. Since $P_x^{(i+1)} P_{x'}^{(i)}|\Psi\rangle_S \in \operatorname{span} V_{i+1}$ (it is shown using the distinguisher $\mathcal{D}_6^{(i+1)}$ in Claim 10), the linearity of $U^{(i+2)}$ and Property 8, the output of the $(i+2)$-th query is

  $$|x\rangle_X |0\rangle_Y P_x^{(i+2)} P_{x'}^{(i+1)} \overline{P_x^{(i)}}|\Psi\rangle_S + |x\rangle_X |1\rangle_Y \overline{P_x^{(i+2)}} P_{x'}^{(i+1)} \overline{P_x^{(i)}}|\Psi\rangle_S.$$

  Since $b = b''$ with probability 1, then $P_x^{(i+2)} P_{x'}^{(i+1)} \overline{P_x^{(i)}}|\Psi\rangle = 0$.

Case 2. If $\Pr[b = 0] = 1$ then $\overline{P_x^{(i)}}|\Psi\rangle_S = 0$ and consequently $P_x^{(i+2)} P_{x'}^{(i+1)} \overline{P_x^{(i)}}|\Psi\rangle = 0$. Analogous to Case 1, we can also deduce $\overline{P_x^{(i+2)}} P_{x'}^{(i+1)} P_x^{(i)}|\Psi\rangle = 0$.

Case 3. If $\Pr[b = 1] = 0$ then $P_x^{(i)}|\Psi\rangle_S = 0$ and consequently $\overline{P_x^{(i+2)}} P_{x'}^{(i+1)} P_x^{(i)}|\Psi\rangle = 0$. Analogous to Case 1, we can also conclude $P_x^{(i+2)} P_{x'}^{(i+1)} \overline{P_x^{(i)}}|\Psi\rangle = 0$. □

Lemma 2 *Let P and Q be rank-one projectors over a two dimensional Hilbert space $\mathcal{H}$ such that for any $|\Psi\rangle \in \mathcal{H}$, $\bar{Q}PQ|\Psi\rangle = 0$ and $QP\bar{Q}|\Psi\rangle = 0$. Then, P and Q commute on $\mathcal{H}$, i.e, $\forall\ |\Psi\rangle \in \mathcal{H},\ PQ|\Psi\rangle = QP|\Psi\rangle$.*

Proof. There exists some normalized vectors $|\alpha\rangle$ and $|\beta\rangle$ such that $P = |\alpha\rangle\langle\alpha|$ and $Q = |\beta\rangle\langle\beta|$. By the Gram-Schmidt process, we can obtain two orthonormal bases $\{|\alpha\rangle, |\bar{\alpha}\rangle\}$ and $\{|\beta\rangle, |\bar{\beta}\rangle\}$ for $\mathcal{H}$. If $|\Psi\rangle = 0$, then $PQ|\Psi\rangle = QP|\Psi\rangle$. We show the lemma for any $|\Psi\rangle \neq 0$. From $\bar{Q}PQ|\Psi\rangle = 0$ and $QP\bar{Q}|\Psi\rangle = 0$, we can write, respectively,

$$|\bar{\beta}\rangle\langle\bar{\beta}|\alpha\rangle\langle\alpha|\beta\rangle\langle\beta|\Psi\rangle = 0 \text{ and } |\beta\rangle\langle\beta|\alpha\rangle\langle\alpha|\bar{\beta}\rangle\langle\bar{\beta}|\Psi\rangle = 0.$$

Thus, one of $\langle\bar{\beta}|\alpha\rangle, \langle\alpha|\beta\rangle$ or $\langle\beta|\Psi\rangle$ is zero and one of $\langle\beta|\alpha\rangle,\ \langle\alpha|\bar{\beta}\rangle$ or $\langle\bar{\beta}|\Psi\rangle$ is zero. Since $\langle\beta|\Psi\rangle$ and $\langle\bar{\beta}|\Psi\rangle$ can not be zero simultaneously, one of the following cases has to occur:

1. If $\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle = 0$, then $PQ|\Psi\rangle = QP|\Psi\rangle = 0$
2. If $\langle\bar{\beta}|\alpha\rangle = \langle\alpha|\bar{\beta}\rangle = 0$, then $P\bar{Q} = \bar{Q}P = 0$. Hence,

$$PQ = P(I - \bar{Q}) = P - P\bar{Q} = P - \bar{Q}P = (I - \bar{Q})P = QP.$$

□

Property 11 *For any $i \in [q-2]$, $|\Psi\rangle \in V_{i-1}$, x, x': $P_{x'}^{(i+1)} P_x^{(i)}|\Psi\rangle = P_x^{(i+1)} P_{x'}^{(i)}|\Psi\rangle$.*

Claim 12 Sim_3 *fulfils Property 11.*

Proof. By Claim 11, for any $i \in [q-2]$, $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$, $x, x' \in X$:

$$\overline{P_x^{(i+2)}} P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle = 0 \text{ and } P_x^{(i+2)} P_{x'}^{(i+1)} \overline{P_x^{(i)}} |\Psi\rangle = 0.$$

Since we show in the proof of Property 9 that for any $x \in X$ and $|\Psi\rangle \in V_{i-1}$, $P_x^{(i)}|\Psi\rangle, \overline{P_x^{(i)}}|\Psi\rangle \in \operatorname{span} V_i$ and using Claim 10, we can rewrite the equation above as

$$\overline{P_x^{(i+2)}} P_{x'}^{(i+2)} P_x^{(i)} |\Psi\rangle = 0 \text{ and } P_x^{(i+2)} P_{x'}^{(i+2)} \overline{P_x^{(i)}} |\Psi\rangle = 0.$$

And by Claim 6 and Claim 10, for any $x \in X$ and $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$: $P_x^{(i)}|\Psi\rangle = P_x^{(i+1)}|\Psi\rangle = P_x^{(i+2)}|\Psi\rangle$, therefore we can rewrite the equations above as

$$\bar{P}_x^{(i+2)} P_{x'}^{(i+2)} P_x^{(i+2)} |\Psi\rangle = 0 \text{ and } P_x^{(i+2)} P_{x'}^{(i+2)} \bar{P}_x^{(i+2)} |\Psi\rangle = 0.$$

For simplicity, we use the abbreviation $Q := P_x^{(i+2)}$ and $P := P_{x'}^{(i+2)}$. Now using Jordan's Lemma [Jor75], that says two orthogonal projectors are simultaneously block diagonalizable, we can write

$$P = \begin{pmatrix} P_1 & 0 & \cdots & 0 \\ 0 & P_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P_n \end{pmatrix}, \; Q = \begin{pmatrix} Q_1 & 0 & \cdots & 0 \\ 0 & Q_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Q_n \end{pmatrix}, \; |\Psi\rangle = \begin{pmatrix} \Psi_1 \\ \Psi_2 \\ \vdots \\ \Psi_n \end{pmatrix},$$

where P_i and Q_i are 1-by-1 matrices or rank-one 2-by-2 matrices. (We assume Ψ_i is 1-dimension vector when P_i and Q_i are 1-by-1 matrices and otherwise Ψ_i is 2-dimension vector.) Since $PQ\overline{P}|\Psi\rangle = 0$ and $\overline{P}QP|\Psi\rangle = 0$, we have for any $i \in [n]$, $P_i Q_i \overline{P_i}|\Psi_i\rangle = 0$ and $\overline{P_i} Q_i P_i |\Psi_i\rangle = 0$. We show that for any $i \in [n]$, $P_i Q_i |\Psi_i\rangle = Q_i P_i |\Psi_i\rangle$. The non-trivial case is when they are 2-by-2 matrices and it follows by Lemma 2 since they are rank-one and $\overline{Q_i} P_i Q_i |\Psi_i\rangle = 0$ and $Q_i P_i \overline{Q_i} |\Psi_i\rangle = 0$. We have proven:

$$\forall\ |\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3} :\ P_x^{(i+2)} P_{x'}^{(i+2)} |\Psi\rangle = P_{x'}^{(i+2)} P_x^{(i+2)} |\Psi\rangle.$$

By Claim 6, Claim 10, for any $x \in X$ and $|\Psi\rangle \in V_{i-1}^{\mathsf{Sim}_3}$, $P_x^{(i+2)}|\Psi\rangle = P_x^{(i)}|\Psi\rangle$, therefore

$$P_x^{(i+2)} P_{x'}^{(i)} |\Psi\rangle = P_{x'}^{(i+2)} P_x^{(i)} |\Psi\rangle,$$

and since for any $x \in X$, $P_x^{(i)}|\Psi\rangle \in \operatorname{span} V_i$ and using Claim 10 we can write

$$P_x^{(i+1)} P_{x'}^{(i)} |\Psi\rangle = P_{x'}^{(i+1)} P_x^{(i)} |\Psi\rangle.$$

□

Corollary 1 *For any $|\Psi\rangle \in \operatorname{span} V_{q-2}^{\mathsf{Sim}_3}$, x, x': $P_{x'}^{(q-1)} P_x^{(q-1)} |\Psi\rangle = P_x^{(q-1)} P_{x'}^{(q-1)} |\Psi\rangle$.*

Proof. By Claim 10 and Claim 12, it is clear that for any $|\Psi\rangle \in V_{q-2}^{\mathsf{Sim}_3}$, x, x': $P_{x'}^{(q-1)} P_x^{(q-1)} |\Psi\rangle = P_x^{(q-1)} P_{x'}^{(q-1)} |\Psi\rangle$. The result follows by the linearity of $P_x^{(q-1)}$.

□

Corollary 2 *For any $x_1, x_2, \ldots, x_{q-1} \in X$,*

$$P_{x_1}^{(q-1)} P_{x_2}^{(q-1)} \ldots P_{x_{q-1}}^{(q-1)} |\Phi\rangle = P_{\pi(x_1)}^{(q-1)} P_{\pi(x_2)}^{(q-1)} \ldots P_{\pi(x_{q-1})}^{(q-1)} |\Phi\rangle,$$

where π is a permutation on the set $\{x_1, \ldots, x_{q-1}\}$.

Proof. It is easy to show that any permutation π, the sequence $\pi(x_1)\pi(x_2)\dots\pi(x_{q-1})$ can be produced from the sequence $x_1\dots x_{q-1}$ only using the pairwise commutativity property of the elements of $\{x_1,\dots,x_{q-1}\}$. This can be shown by induction. First, we commute $x_j := \pi(x_1)$ to the beginning of the sequence $x_1\dots x_{q-1}$ and then use the induction hypothesis to the rest of the sequence. By Claim 10 and Equation 5, we can deduce that for any $x_1, x_2, \dots, x_{q-3} \in X$ and $j \leq q-3$, $P_{x_1}^{(q-1)} P_{x_2}^{(q-1)} \dots P_{x_j}^{(q-1)} |\Phi\rangle \in \operatorname{span} V_{j+1}$. Since for $j \leq q-3$, $\operatorname{span} V_{j+1} \subseteq \operatorname{span} V_{q-2}$, then the corollary holds using the pairwise commutativity property proved in 1 and the argument above. □

Due to the commutativity property proved in the corollary above 2, we can use the Conjecture 2 (with $q-1$ instead of t) in the following theorem.

Definition 6 *Let Sim_{sl} be a classical simulator that samples a bit-string $b_1 b_2 \dots b_N$ according to the distribution D defined in Conjecture 2. Then upon receiving the i-th classical query, it outputs the bit b_i as the answer.*

Claim 13 *The simulator Sim_{sl} is perfect for $\mathcal{D}_{cl}$.*

Proof. The distinguisher $\mathcal{D}_{cl}$ makes at most $q-1$ classical queries and the distribution D_I is the marginal of D for every I of size $q-1$, therefore Sim_{sl} is indistinguishable from Sim_3 for $\mathcal{D}_{cl}$. The result follows since Sim_3 is a perfect simulator for $\mathcal{D}_{cl}$. □

From the definitions of the distinguishers in the lines above, it is clear that $\mathbb{D}$ is finite-size.

4.1 Generalization to n-bit primitives

Let $F : [2^m] \to [2^n]$ be a function. We define the function $f : [2^m] \times [n] \to \{0,1\}$ as $f(x,i) = F(x)_i$ where $F(x)_i$ is the i-th bit of $F(x)$. Note that every construction $\mathcal{C}[F]$ can be implemented by f where every query, let say on input x, to F can be answered by n queries to f on inputs $(x,1),\dots,(x,n)$, i.e, it can be answered by $f(x,1)\|\dots\|f(x,n)$. We call the above implementation of $\mathcal{C}[F]$ by f, the construction $\mathcal{C}'[f]$.

Theorem 3 *If $\mathcal{C}[F]$ and H are perfectly quantum indifferentiable, then $\mathcal{C}'[f]$ and H are perfectly quantum indifferentiable.*

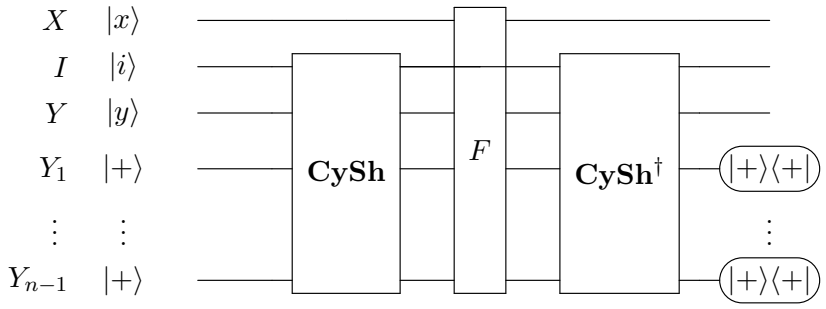
Proof. Fix a quantum distinguisher $\mathcal{D}$ that wants to differentiate $\mathcal{C}'[f]$ from H. We show that there exists a simulator Sim such that:

$$|\Pr[\mathcal{D}(\overline{\mathcal{C}'[f]}, f) = 1] - \Pr[\mathcal{D}(\overline{H}, \mathsf{Sim}(H)) = 1]| = 0. \tag{7}$$

Let $\mathcal{D}'$ be a quantum distinguisher that runs $\mathcal{D}$ and answers to its queries as follows:

- For any classical query of $\mathcal{D}$ to $\mathcal{C}'[f]$, it forwards the query to its oracle and then forwards back the answer to $\mathcal{D}$.
- For any quantum query of $\mathcal{D}$, using registers XIY to f, it prepares $n-1$ ancillary wires $Y_1,\dots,Y_{n-1}$ containing $|+\rangle$, then it applies the unitary **CySh** that maps $|i,y,y_1,\dots,y_{n-1}\rangle$ to $|i,y_1,\dots,y_{i-1},y,y_{i-1},\dots y_{n-1}\rangle$, it queries F, undoes the unitary **CySh**, and then measures

the $Y_1, \ldots, Y_{n-1}$ in $\{|+\rangle, |-\rangle\}$ (all the measurement outcomes are $|+\rangle$ with probability 1), it sends back XIY to $\mathcal{D}$. The following circuit shows how $\mathcal{D}'$ handles $\mathcal{D}$'s queries.



- Finally, it returns the output of $\mathcal{D}$.

Note that it is clear that $\Pr[\mathcal{D}'(\overline{\mathcal{C}[F]}, F) = 1] = \Pr[\mathcal{D}(\overline{\mathcal{C}'[f]}, f) = 1]$. By perfect quantum indifferentiability of $\mathcal{C}[F]$ and H, there exists a simulator Sim' such that $\Pr[\mathcal{D}'(\overline{\mathcal{C}[F]}, F) = 1] = \Pr[\mathcal{D}'(\overline{H}, \mathsf{Sim}'(H)) = 1]$. Now, we show that there exists a simulator Sim such that $\Pr[\mathcal{D}'(\overline{H}, \mathsf{Sim}'(H)) = 1] = \Pr[\mathcal{D}(\overline{H}, \mathsf{Sim}(H)) = 1]$. Let Sim be a simulator such that for any quantum query of $\mathcal{D}$, using registers XIY to f, it prepares $n-1$ ancillary wires $Y_1, \ldots, Y_{n-1}$ containing $|+\rangle$, then it applies the unitary **CySh**, it queries Sim', undoes the unitary **CySh**, and then measures the $Y_1, \ldots, Y_{n-1}$ in $\{|+\rangle, |-\rangle\}$ (all the measurement outcomes are $|+\rangle$ with probability 1), it sends back XIY to $\mathcal{D}$. Therefore,

$$\Pr[\mathcal{D}(\overline{\mathcal{C}'[f]}, f) = 1] = \Pr[\mathcal{D}(\overline{H}, \mathsf{Sim}(H)) = 1].$$

□

In the following, we write the generalization of the main result of the previous section, Theorem 2.

Theorem 4 *If two construction $\mathcal{C}[F]$ and H are perfectly quantum indifferentiable then for any classical "one-sided" distinguisher $\mathcal{D}_{cl}$ (cl stands for classical), there exists a stateless simulator Sim_{sl} (sl stands for stateless) such that*

$$|\Pr[\mathcal{D}_{cl}(\overline{\mathcal{C}'[f]}, \overline{f}) = 1] - \Pr[\mathcal{D}_{cl}(\overline{H}, \overline{\mathsf{Sim}_{sl}(H)}) = 1]| = 0.$$

Proof. If two construction $\mathcal{C}[F]$ and H are perfectly quantum indifferentiable then by Theorem 3, the construction $\mathcal{C}'[f]$ and H are perfectly quantum indifferentiable and consequently by Theorem 2, we can conclude for any classical distinguisher $\mathcal{D}_{cl}$, there exists a stateless simulator Sim_{sl} such that

$$|\Pr[\mathcal{D}_{cl}(\overline{\mathcal{C}'[f]}, \overline{f}) = 1] - \Pr[\mathcal{D}_{cl}(\overline{H}, \overline{\mathsf{Sim}_{sl}(H)}) = 1]| = 0.$$

□

5 Quantum indifferentiability of constructions

In this section, we construct a classical distinguisher that can differentiate the real case from the ideal case if we only consider a stateless simulator.

Construction of $\mathcal{D}_{cl}$. The distinguisher $\mathcal{D}_{cl}$ that wants to distinguish $(\mathcal{C}'[f], f)$ from $(H, \mathsf{Sim}_{sl}(H))$ picks a random element x from the domain. Then it evaluates $\mathcal{C}'[f](x)$ without querying x to the

public interface of the construction and only using queries to f (this is possible since the construction has been built from f). We call this value y. Then it queries x to the public interface of the construction to get $\mathcal{C}'[f](x)$. Finally, it outputs 1 if $y = \mathcal{C}'[f](x)$ and 0 otherwise. It is clear that in the real case, when $\mathcal{D}_{cl}$ interacts with $(\mathcal{C}'[f], f)$, the output of $\mathcal{D}_{cl}$ is 1 with probability 1. In the following lemma, we calculate an upper bound for the probability of outputting 1 in the ideal case.

Lemma 3 *Let $\mathbb{H}$ and $\mathbb{F}$ be some family of functions from $X \to Y$. $\mathbb{F}_h$ is a subset of $\mathbb{F}$ that depends on h. Then,*

$$\Pr[h(x) = f(x) : h \xleftarrow{\$} \mathbb{H}, \forall f \in \mathbb{F}_h, x \xleftarrow{\$} X] \leq \frac{|\mathbb{F}|}{|\mathbb{H}|}(d \cdot |X|^d \cdot |Y|^d) + (1 - \frac{d}{|X|}),$$

for any integer $d \leq |X|$.

Proof. Let $B_d^f := \{h : \ |\{x; h(x) \neq f(x)\}| \leq d\}$. Then,

$$|B_d^f| = \sum_{i=0}^{d} \binom{|X|}{i} (|Y| - 1)^i \leq d \cdot |X|^d \cdot |Y|^d.$$

$$\begin{aligned}
&\Pr[h(x) = f(x) : h \xleftarrow{\$} \mathbb{H}, \forall f \in \mathbb{F}_h, x \xleftarrow{\$} X] \\
&\quad = \Pr[h(x) = f(x) \wedge h \in B_d^f : h \xleftarrow{\$} \mathbb{H}, \forall f \in \mathbb{F}_h, x \xleftarrow{\$} X] \\
&\qquad + \Pr[h(x) = f(x) \wedge h \notin B_d^f : h \xleftarrow{\$} \mathbb{H}, \forall f \in \mathbb{F}_h, x \xleftarrow{\$} X] \\
&\quad = \Pr[h(x) = f(x) : h \xleftarrow{\$} \mathbb{H}, \forall f \in \mathbb{F}_h, x \xleftarrow{\$} X \mid h \in B_d^f] \cdot \Pr[h \in B_d^f : h \xleftarrow{\$} \mathbb{H}, \forall f \in \mathbb{F}_h] \\
&\qquad + \Pr[h(x) = f(x) : h \xleftarrow{\$} \mathbb{H}, \forall f \in \mathbb{F}_h, x \xleftarrow{\$} X \mid h \notin B_d^f] \cdot \Pr[h \notin B_d^f : h \xleftarrow{\$} \mathbb{H}, \forall f \in \mathbb{F}_h] \\
&\quad \leq 1 \cdot \frac{|\mathbb{F}||B_d^f|}{|\mathbb{H}|} + (1 - \frac{d}{|X|}) \cdot 1 \\
&\quad \leq \frac{|\mathbb{F}|}{|\mathbb{H}|}(d \cdot |X|^d \cdot |Y|^d) + (1 - \frac{d}{|X|})
\end{aligned}$$

□

5.1 Application of the attack

We use the classical distinguisher $\mathcal{D}_{cl}$ and the Lemma 3 to show that the sponge and Feistel constructions are not perfectly quantum indifferentiable.

Sponge Construction. The classical indifferentiability of the sponge construction has been studied in [BDPA08]. They prove that the sponge construction, $\mathcal{SP}(F) : \mathbf{Z}_2^{r*} \to \mathbf{Z}_2^{\infty}$, where $F : \{0,1\}^{r+c} \to \{0,1\}^r \times \{0,1\}^c$ is a random transformation or a random permutation, is indifferentiable from a random oracle. We recall the definition of the sponge construction to show that it is not **perfectly quantum** indifferentiable from a random oracle.

Definition 7 *The sponge construction $\mathcal{SP}(F)$ has two phases. The absorbing phase absorbs the input and the squeezing phase returns the output with desired size.*

1. ***Absorbing phase.*** *On the input $(M_1, \ldots, M_k)$ where each M_i is of size r bits: (For simplicity, we assume that the input size is a multiple of r.)*
   Let $\mathcal{SP}_1^{ab} := F(M_1 \| 0^c)$. For $i = 2, \ldots, k$: compute $\mathcal{SP}_i^{ab} := F(\mathcal{SP}_{i-1}^{ab} \oplus M_i \| 0^c)$. Return $\mathcal{SP}_k^{ab}$.

2. ***Squeezing phase.*** *Assume that the desired output size is M_{out} bits. Let $\mathcal{SP}_1^{sq} := F(\mathcal{SP}_k^{ab})$. For $j = 2, \ldots, \lceil M_{out}/r \rceil$: compute $\mathcal{SP}_j^{sq} := F(\mathcal{SP}_{j-1}^{sq})$. Return the first r bits of $\mathcal{SP}_j^{sq}$, for $j = 1, \ldots, \lceil M_{out}/r \rceil$. (the extra bits will be discarded.)*

Let consider $\mathcal{SP}(F) : \mathbf{Z}_2^{rk} \to \mathbf{Z}_2^{rk'}$ for some integers k, k', where $F : \{0,1\}^{r+c} \to \{0,1\}^r \times \{0,1\}^c$ is a random transformation. Let $\mathbb{H}$ be the set of all functions from $\mathbf{Z}_2^{rk} \to \mathbf{Z}_2^{rk'}$ and $\mathbb{F}$ be the set of all possible constructions $\mathcal{SP}(F) : \mathbf{Z}_2^{rk} \to \mathbf{Z}_2^{rk'}$ when F is a random function. Then,

$$|\mathbb{H}| = (2^{k'r})^{2^{kr}} (= |Y|^{|X|}) \text{ and } |\mathbb{F}| = (2^{r+c})^{2^{r+c}}.$$

According to the application of the sponge construction, $\frac{\log|X|}{\log|Y|}$ can be ≤ 1 or ≥ 1. Let first assume $\frac{\log|X|}{\log|Y|} \geq 1$. We use the bound in Lemma 3 assuming $d = \frac{|X|}{\delta}$ where $\delta = 4\frac{\log|X|}{\log|Y|} = \frac{4k}{k'}$. Since $\delta \geq 4$,

$$\frac{|X|^d |Y|^d}{|\mathbb{H}|} = \frac{|Y|^{\frac{\log|X|}{\log|Y|}d} |Y|^d}{|Y|^{|X|}} \leq \frac{|Y|^{\frac{|X|}{4}} |Y|^{\frac{|X|}{4}}}{|Y|^{|X|}} \leq \frac{1}{|Y|^{\frac{|X|}{2}}},$$

and we can get the upper bound

$$(\frac{2^{kr}k'r}{4kr})(\frac{(2^{r+c})^{2^{r+c}}}{(2^{rk'})^{2^{rk-1}}}) + (1 - \frac{k'}{4k}).$$

Therefore,

$$\varepsilon := |\Pr[\mathcal{D}_{cl}(\mathcal{SP}[F], F) = 1] - \Pr[\mathcal{D}_{cl}(H, \mathsf{Sim}_{sl}) = 1]| \geq 1 - \big(\frac{k'2^{rk}(2^{r+c})^{2^{(r+c)}}}{4k(2^{rk'})^{2^{rk-1}}} + (1 - \frac{k'}{4k})\big).$$

In order to obtain a lower bound for B, we assume the following bounds:
(a) $\log(k') \leq (r+c) \cdot 2^{r+c}$
(b) $rk \leq (r+c) \cdot 2^{r+c}$
(c) $r + c + \log(r+c) + 4 \leq rk$
Then looking at the first summand:

$$\begin{aligned}
\frac{k'2^{rk}(2^{r+c})^{2^{(r+c)}}}{4k(2^{rk'})^{2^{rk-1}}} &\leq \frac{k' \cdot 2^{rk} \cdot 2^{(r+c)\cdot 2^{r+c}}}{2^{2^{rk-1}}} = \frac{2^{\log k'} \cdot 2^{rk} \cdot 2^{2^{r+c+\log(r+c)}}}{2^{2^{rk-1}}} \\
&\overset{(*)}{\leq} \frac{2^{2^{r+c+\log(r+c)}} \cdot 2^{2^{r+c+\log(r+c)}} \cdot 2^{2^{r+c+\log(r+c)}}}{2^{2^{rk-1}}} \\
&\leq \frac{2^{2^{r+c+\log(r+c)+2}}}{2^{2^{rk-2}+2^{rk-2}}} \overset{(**)}{\leq} \frac{2^{2^{rk-2}}}{2^{2^{rk-2}} \cdot 2^{2^{rk-2}}} = \frac{1}{2^{2^{rk-2}}}
\end{aligned}$$

where $(*)$ uses (a), (b), and $(**)$ uses (c).Therefore,

$$\varepsilon \geq 1 - \big(\frac{1}{2^{2^{rk-2}}} + (1 - \frac{k'}{4k})\big) \geq \frac{k'}{4k} - \frac{1}{2^{2^{rk-2}}}.$$

When $\frac{\log|X|}{\log|Y|} \leq 1$, then by defining $\delta := 4$ we can have the bound:

$$\varepsilon \geq 1 - \big(\frac{1}{2^{2^{rk-2}}} + (1 - \frac{1}{4})\big) \geq \frac{1}{4} - \frac{1}{2^{2^{rk-2}}}.$$

Feistel Networks. In [DS16], they prove an 8-round Feistel network is indifferentiable from a random permutation where the underlying functions are random oracles. The definition of a r-round Feistel construction is presented in the following.

Definition 8 *Let $f_1, \ldots, f_r : \{0,1\}^n \to \{0,1\}^n$ be some functions. $\mathcal{FS}[f_i]_{i=1}^r : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is a permutation such that for any $L_0, R_0 \in \{0,1\}^n$,*

$$\mathcal{FS}[f_i]_{i=1}^r(L_0, R_0) = (L_r, R_r),$$

where (L_r, R_r) is calculated by the sequence $L_i = R_{i-1}$ and $R_i = f_i(R_{i-1}) \oplus L_{i-1}$ for $i = 1, \cdots, r$.

Let $\mathbb{F}$ be the set of all possible c-round Feistel networks and $\mathbb{H}$ be number of all permutations on $\{0,1\}^{2n}$. Then,

$$|\mathbb{H}| = (2^{2n})! \text{ and } |\mathbb{F}| = 2^{nc2^n}.$$

Using the bound in Lemma 3 ,

$$\varepsilon := |\Pr[\mathcal{D}_{cl}(\mathcal{SP}[F], F) = 1] - \Pr[\mathcal{D}_{cl}(H, \mathsf{Sim}_{sl}) = 1]| \geq 1 - (\frac{d2^{nc2^n}2^{4dn}}{(2^{2n})!} + (1 - \frac{1}{2^{2n}})^d)$$

Assuming $d = \frac{|X|}{8}$, $n \geq 3$ and $c \leq 2^n - n$:

$$\begin{aligned}
\frac{d2^{nc2^n}2^{4dn}}{(2^{2n})!} + (1 - \frac{d}{2^{2n}}) &\leq \frac{2^{2^{2n-3}}2^{nc2^n}2^{n2^{2n-1}}}{(2^{2n})!} + 7/8 \\
&\leq \frac{2^{2^{2n-3}}2^{nc2^n}2^{n2^{2n-1}}}{(2^{2n})^{2n}e^{-n}2^n} + 7/8 \\
&\leq \frac{1}{(2^{2n-2})^{2^{2n}}} \cdot \frac{2^{2^{2n-3}}e^n}{2^n(2^{2n-2})^{2^{2n}}} \cdot \frac{2^{nc2^n}}{(2^{2n-2})^{2^{2n}}} \cdot \frac{2^{n2^{2n-1}}}{(2^{2n-2})^{2^{2n}}} + 7/8 \\
&\leq \frac{1}{(2^{2n-2})^{2^{2n}}} + 7/8 \leq 1/2^{32} + 7/8 \leq 15/16
\end{aligned}$$

Therefore,

$$\varepsilon := |\Pr[\mathcal{D}_{cl}(\mathcal{SP}[F], F) = 1] - \Pr[\mathcal{D}_{cl}(H, \mathsf{Sim}_{sl}) = 1]| \geq 1/16.$$

The same counting argument can be applied to other constructions [CDMP05, DSSL16, ABD+13, DSST17].

Acknowledgments. Carstens, Ebrahimi, Tabia and Unruh were supported by institutional research funding IUT2-1 of the Estonian Ministry of Education and Research. Carstens, Ebrahimi, and Unruh were supported by the Estonian Centre of Exellence in IT (EXCITE) funded by ERDF. Carstens and Unruh were supported by the US Air Force AOARD grant "Verification of Quantum Cryptography" (FA2386-17-1-4022).

References

[ABD+13] Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger. On the indifferentiability of key-alternating ciphers. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 531–550. Springer, 2013.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun

Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

[BDPA08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In *EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 181–197. Springer, 2008.

[CBH+17] Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner, and Dominique Unruh. Post-quantum security of the sponge construction. *IACR Cryptology ePrint Archive*, 2017:771, 2017.

[CDMP05] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle-damgård revisited: How to construct a hash function. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 430–448. Springer, 2005.

[CHK+16] Jean-Sébastien Coron, Thomas Holenstein, Robin Künzler, Jacques Patarin, Yannick Seurin, and Stefano Tessaro. How to build an ideal cipher: The indifferentiability of the feistel construction. *J. Cryptology*, 29(1):61–114, 2016.

[DKT16] Dana Dachman-Soled, Jonathan Katz, and Aishwarya Thiruvengadam. 10-round feistel is indifferentiable from an ideal cipher. In Fischlin and Coron [FC16], pages 649–678.

[DS16] Yuanxi Dai and John P. Steinberger. Indifferentiability of 8-round feistel networks. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 95–120. Springer, 2016.

[DSSL16] Yevgeniy Dodis, Martijn Stam, John P. Steinberger, and Tianren Liu. Indifferentiability of confusion-diffusion networks. In Fischlin and Coron [FC16], pages 679–704.

[DSST17] Yuanxi Dai, Yannick Seurin, John P. Steinberger, and Aishwarya Thiruvengadam. Indifferentiability of iterated even-mansour ciphers with non-idealized key-schedules: Five rounds are necessary and sufficient. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 524–555. Springer, 2017.

[FC16] Marc Fischlin and Jean-Sébastien Coron, editors. *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*. Springer, 2016.

[Jor75] C. Jordan. In *Bulletin de la S. M. F.*, pages 3,103, 1875.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[MRH04] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2004.

[NIS14] NIST. SHA-3 standard: Permutation-based hash and extendable-output functions. Draft FIPS 202, 2014. Available at `http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf`.

[RSS11] Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. Careful with composition: Limitations of the indifferentiability framework. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 487–506. Springer, 2011.