Generalized Hybrid Search and Applications

Alexandru Cojocaru\textsuperscript{1}, Juan Garay\textsuperscript{2}, and Fang Song\textsuperscript{3}

\textsuperscript{1} QuICS, University of Maryland, USA.
\texttt{cojocaru@umd.edu}

\textsuperscript{2} Department of Computer Science and Engineering, Texas A&M University, USA.
\texttt{garay@tamu.edu}

\textsuperscript{3} Department of Computer Science, Portland State University, USA.
\texttt{fang.song@pdx.edu}

Abstract. In this work we examine the hardness of solving various search problems by hybrid quantum-classical strategies, namely, by algorithms that have both quantum and classical capabilities. Specifically, for search problems that are allowed to have multiple solutions and in which the input is sampled according to uniform or Bernoulli distributions, we establish their hybrid quantum-classical query complexities—i.e., given a fixed number of classical and quantum queries, determine what is the probability of solving the search task. At a technical level, our results generalize the framework for hybrid quantum-classical search algorithms recently proposed by Rosmanis [Ros22]. Namely, for an arbitrary distribution $D$ on Boolean functions, the probability that an algorithm equipped with $\tau_c$ classical queries and $\tau_q$ quantum queries succeeds in finding a preimage of 1 for a function sampled from $D$ is at most $\nu_D \cdot (2\sqrt{\tau_c} + 2\tau_q + 1)^2$, where $\nu_D$ captures the average (over $D$) fraction of preimages of 1.

As applications of our results, we first revisit and generalize the formal security treatment of the Bitcoin protocol called the Bitcoin backbone [Eurocrypt 2015], to a setting where the adversary has both quantum and classical capabilities, presenting a new hybrid honest majority condition necessary for the protocol to properly operate. Secondly, we re-examine the generic security of hash functions [PKC 2016] against quantum-classical hybrid adversaries.
1 Introduction

The query model is an elegant abstraction and is widely adopted in cryptography. A notable example is the random oracle (RO) model [BR93], where a hash function $f$ is modeled as a random black-box function, and all parties including the adversary can evaluate it only by issuing a query $x$ and receiving $f(x)$ in response. Numerous cryptosystems have been designed and analyzed in the random oracle model (e.g., [BR94, BR96, Sho01, FOPS04, FO13]).

Quantum computing brings about a new quantum query model, where superposition queries to the hash function $f$ are permitted in the form of $\sum_{x,y} \alpha_{x,y} |x\rangle |y\rangle \rightarrow \sum_{x,y} \alpha_{x,y} |x\rangle |y \oplus f(x)\rangle$. This equips quantum adversaries with new capabilities. Indeed, some classically secure digital signature and public-key encryption schemes are broken in the quantum random oracle (QRO) model, where a quantum adversary makes superposition queries to $f$ [YZ21]. A significant amount of effort has been devoted to address such quantum-query adversaries (cf., [BDF+11, ES15, Unr15, HHK17, AHU19, DFMS19, CMS19, ES20, DFMS22]) and often, in order to maintain security, we need to pay a considerable efficiency overhead, such as more complex constructions or larger key sizes.

The threat is alarming, but it also requires running a large-scale quantum computer coherently for a long time. The quantum devices available in the near-to-intermediate term are likely to be computationally restricted as well as expensive [Pre18]. This reality inspires a hybrid query model, where one is granted a quota of both classical queries and quantum queries, a model which subsumes classical and fully quantum queries as special cases. Establishing a trade-off between classical and quantum queries allows us to give a more accurate estimation of security and hence optimized parameter choices of a cryptosystem depending on what resources are available to a (near-term) quantum adversary.

Recently, Rosmanis presented the first analysis of the basic unstructured search problem in the hybrid query model [Ros22], where given oracle function $f : X \rightarrow \{0,1\}$, one wants to find a “marked” input, i.e., $x$ with $f(x) = 1$. In fact, this problem has been extensively studied when all queries are quantum. Grover’s quantum algorithm [Gro96] shows a quadratic speedup over classical algorithms, which is also proven optimal [BBBV97]. The generalized search version, when there are multiple marked inputs or they are randomly chosen, is also well understood [Zal99, DH09, Zha19]. Rosmanis’s work proves the hardness of searching in the domain of a function with a unique marked input $x^*$ in the hybrid query model and shows that for any quantum algorithm with $\tau_c$ classical queries and $\tau_q$ quantum queries, it succeeds in finding $x^*$ with probability at most $\frac{1}{|X|} \cdot (2\sqrt{\tau_c} + 2\tau_q + 1)^2$. This result also holds when $x^*$ is chosen at random, but other generalizations are unknown.
1.1 Our Contributions

In this paper we prove hardness of generalized search problems in the hybrid query model. We consider an arbitrary distribution $D$ on the function family $\mathcal{F} = \{ f : X \to \{0, 1\} \}$, and give a precise upper bound on the probability of finding a pre-image $x$ with $f(x) = 1$ when $f \leftarrow D$, for any quantum algorithm spending $\tau_c$ classical and $\tau_q$ quantum queries. Specifically,

$$\Pr_{f \leftarrow D}[f(x) = 1 : x \leftarrow A] \leq \nu_D \cdot (2\sqrt{\tau_c} + 2\tau_q + 1)^2,$$

where $\nu_D \triangleq \sup_{\|\varphi\|_2 \leq 1} \left( \mathbb{E}_{f \leftarrow D} \left\| \left( \sum_{x : f(x) = 1} |x\rangle \langle x| \right) \varphi \right\|_2^2 \right)$ captures the average fraction of preimages of 1, and is solely determined by the distribution $D$.

With our generalized bound, deriving hardness bounds for specific distributions becomes remarkably convenient. All we need to do is analyze $\nu_D$, and this usually can be done by a simple combinatorial argument. For instance, let $D$ be the uniform distribution over functions with exactly one marked input. Then we can observe that $\nu_D = \Pr_{f \leftarrow D}[f(x) = 1] = 1/|X|$ for an arbitrary $x$, which coincides with the result of Rosmanis [Ros22]. By a similar token, the hardness of searching a function with $w$ marked items can be obtained.

We further demonstrate our result on another distribution $D_\eta$, where each input is marked according to a Bernoulli trial. Namely, for every $x \in X$, we set $f(x) = 1$ independently. By determining $\nu_D$ in this case, we obtain the hardness of search in $f \leftarrow D_\eta$.

This search problem under $D_\eta$, which we call Bernoulli Search, is particularly useful in several cryptographic applications. Firstly, we can prove generic security bounds for hash function properties, such as preimage-resistance, second-preimage resistance and their multi-target extensions, against hybrid quantum-classical adversaries. This follows almost verbatim by plugging in our hybrid hardness bound of Bernoulli Search to the result of [HRS16], where the authors relate the hash properties to Bernoulli Search in the fully quantum query setting. In another application, Bernoulli search was shown to dictate the security of proofs of work (PoWs) and security properties of Bitcoin-like blockchains in the random oracle model (with fully quantum queries) [CGK+23]. This allows us to identify a new honest-majority condition under which the security of Bitcoin blockchain holds against hybrid adversaries with classical and quantum queries.

At a technical level, the proof of our hardness bound follows the overall strategy of [Ros22]. As in the standard optimality proof of Grover’s algorithm [BBBV97], one would consider running an adversary’s algorithm with respect to the input function $f \leftarrow D$ or a constant-0 function. Then one argues that each query diverges the states in these two cases, which is called a progress measure, by a small amount. On the other hand, in order to find a marked input in $f$, the
final states need to differ significantly. Therefore, sufficiently many queries are necessary for the cumulative progress to grow adequately.

Now, when classical queries are mixed with quantum queries, the quantum states would collapse after each classical query and it becomes unclear how to measure the progress. To address this, Rosmanis considers instead an intermediate oracle named pseudo-classical. Namely, consider a quantum query with the output register initialized in $|0\rangle$: $\sum_x \alpha_x |x\rangle|0\rangle \rightarrow \sum_x \alpha_x |x\rangle|f(x)\rangle$. We can then view a classical query as the result of measuring the input register that collapses to $x$ and receiving $f(x)$, whereas a pseudo-classical oracle measures the output register, resulting in one of two possible outcomes, $\sum_{x:f(x)=0} \alpha_x |x\rangle|0\rangle$ (denoted as the 0-outcome branch) or $\sum_{x:f(x)=1} \alpha_x |x\rangle|1\rangle$ (denoted as the 1-outcome branch). With this change, one instead tracks the progress between the 0-outcome branch in case of $f \leftarrow D$ and the state in case of the constant-0 function (which always stays in the 0-outcome branch). The algorithm fails if its state stays in the 0-outcome branch and is close to the state in the constant-0 case. A key ingredient in our proof is to deliberately separate the evolution of various objects on an individual function and what characteristics of the distribution $D$ influence the evolution and in what way. This enables us to obtain a clean and concise bound for the generalized hybrid search problem.

1.2 Organization of the Paper

The rest of the paper is organized as follows. The generalized search problem—which we term Distributional Search (Dist-Search)—with hybrid quantum-classical queries is presented in Section 2. The problem is defined in Section 2.1, its hardness is established in Section 2.2—the core of our technical contributions—and two case studies—Grover-like Search and Bernoulli Search—are presented in Section 2.3. Section 3 is dedicated to applications of the Bernoulli Search results, namely, the generic security of hash functions and the security of the Bitcoin blockchain against hybrid adversaries (Sections 3.1 and 3.2, respectively). We offer some conclusions and directions for future work in Section 4.

2 Distributional Search with Hybrid Strategies

2.1 The Distributional Search Problem

The problem we consider is to search a preimage of 1 in an arbitrarily distributed black-box function.

**Distributional Search Problem (Dist-Search)**

Let $D$ be an arbitrary distribution supported on the function family $\mathcal{F} := \{f : X \rightarrow \{0, 1\}\}$.

**Given:** Black-box access to function $f$ drawn from distribution $D$. 

3
Goal: Find $x$ such that $f(x) = 1$ if there exists such an $x$.

It is not surprising that the hardness of the problem is crucially influenced by the number of preimages of 1 on average under $D$; however, what is interesting about our study is that we can show a clean quantitative relation. Let $f : X \rightarrow \{0, 1\}$ be an arbitrary function. Define a projector on the space spanned by preimages of 1:

$$
\pi_f \overset{\text{def}}{=} \sum_{x : f(x) = 1} |x\rangle \langle x| \quad \text{and} \quad \Pi_f \overset{\text{def}}{=} \pi_f \otimes 1.
$$

Denote $\pi_f^\perp \overset{\text{def}}{=} I - \pi_f$ and $\Pi_f^\perp \overset{\text{def}}{=} I - \Pi_f$, and let $D$ be a distribution on $F$. We define the value that captures the average fraction of preimages of 1 as:

**Definition 1 ($\nu_D$).** The average fraction of preimages of 1 is defined as:

$$
\nu_D \overset{\text{def}}{=} \sup_{\|\varphi\| \leq 1} \left( \mathbb{E}_{f \leftarrow D} \|\pi_f \varphi\|^2 \right)
$$

where $\|\cdot\|$ is the Euclidean norm.

In this paper, we are able to establish the following bound for the success probability of solving Dist-Search, which constitutes our main result:

**Theorem 1 (Hardness of Dist-Search).** For any algorithm $A$ making up to $\tau_c$ classical queries and $\tau_q$ quantum queries, it holds that:

$$
\text{Succ}_{A,D} := \mathbb{P}_{f \leftarrow D} \left[ f(x) = 1 : x \leftarrow A \right] \leq \nu_D \cdot (2\sqrt{\tau_c} + 2\tau_q + 1)^2.
$$

Next, we turn to proving the above result.

### 2.2 Hardness of Dist-Search

#### 2.2.1 Preliminaries and Overview

We first formally describe an oracle function for the case of quantum and pseudo-classical queries.

**Definition 2 (Query Operators).** We define the following operators, which describe the actions of quantum and pseudo-classical oracles for a hybrid algorithm given a function $f$.

- A pseudo-classical oracle is described by

$$
P_{f,b} \overset{\text{def}}{=} \sum_{x : f(x) = b} |x\rangle \langle x| \otimes 1 \otimes |b\rangle
$$


A quantum oracle is described by

\[ Q_f \overset{\text{def}}{=} \sum_{x,b} |x\rangle\langle x| \otimes 1 \otimes |b\otimes f(x)\rangle\langle b| \]

Namely, on a pseudo-classical query, the two operators \( P_{f,0} = \Pi_f^\perp \otimes |0\rangle \) and \( P_{f,1} = \Pi_f \otimes |1\rangle \) correspond to the two possible measurement outcomes. It is more convenient to answer quantum queries by the corresponding phase oracle:

\[ Q_f \overset{\text{def}}{=} 1 - 2\Pi_f . \]

This can be seen as setting the output register of the standard oracle in \(|-\rangle\), and as a result, a quantum query flips the signs of the 1-preimages.

When running a hybrid query algorithm with \( f \), we will keep track of the (sub-normalized) pure state \( \psi_f^{(t)} \), which denotes the state of the algorithm on input \( f \) after \( t \) queries in the situation where every pseudo-classical query measures 0 (we will call this the 0-branch of \( A_f \)). Namely, consider an arbitrary algorithm with at most \( \tau \) queries (\( \tau_q \) quantum and \( \tau_c \) pseudo-classical) specified by a sequence of unitary operators\(^4\) \((U^{(0)}, U^{(1)}, \ldots, U^{(\tau)})\). Let \( T_c = \{ t : t\text{-th query is pseudo-classical} \} \) and \( T_q = \{ t : t\text{-th query is quantum} \} \). Then \( \psi_f^{(t)} \) is defined recursively by

\[
\psi_f^{(t)} = \begin{cases} 
U^{(t)} P_{f,0} \psi_f^{(t-1)}, & \text{if } t \in T_c; \\
U^{(t)} Q_f \psi_f^{(t-1)}, & \text{if } t \in T_q.
\end{cases}
\]

(2)

From this definition, the projection of \( \psi_f^{(t)} \) under \( \Pi_f^\perp \) characterizes the event that an algorithm fails to find a 1-preimage.

**Lemma 1.** For any algorithm \( A \), the failure probability of finding a 1-preimage of \( f \) after \( t \) queries is

\[ \delta_f^{(t)} = \Pr[f(x) \neq 1 : x \leftarrow A_f] \geq \left\| \Pi_f^\perp \psi_f^{(t)} \right\|^2 . \]

Hence, the failure probability with respect to distribution \( D \) satisfies

\[ \delta_D^{(t)} = \mathbb{E}_{f \leftarrow D} \delta_f^{(t)} \geq \mathbb{E}_{f \leftarrow D} \left\| \Pi_f^\perp \psi_f^{(t)} \right\|^2 . \]

Thus, our goal becomes lower-bounding \( \left\| \Pi_f^\perp \psi_f^{(t)} \right\| \). To do this, we consider running the same algorithm, but with a null function:

\[ f_\emptyset : x \mapsto 0, \forall x \in X . \]

\(^4\) Dimensions may grow depending on the arrangement of the pseudo-classical queries.
In this case, a quantum query is equivalent to applying identity (denoted $Q_0 \overset{\text{def}}{=} 1$), and a pseudo-classical query does not tamper the input state either but just appends $|0\rangle$. To be precise, we define

$$P_{0,0} \overset{\text{def}}{=} 1 \otimes |0\rangle,$$

and at each step $t \geq 0$, the state of the algorithm denoted by $\phi^{(t)}$ can be described as:

$$\phi^{(t)} = \begin{cases} U^{(t)} P_{0,0} \phi^{(t-1)}, & \text{if } t \in T_c; \\ U^{(t)} \phi^{(t-1)}, & \text{if } t \in T_q. \end{cases}$$

Without loss of generality we assume initially $\psi^{(0)} = \phi^{(0)} = |0\rangle$, and hence $\|\Pi_f^+ \psi_f^{(0)}\| = \|\Pi_f^+ \phi^{(0)}\| = 1$. In order to succeed, algorithm $A_f$ needs to move $\psi_f^{(t)}$ away from the kernel of $\Pi_f^+$ or reduce its norm. This motivates defining the progress measures below.

**Definition 3 (Progress Measures $(A^{(t)}, B^{(t)})$).** For any function $f$ and $t \geq 0$, define

$$A^{(t)}_f \overset{\text{def}}{=} \left| \langle \phi^{(t)}, \psi_f^{(t)} \rangle \right|^2, \quad B^{(t)}_f \overset{\text{def}}{=} \left\| \psi_f^{(t)} \right\|^2 - \left| \langle \phi^{(t)}, \psi_f^{(t)} \rangle \right|^2.$$

Given a distribution $D$ on $\mathcal{F}$, define the expected progress measures by

$$A^{(t)}_D \overset{\text{def}}{=} \mathbb{E}_{f \leftarrow D} \left( A^{(t)}_f \right), \quad B^{(t)}_D \overset{\text{def}}{=} \mathbb{E}_{f \leftarrow D} \left( B^{(t)}_f \right).$$

Notice that:

$$A^{(t)}_f + B^{(t)}_f = \left\| \psi_f^{(t)} \right\|^2, \quad A^{(0)}_f = 1, \quad B^{(0)}_f = 0.$$

We will show that $A^{(t)}_D - B^{(t)}_D$ essentially lower bounds the failure probability $\delta^{(t)}_D$ (Lemma 5). Hence, an algorithm’s objective would be to reduce $A^{(t)}_D$ and increase $B^{(t)}_D$. However, we can limit how much change can occur after $\tau$ queries (Proposition 1). This is by carefully analyzing the effect of each quantum or pseudo-classical query (Lemmas 7 and 8). Roughly speaking,

- A quantum query reduces $A^{(t)}_D$ by at most $4\sqrt{\nu_D \cdot B^{(t)}_D}$ and increases $B^{(t)}_D$ by the same amount (as a quantum query does not affect $\left\| \psi_f^{(t)} \right\|^2$);

- A pseudo-classical query increases $B^{(t)}_D$ by at most $\nu_D$, while a part $z^{(t)}$ of $B^{(t)}_D$ can also be spent to decrease $A^{(t)}_D$ by $\sqrt{\nu_D \cdot z^{(t)}}$. 


\[ \sum_{x, f(x) = 1} |x\rangle\langle x| \]

\[ \pi \otimes I \text{ (I on ancilla registers)} \]

\[ \delta_f \text{ Pr}[f(x) \neq 1 : x \leftarrow A^f] \text{ (Failure probability with f)} \]

\[ \delta_D \text{ E}_D\delta_f \text{ (Failure probability with f \leftarrow D)} \]

\[ \phi^{(0)} = \psi^{(0)} \text{ Initial state} \]

\[ \phi^{(t)} \text{ State after t-th query in } A^f \]

\[ \psi^{(t)} \text{ State on the 0-branch after t-th query in } A^f \]

\[ Q_f = I - 2\Pi_f \text{ (quantum oracle of f)} \]

\[ P_{f,0} = H_f \otimes |0\rangle \text{ (pseudo-classical oracle of f)} \]

\[ P_{f,1} = H_f \otimes |1\rangle \text{ (pseudo-classical oracle of f)} \]

\[ P_{\emptyset,0} = I \otimes |0\rangle \text{ (pseudo-classical oracle of } \emptyset) \]

\[ \gamma^{(t)} = \left\| H_f \phi^{(t)} \right\|^2 \]

\[ \gamma^{(t)} = \text{ E}_D(\gamma^{(t)}) \]

Table 1: Summary of variables and quantities used in our Dist-Search analysis.

2.2.2 Proof of Theorem 1

First off, we state the following simple fact on expectations which is used in multiple places of our analysis.

Lemma 2. Let Z be a discrete random variable. Let g(Z) and h(Z) be two non-negative functions. Then it holds that

\[ \mathbb{E}_Z \left( \sqrt{g(Z) \cdot h(Z)} \right) \leq \sqrt{\mathbb{E}_Z g(Z) \cdot \mathbb{E}_Z h(Z)}. \]

Proof. Let \( p_z := \text{Pr}(Z = z) \). By definition,

\[ \mathbb{E}_Z \left( \sqrt{g(Z) \cdot h(Z)} \right) = \sum_z p_z \sqrt{g(z)h(z)} \]

\[ = \sum_z \sqrt{p_z g(z) \cdot p_z h(z)} \]

\[ \leq \sqrt{\sum_z p_z g(z)} \cdot \sqrt{\sum_z p_z h(z)} \quad \text{(Cauchy-Schwarz)} \]

\[ = \sqrt{\mathbb{E}_Z g(Z)} \cdot \sqrt{\mathbb{E}_Z h(Z)}. \]

In multiple places of our analysis, it is helpful to consider a two-dimensional plane, which we now define explicitly.
Definition 4 (Useful 2-D Plane). For \( t \geq 0 \), let
\[
\phi_f^{(t)} = \frac{\Pi_f \phi^{(t)}}{\|\Pi_f \phi^{(t)}\|} = \Pi_f \phi^{(t)}/\sqrt{\gamma_f^{(t)}}, \quad \phi_f^{(t)\perp} = \frac{\Pi_f^\perp \phi^{(t)}}{\|\Pi_f^\perp \phi^{(t)}\|} = \Pi_f^\perp \phi^{(t)}/\sqrt{1 - \gamma_f^{(t)}},
\]
be the normalized vectors resulting of projecting \( \phi \) on the orthogonal subspaces spanned by \( 1 \) and \( 0 \) preimages of \( f \) respectively.

Let \( \Phi^{(t)} \) to be the 2-dimensional plane spanned by \( \{\phi_f^{(t)}, \phi_f^{(t)\perp}\} \). Then \( \phi_f^{(t)\perp} \) is identified as the normalized state perpendicular to \( \phi^{(t)} \) in \( \Phi^{(t)} \), i.e.,
\[
\phi_f^{(t)\perp} = \frac{\phi_f^{(t)}}{\sqrt{1 - \gamma_f^{(t)}}} - \phi_f^{(t)\perp} \sqrt{\gamma_f^{(t)}}.
\]
It is then useful to decompose \( \psi_f^t \) with respect to \( \Phi^{(t)} \).

Lemma 3 (Decomposition of \( \psi_f^{(t)} \) wrt \( \Phi^{(t)} \)). Let \( a \) and \( b \) be projecting \( \psi_f^{(t)} \) on the plane \( \Phi^{(t)} \) and then decomposing it under basis \( \{\phi, \phi^\perp\} \), and let \( c \) be the remaining component of \( \psi_f^{(t)} \) orthogonal to \( \Phi^{(t)} \), i.e., \( c \perp \Phi^{(t)} \). Then \( \psi_f^{(t)} \) can be expressed as \( \psi_f^{(t)} = a + b + c \) with
\[
a = \phi^{(t)} \sqrt{A_f^{(t)}}, \quad b = \omega \sqrt{B_f^{(t)} - \|c\|^2} \cdot \phi^{(t)\perp},
\]
where \( \omega \) is a complex phase (i.e., \( |\omega| = 1 \)) of the vector \( \psi_f^{(t)} - \langle \psi_f^{(t)}, \phi_f^{(t)\perp}\rangle \cdot \phi^{(t)} - c \).

As a result,
\[
\Pi_f^\perp \psi_f^{(t)} = \phi_f^{(t)\perp} \left( \sqrt{1 - \gamma_f^{(t)}} \sqrt{A_f^{(t)}} - \sqrt{\gamma_f^{(t)}} \cdot \omega \sqrt{B_f^{(t)} - \|c\|^2} \right) + c_f^t,
\]
with \( c_f^t := \Pi_f^\perp c \).

Lemma 4. For any fixed \( f \) and \( t \geq 0 \),
\[
\delta_f^{(t)} \geq A_f^{(t)} - \gamma_f^{(t)} - 2 \sqrt{\gamma_f^{(t)} \cdot B_f^{(t)}}.
\]

Proof. For convenience, we omit writing the superscript \( (t) \) in this proof. We first show that \( \|\pi_f^+ \psi_f\| \geq \sqrt{(1 - \gamma_f)A_f} - \sqrt{\gamma_f B_f} \). By Lemma 3, we have that
\[
\Pi_f^+ \psi_f = \phi_f^t \left( \sqrt{1 - \gamma_f} \sqrt{A_f} - \sqrt{\gamma_f} \cdot \omega \sqrt{B_f - \|c\|^2} \right) + c_f^t,
\]
with \( c_f^t := \pi_f^+ c \). Since \( c \perp \Phi \), it follows that
\[
\langle \phi_f^+, c_f^t \rangle = \langle \phi_f^+, \Pi_f^+ c \rangle = \langle \Pi_f^+ \phi_f^+, c \rangle = \langle \phi_f^+, c \rangle = 0.
\]
We can then obtain

$$\| \Pi_f^\perp \psi_f \| = \left| \sqrt{1 - \gamma_f} \cdot \sqrt{A_f} - \sqrt{\gamma_f} \cdot \omega \sqrt{B_f} - \| c \| \right| + \| c_f^\perp \|$$

Hence by choosing $c = 0, \omega = 1$, we get that

$$\| \Pi_f^\perp \psi_f \| \geq \sqrt{(1 - \gamma_f)A_f} - \sqrt{\gamma_f B_f}.$$ 

Therefore we can lower bound the failure probability

$$\delta_f \geq \| \Pi_f^\perp \psi_f \|^2$$ 

$$\geq (1 - \gamma_f)A_f - 2 \sqrt{(1 - \gamma_f)\gamma_f B_f}$$ 

$$\geq A_f - \gamma_f - 2 \sqrt{\gamma_f B_f} \quad (A_f, \gamma_f \leq 1)$$

Taking the expectation over $D$, we can express the failure probability with respect to the distribution.

**Lemma 5.** For any distribution $D$ and $t \geq 0$,

$$\delta_D^{(t)} \geq A^{(t)} - \gamma^{(t)} - 2 \sqrt{\gamma^{(t)} \cdot B^{(t)}}.$$ 

**Proof.**

$$\delta_D^{(t)} = \mathbb{E}_{f \sim D}(\delta_f^{(t)})$$

$$\geq \mathbb{E}_D(A_f^{(t)}) - \mathbb{E}_D(\gamma_f^{(t)}) - 2 \mathbb{E}_D(\sqrt{\gamma_f^{(t)} \cdot B_f^{(t)}}) \quad \text{(Linearity of expectation)}$$

$$\geq A^{(t)} - \gamma^{(t)} - 2 \sqrt{\mathbb{E}_D(\gamma_f^{(t)}) \cdot \mathbb{E}_D(B_f^{(t)})} \quad \text{(Lemma 2)}$$

$$= A^{(t)} - \gamma^{(t)} - 2 \sqrt{\gamma^{(t)} \cdot B^{(t)}}$$

We can also relate $\gamma^{(t)}$ to the value $\nu_D$ determined by the distribution $D$:

**Lemma 6.** For any $t \geq 0$ and any distribution $D$, we have: $\gamma^{(t)} \leq \nu_D$. 

9
Proof.

\[ \gamma^{(t)} := \mathbb{E}_{f \leftarrow D} \left\| \Pi_f \phi^{(t)} \right\|^2 = \mathbb{E}_{f \leftarrow D} \left\| (\pi_f \otimes \mathbb{1}) \phi^{(t)} \right\|^2 \]

We will use Schmidt decomposition for the state \( \phi^{(t)} \in \mathcal{H}_1 \otimes \mathcal{H}_2 \). Namely, Schmidt decomposition ensures that there exist orthonormal states \( \{|u_i\rangle\} \subset \mathcal{H}_1 \) for the first system and orthonormal states \( \{|v_i\rangle\} \subset \mathcal{H}_2 \) for the second system such that:

\[ \phi^{(t)} = \sum_i \alpha_i |u_i\rangle \otimes |v_i\rangle, \]

where \( \alpha_i \geq 0 \) such that \( \sum_i \alpha_i^2 = 1 \) (known as Schmidt coefficients). Then we can rewrite \( \gamma^{(t)} \) as:

\[
\begin{align*}
\gamma^{(t)} &:= \mathbb{E}_{f \leftarrow D} \left\| (\pi_f \otimes \mathbb{1}) \phi^{(t)} \right\|^2 = \mathbb{E}_{f \leftarrow D} \left\| (\pi_f \otimes \mathbb{1}) \left( \sum_i \alpha_i |u_i\rangle \otimes |v_i\rangle \right) \right\|^2 \\
&= \mathbb{E}_{f \leftarrow D} \sum_i \alpha_i^2 \left\| (\pi_f |u_i\rangle \otimes |v_i\rangle) \right\|^2 \quad (|v_i\rangle \text{ are orthogonal}) \\
&= \mathbb{E}_{f \leftarrow D} \sum_i \alpha_i^2 \|\pi_f |u_i\rangle\|^2 \cdot ||v_i\rangle|^2 \quad (\|a \otimes b\| = \|a\| \cdot \|b\|) \\
&= \sum_i \alpha_i^2 \mathbb{E}_{f \leftarrow D} \|\pi_f |u_i\rangle\|^2 \\
&\leq \sum_i \alpha_i^2 \nu_D \quad \text{(definition of } \nu_D) \\
&= \nu_D \sum_i \alpha_i^2 = \nu_D
\end{align*}
\]

\[ \square \]

**Proposition 1 (Bounding the Progress Measures).** After \( \tau = \tau_c + \tau_q \) queries,

\[
A^{(\tau)} \geq 1 - 4\nu_D \cdot (\sqrt{\tau_c} + \tau_q)^2, \quad B^{(\tau)} \leq \nu_D \cdot (\sqrt{\tau_c} + 2\tau_q)^2.
\]

As it turns out, proving Proposition 1 is the most involved step technically speaking. For the sake of modularity, we present the details separately in Section 2.2.3, and here we assume its validity and use it to prove Theorem 1.

**Proof of Theorem 1.** Assuming the bounds above on the two progress measures, we obtain that
\[ \delta^{(r)} \geq 1 - 4\gamma^{(r)} \cdot (\sqrt{\tau_c} + \tau_q)^2 - \gamma^{(r)} - 2\gamma^{(t)} \cdot (\sqrt{\tau_c} + 2\tau_q) \quad \text{(Proposition 1)} \]

\[ = 1 - \gamma^{(r)} \cdot (4(\sqrt{\tau_c} + \tau_q) + 2\sqrt{\tau_c} + 4\tau_q + 1) \]

\[ \geq 1 - \gamma^{(r)} \cdot (2(\sqrt{\tau_c} + \tau_q) + 1)^2 \quad (\tau_c \geq 0) \]

\[ \geq 1 - \nu_D \cdot (2\sqrt{\tau_c} + 2\tau_q + 1)^2 \quad (\gamma^{(r)} \leq \nu_D \text{ Lemma 6}) \]

Therefore,

\[ \text{Succ}_{A,D} \leq 1 - \delta^{(r)} \leq \nu_D \cdot (2\sqrt{\tau_c} + 2\tau_q + 1)^2. \]

\[ \square \]

### 2.2.3 Bounding the Progress Measures (Proposition 1)

Proposition 1 is proven via a series of steps. First, we consider a fixed function \( f \), and bound how much each query can possibly reduce \( A^{(t)}_f \) and increase \( B^{(t)}_f \).

**Lemma 7 (Progress Measures for a Fixed Function).** For every \( t \) the progress measures after the \( t+1 \)-th query satisfy the following recurrent relations:

- If the \( t+1 \)-th query is pseudo-classical, then there exists a sequence \( \left(z_f^{(t)}\right)_{t \geq 0} \), satisfying \( 0 \leq z_f^{(t)} \leq B_f^{(t)} \), such that:

  \[
  A_f^{(t+1)} \geq A_f^{(t)} - 2\sqrt{z_f^{(t)}} \cdot \sqrt{\gamma_f^{(t)}} \\
  B_f^{(t+1)} \leq B_f^{(t)} + \gamma_f^{(t)} - z_f^{(t)}
  \]

- If the \( t + 1 \)-th query is quantum, then:

  \[
  A_f^{(t+1)} \geq A_f^{(t)} - 4\gamma_f^{(t)} - 4\sqrt{B_f^{(t)}} \cdot \sqrt{\gamma_f^{(t)}} \\
  B_f^{(t+1)} \leq B_f^{(t)} + 4\gamma_f^{(t)} + 4\sqrt{B_f^{(t)}} \cdot \sqrt{\gamma_f^{(t)}}
  \]

**Proof.** We analyze the two cases separately.

**Pseudo-classical query case.** If the \( (t+1) \)-th query is pseudo-classical, according to the evolution of the state definition (Eq. (2)), the states after the \( t + 1 \) query are

\[
\psi_f^{(t+1)} = U^{(t+1)} P_{f,0}\psi_f^{(t)}, \quad \phi^{(t+1)} = U^{(t+1)} P_{0,0}\phi^{(t)}.
\]
Therefore, we have:
\[ A_f^{(t+1)} = |\langle \phi^{(t+1)}, \psi_f^{(t+1)} \rangle|^2 \]
\[ = |\langle P_{\theta,0}\phi^{(t)}, P_{f,0}\psi_f^{(t)} \rangle|^2 \]
\[ = |\langle \phi^{(t)}|0, \Pi_f^\perp \psi_f^{(t)}|0 \rangle|^2 \]
\[ = |\langle \phi^{(t)}, \Pi_f^\perp \psi_f^{(t)} \rangle|^2 \]

By the decomposition of \( \psi_f^{(t)} \) (Lemma 3), we know that:
\[ \Pi_f^\perp \psi_f^{(t)} = \phi_f^{(t)\perp} \left( \sqrt{1 - \gamma_f^{(t)}} \sqrt{A_f^{(t)}} - \sqrt{\gamma_f^{(t)}} \cdot \omega \sqrt{B_f^{(t)}} - \|c\|^2 \right) + c_f^{(t)} \],
where \(|\omega| = 1\) and \( c_f^{(t)} := \Pi_f^\perp c \) and \( c \perp \Phi = \text{span}\{\phi^{(t)}, \phi_f^{(t)\perp}\} \).

Note that \( \langle \phi^{(t)}, c_f^{(t)} \rangle = \langle \phi_f^{(t)\perp}, c_f^{(t)} \rangle = 0\) and \( \langle \phi^{(t)}, \phi_f^{(t)\perp} \rangle = \sqrt{1 - \gamma_f^{(t)}} \). As a result, we obtain:

\[ |\langle \phi^{(t)}, \Pi_f^\perp \psi_f^{(t)} \rangle|^2 = \left| \sqrt{1 - \gamma_f^{(t)}} \sqrt{A_f^{(t)}} - \sqrt{\gamma_f^{(t)}} \cdot \omega \sqrt{B_f^{(t)}} - \|c\|^2 \right|^2 \cdot (1 - \gamma_f^{(t)}) \]
\[ \geq (1 - \gamma_f^{(t)})^2 A_f^{(t)} - 2 \cdot \sqrt{\gamma_f^{(t)}} \cdot \sqrt{B_f^{(t)}} - \|c\|^2 \]
\[ \geq A_f^{(t)} - 2\gamma_f^{(t)} - 2 \cdot \sqrt{\gamma_f^{(t)}} \cdot \sqrt{B_f^{(t)}} - \|c\|^2. \]

Noting that \( \|c_f^{(t)}\|^2 = \|\Pi_f^\perp c\|^2 = \|c - \Pi_f c\|^2 \leq \|c\|^2\), we get:
\[ A_f^{(t+1)} \geq A_f^{(t)} - 2\gamma_f^{(t)} - 2 \cdot \sqrt{\gamma_f^{(t)}} \cdot \sqrt{B_f^{(t)}} - \|c_f^{(t)}\|^2 \]

Hence, by setting \( z_f^{(t)} \overset{\text{def}}{=} B_f^{(t)} - \|c_f^{(t)}\|^2 \in [0, B_f^{(t)}] \), we have that:
\[ A_f^{(t+1)} \geq A_f^{(t)} - 2\gamma_f^{(t)} - 2 \sqrt{z_f^{(t)}} \cdot \sqrt{\gamma_f^{(t)}}. \]

Next we analyze \( B_f^{(t+1)} \). By definition,
\[ B_f^{(t+1)} = \|\psi_f^{(t+1)}\|^2 - A_f^{(t+1)} \]
\[ = \|U^{(t+1)} P_{f,0} \psi_f^{(t)}\|^2 - A_f^{(t+1)} \]
\[ = \|\Pi_f^\perp \psi_f^{(t)}\|^2 - A_f^{(t+1)}. \]
Denote $E(t) \overset{\text{def}}{=} \sqrt{1 - \gamma_f(t)} \sqrt{A_f} - \sqrt{\gamma_f(t) \cdot c \cdot B_f} - \|c\|^2$. Observe that:

$$\| \Pi_f \psi_f(t) \|^2 = \| \phi_f \|^2 \cdot E(t) + \| c_f \|^2 = E(t) + \| c_f \|^2.$$ 

Meanwhile from above,

$$A_{f(t+1)} = |\langle \phi_f(t) \Pi_f \psi_f(t) \rangle|^2 = E(t)(1 - \gamma_f(t)).$$

Since $E(t) \leq A_f(t) + B_f(t) \leq 1$, we have that

$$B_f(t+1) = \| \Pi_f \psi_f(t+1) \|^2 - A_{f(t+1)} = E(t) + \| c_f \|^2 \leq B_f(t) + \gamma_f(t) - z_f(t).$$

where recall that the sequence $(z_f(t))$ is equal to $z_f(t) := B_f(t) - \| c_f \|^2 \in [0, B_f(t)]$.

**Quantum query case.** If the $(t+1)$-th query is quantum, according to the evolution of the state definition (Eq. (2)), the algorithm states after the $t+1$ query are:

$$\psi_f(t+1) = U(t+1) \psi_f(t) ; \quad \phi_f(t+1) = U(t+1) \phi_f(t).$$

where $U(t+1)$ is a unitary independent of input, and $Q_f = I - 2\Pi_f$.

Then, we have that:

$$\sqrt{A_f(t+1)} = |\langle \phi_f(t+1) \Pi_f \psi_f(t) \rangle| = |\langle \phi_f(t) U(t+1), U(t+1) \psi_f(t) \rangle| = |\langle \phi_f(t), Q_f \psi_f(t) \rangle| = |\sqrt{A_f(t)} - 2\langle \Pi_f \phi_f(t), \Pi_f \psi_f(t) \rangle|$$

By the decomposition of $\psi_f(t)$ (Lemma 3), we know that:

$$\psi_f(t) = \sqrt{A_f(t)} \cdot \phi_f(t) + \omega \sqrt{B_f(t)} - ||c||^2 \cdot \phi_f(t) + c$$

where $|\omega| = 1$ and $c \perp \Phi = \text{span}\{\phi_f(t), \phi_f(t)\}$. Then, we have:

$$\langle \Pi_f \phi_f(t), \Pi_f \psi_f(t) \rangle = \langle \Pi_f \phi_f(t), \sqrt{A_f(t)} \cdot \Pi_f \phi_f(t) + \omega \sqrt{B_f(t)} - ||c||^2 \cdot \Pi_f \phi_f(t) + \Pi_f c \rangle$$

$$= \sqrt{A_f(t)} \cdot \gamma_f(t) + \omega \sqrt{B_f(t)} - ||c||^2 \langle \Pi_f \phi_f(t), \Pi_f \phi_f(t) \rangle.$$
As for a quantum query we have:

$$H_f \phi^{(t)\perp} = H_f \left( \phi_f^{(t)} \sqrt{1 - \gamma_f^{(t)}} - \phi_f^{(t)\perp} \sqrt{\gamma_f^{(t)}} \right) = \sqrt{1 - \gamma_f^{(t)}} \phi_f^{(t)}$$

$$\langle H_f \phi^{(t)}, H_f \phi^{(t)\perp} \rangle = \langle \sqrt{\gamma_f^{(t)}} \phi_f^{(t)}, \sqrt{1 - \gamma_f^{(t)}} \phi_f^{(t)} \rangle = \gamma_f^{(t)} \cdot \sqrt{1 - \gamma_f^{(t)}}$$

As a result, we can rewrite $A_f^{(t+1)}$ as:

$$\sqrt{A_f^{(t+1)}} = \left| (1 - 2\gamma_f^{(t)}) \sqrt{A_f^{(t)}} - 2\omega \sqrt{B_f^{(t)}} - ||c||^2 : \sqrt{\gamma_f^{(t)}} \cdot \sqrt{1 - \gamma_f^{(t)}} \right|$$

Using the inequality $|a - b| \geq ||a| - |b|| \geq |a - b|$ for any $a, b$ complex numbers:

$$\sqrt{A_f^{(t+1)}} \geq \left| 1 - 2\gamma_f^{(t)} \right| \sqrt{A_f^{(t)}} - 2\omega \sqrt{B_f^{(t)}} - ||c||^2 \cdot \sqrt{\gamma_f^{(t)}} \cdot \sqrt{1 - \gamma_f^{(t)}}$$

Using that $\sqrt{A_f^{(t)}} \leq 1$ and the observation that if $x \geq a - b$, this implies that $x^2 \geq a(a - 2b)$ for any $a, b > 0$, we can determine the lower bound on $A_f^{(t+1)}$:

$$A_f^{(t+1)} \geq \left| 1 - 2\gamma_f^{(t)} \right| \sqrt{A_f^{(t)}} \cdot \left( \left| 1 - 2\gamma_f^{(t)} \right| \sqrt{A_f^{(t)}} - 4 \cdot \sqrt{\gamma_f^{(t)}} \sqrt{B_f^{(t)}} \right)$$

$$\geq \left( 1 - 2\gamma_f^{(t)} \right)^2 A_f^{(t)} - 4 \left| 1 - 2\gamma_f^{(t)} \right| \sqrt{\gamma_f^{(t)}} \sqrt{B_f^{(t)}}$$

$$\geq A_f^{(t)} - 4\gamma_f^{(t)} - 4\sqrt{\gamma_f^{(t)}} \sqrt{B_f^{(t)}}$$

As for a quantum query we have: $A_f^{(t+1)} + B_f^{(t+1)} = A_f^{(t)} + B_f^{(t)}$, we get:

$$B_f^{(t+1)} = A_f^{(t)} + B_f^{(t)} - A_f^{(t+1)} \leq A_f^{(t)} + B_f^{(t)} - A_f^{(t)} + 4\gamma_f^{(t)} + 4\sqrt{\gamma_f^{(t)}} \sqrt{B_f^{(t)}}$$

$$\leq B_f^{(t)} + 4\gamma_f^{(t)} + 4\sqrt{\gamma_f^{(t)}} \sqrt{B_f^{(t)}}$$

\[ \square \]

Lemma 8 (Progress Measures for Dist-Search). For every $t$, the progress measures after the $t + 1$-th query satisfy the following recurrent relations:

- If the $t + 1$-th query is pseudo-classical, there exists $z_t \in [0, B^{(t)}]$ s.t.:

  $$A^{(t+1)} \geq A^{(t)} - 2\nu_D - 2\sqrt{\nu_D} \cdot \sqrt{z_t}$$

  $$B^{(t+1)} \leq B^{(t)} - z_t + \nu_D$$

(5)
If the $t+1$-th query is quantum, then we have:

$$A^{(t+1)} \geq A^{(t)} - 4 \cdot \nu_D - 4 \cdot \sqrt{\nu_D} \cdot \sqrt{B^{(t)}}$$

$$B^{(t+1)} \leq B^{(t)} + 4 \cdot \nu_D + 4 \cdot \sqrt{\nu_D} \cdot \sqrt{B^{(t)}}$$ (6)

**Proof.** Letting $z_t \overset{\text{def}}{=} \mathbb{E}_{f \leftarrow D}(z^t_f)$, we can observe that $z_t \in [0, B(t)]$. Taking expectations over $D$, and applying Lemma 2 ($\mathbb{E}\sqrt{g(Z) \cdot h(Z)} \leq \sqrt{\mathbb{E}g(Z) \cdot \mathbb{E}h(Z)}$) and Lemma 6 ($\gamma(t) \leq \nu_D$), the relations for $A(t)$ and $B(t)$ follow.

Next, since we intend to lower bound $A(\tau)$ and upper bound $B(\tau)$, we can change the inequalities to equalities and analyze instead the new sequences $(a_t, b_t)$ defined below. It is clear that $A(\tau) \geq a_\tau$ and $B(\tau) \leq b_\tau$.

**Definition 5 (Sequences $(a_t)_{t \geq 0}, (b_t)_{t \geq 0}$).** We define the following sequences based on the evolution of the progress measures $A$ and $B$:

$$a_0 \overset{\text{def}}{=} A(0) = 1$$

$$b_0 \overset{\text{def}}{=} B(0) = 0$$

$$a_{t+1} \overset{\text{def}}{=} \begin{cases} a_t - 2 \cdot \nu_D - 2 \cdot \sqrt{\nu_D} \cdot \sqrt{z_t}, & \text{if } t+1 \in T_c \\ a_t - 4 \cdot \nu_D - 4 \cdot \sqrt{\nu_D} \cdot \sqrt{b_t}, & \text{if } t+1 \in T_q \end{cases}$$

$$b_{t+1} \overset{\text{def}}{=} \begin{cases} b_t + \nu_D - z_t, & \text{if } t+1 \in T_c \\ b_t + 4 \cdot \nu_D + 4 \cdot \sqrt{\nu_D} \cdot \sqrt{b_t}, & \text{if } t+1 \in T_q \end{cases}$$

where $(z_t)_{t \geq 1}$ is the sequence defined in the proof of Lemma 8, which satisfies $0 \leq z_t \leq B(t)$ for any $t$.

**Lemma 9 (Bounding $a_\tau$ and $b_\tau$).**

$$a_\tau \geq 1 - 4 \nu_D \cdot (\sqrt{\tau_c + 2\tau_q})^2, \quad b_\tau \leq \nu_D \cdot (\sqrt{\tau_c + 2\tau_q})^2.$$ (7)

**Proof.** The proof consists of four steps.

(1) First we show that $b_\tau \leq (\sqrt{\tau_c + 2\tau_q})^2 \cdot \nu_D$.

To get an upper bound for each term of this sequence, we can consider $z_t = 0$, and hence instead use the sequence:

$$d_{t+1} \overset{\text{def}}{=} \begin{cases} d_t + \nu_D, & \text{if } t+1 \in T_c \\ d_t + 4 \cdot \nu_D + 4 \cdot \sqrt{\nu_D} \cdot \sqrt{d_t}, & \text{if } t+1 \in T_q \end{cases}$$

As a result we have: $b_t \leq z_t$ for any $t \in [\tau]$. 

15
Our task is to determine the maximum value of the last term of the sequence, i.e. \( d_\tau \). We can see from the definition of \( d_t \) that every hybrid strategy that uses \( \tau_c \) classical queries and \( \tau_q \) quantum queries induces a sequence \((d_t)_\tau\). More concretely, we can write each such strategy \( A \) as a sequence of \( \tau \) bits, \( A = [x_1, \ldots, x_\tau] \), which indicate if the \( i \)-th query of the strategy \( A \) is classical or quantum. Namely if \( x_i = 0 \) this represents that the \( i \)-th query of \( A \) is classical and if \( x_i = 1 \) then the \( i \)-th query is quantum and we know that there are exactly \( \tau_c \) values of 0 and \( \tau_q \) values of 1. Therefore, the sequence \((d_t)_\tau\) parameterized by the strategy \( A \), denoted as \((d_t^A)_\tau\), can be re-written as:

\[
\begin{align*}
d_t^A \defeq & \begin{cases} 
\frac{d_t^A + \nu_D}{d_t^A + 4 \cdot \nu_D + 4 \cdot \sqrt{\nu_D} \cdot \sqrt{d_t^{-1}^A + \nu_D}}, & \text{if } x_{t+1} = 0 \\
\frac{d_t^B}{d_t^B + 4 \sqrt{\nu_D} \sqrt{d_t^{-1}^B}}, & \text{if } x_{t+1} = 1 
\end{cases}
\end{align*}
\]

With this representation in mind, our task reduced to determining the strategy \( A^* \) which achieves the maximum \( d_t^A \) over all possible strategies.

The starting point is the following observation. Let the following two strategies:

\[
\begin{align*}
A &= [x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_\tau] \quad \text{and} \\
B &= [y_1, \ldots, y_{i-1}, y_i, y_{i+1}, \ldots, y_\tau]
\end{align*}
\]

which only differ in the order between a classical query and a quantum query for the \( i \) and \( i+1 \)-th queries, namely: \( x_i = 0 \), \( x_{i+1} = 1 \) and \( y_i = 1 \), \( y_{i+1} = 0 \) and \( x_j = y_j \) for \( j \in \{1, \ldots, \tau\} \setminus \{i, i+1\} \). We will show next that the strategy \( A \) results in a greater last term than the last term in the strategy \( B \), namely: \( d_{t+1}^A > d_{t+1}^B \).

As \( x_1 = y_1, \ldots, x_{i-1} = y_{i-1} \), this implies directly that \( d_{i-1}^A = d_{i-1}^B \). Then for the \( i \)-th and \( i+1 \) terms of the two sequences we have:

\[
\begin{align*}
d_i^A &= d_{i-1}^A + \nu_D \\
d_i^B &= d_{i-1}^B + 4 \nu_D + 4 \sqrt{\nu_D} \sqrt{d_{i-1}^B}
\end{align*}
\]

Then, as \( d_{i-1}^A = d_{i-1}^B \) it is clear that \( d_i^A > d_i^B \). As \( x_j = y_j \) for all \( i+2 \leq j \leq \tau \), this also implies that \( d_{t+1}^A > d_{t+1}^B \), which concludes the claim.

Denote the following swap operation on strategies. Given as input a strategy \( A = [x_1, \ldots, x_i, x_{i+1}, \ldots, x_\tau] \) the function \( \text{swap}_i \) outputs a strategy \( A' \):

\[
\text{swap}_i(A) = A' \text{ where } A' = [x_1, \ldots, x_{i+1}, x_i, \ldots, x_\tau]
\]

Then, our previous observation implies that for a strategy \( A \) such that \( x_i = 0 \) and \( x_{i+1} = 1 \), we have: \( d^A_{t} > d^B_{t} \).

Let the strategy:

\[
A^* \defeq [0, \ldots, 0, 1, \ldots, 1].
\]

We claim that \( A^* \) is the strategy that achieves the maximum last term over all possible strategies. It is not hard to see that any strategy \( A = [x_1, \ldots, x_\tau] \) can be obtained from starting with \( A^* \) and applying a sequence of \( \text{swap}_i \) operations:

\[
A^* \defeq [0, \ldots, 0, 1, \ldots, 1] \xrightarrow{\text{swap}_{i_1}} \cdots \xrightarrow{\text{swap}_{i_k}} A \text{ for some indices } i_1, \ldots, i_k
\]
Applying the previous observation implies that for any strategy $A$, we have that $d^*_t \geq d^A_t$, which shows that $A^*$ is the optimal strategy. Now, let us compute the last term of the optimal strategy, i.e.: $d^*_A$. We can rewrite the sequence corresponding to this sequence as:

$$d^A_{t+1} = \begin{cases} 
  d^A_t + \nu_D, & \text{if } 0 \leq t < \tau_c \\  d^A_t + 4 \cdot \nu_D + 4 \cdot \sqrt{\nu_D} \cdot \sqrt{d^A_t} = \left(\sqrt{d^A_t} + 2 \sqrt{\nu_D}\right)^2, & \text{if } \tau_c \leq t < \tau 
\end{cases}$$

As $d^A_0 = 0$, it is clear that we have: $d^A_{\tau_c} = \tau_c \cdot \nu_D$. For $\tau_c \leq t \leq \tau$, we will prove by induction that:

$$d^A_t = \left(\sqrt{\tau_c} + 2(t - \tau_c)\right)^2 \cdot \nu_D$$

For the base case $t = \tau_c$, we already showed that $d^A_{\tau_c} = \tau_c \cdot \nu_D$. For the inductive step, we have that:

$$d^A_{t+1} = \left(\sqrt{\tau_c} + 2(t - \tau_c)\right)^2 \cdot \nu_D \quad \text{from induction hypothesis}$$

$$= \left(\sqrt{\tau_c} + 2(t - \tau_c + 1)\right) \cdot \nu_D$$

which concludes the inductive proof. Hence, by putting things together we have:

$$b_\tau \leq d_\tau \leq d^*_\tau = \left(\sqrt{\tau_c} + 2\tau_q\right)^2 \cdot \nu_D \quad (9)$$

(2) Secondly, we show that $\sum_{t \in T_q} \sqrt{b_{t-1}} \leq \sqrt{\nu_D} \cdot \tau_q \left(\sqrt{\tau_c} + \tau_q - 1\right)$.

As for $b_\tau$, to get an upper bound we let $z_t = 0$, and thus use the sequence $(d^A_t)_t$. From the definition of the sequence (Equation 8), it is clear that $(d^A_t)_t$ is a strictly increasing sequence for any strategy $A$. This also implies that for any strategy $A$ we have:

$$\sum_{t \in T_q} \sqrt{d^A_{t-1}} \leq \sum_{\tau_c \leq t \leq \tau} \sqrt{d^A_t}$$

In other words, $\sum_{t \in T_q} \sqrt{d^A_{t-1}}$ is maximized when the strategy performs first all $\tau_c$ classical queries and then the $\tau_q$ quantum queries. Hence, the maximum is achieved for the strategy described above by the sequence $(d^A_t)_t$. Using the previous result in Equation 9:

$$\sum_{\tau_c \leq t \leq \tau} d^A_t = \nu_D \cdot \sum_{\tau_c \leq t \leq \tau} \left(\sqrt{\tau_c} + 2(t - \tau_c)\right)^2$$

17
This gives us:

\[
\sum_{t \in T_q} \sqrt{b_t - 1} \leq \sum_{\tau_c \leq t \leq \tau} \sqrt{d_t^*} = \sqrt{\nu_D} \sum_{\tau_c \leq t \leq \tau} \sqrt{\tau_c + 2(t - \tau)}
\]

\[
\leq \sqrt{\nu_D} \left( \tau_q \left( \sqrt{\tau_c - 2}\tau_c \right) + 2 \sum_{\tau_c \leq t \leq \tau} t \right)
\]

\[
= \sqrt{\nu_D} \left( \tau_q \sqrt{\tau_c (1 - 2\sqrt{\tau_c} + 2\sqrt{\tau_c})} + 2 \cdot \frac{(\tau_q - 1)\tau_q}{2} \right)
\]

\[
= \sqrt{\nu_D} \tau_q (\sqrt{\tau_c} + \tau_q - 1)
\]

(3) Thirdly, we show that \(\sum_{t \in T_c} \sqrt{b_t - 1} \leq \sqrt{\nu_D} \cdot (\tau_c + 2\sqrt{\tau_c} \nu_q)\).

By definition of the sequence \(z_t\) (Def. 5), we know that for \(t \in T_c\):

\[
\sum_{t \in T_c} z_{t-1} = \nu_D \cdot \tau_c + \sum_{t \in T_c} (b_{t-1} - b_t)
\]

For the rest of the proof it hence suffices to derive an upper bound on \(\sum_{t \in T_c} (b_{t-1} - b_t)\). We can rewrite \(b_t\) as:

\[
b_t = b_0 + \sum_{i=1}^{\tau} (b_i - b_{i-1}) = \sum_{b_i \geq b_{i-1}} (b_i - b_{i-1}) + \sum_{b_i < b_{i-1}} (b_i - b_{i-1})
\]

As a result, we have that:

\[
\sum_{t \in T_c \land b_t < b_{t-1}} (b_t - b_{t-1}) < \sum_{b_t < b_{t-1}} (b_t - b_{t-1}) + \sum_{b_t \geq b_{t-1}} (b_t - b_{t-1}) - b_t
\]

In other words we also have:

\[
\sum_{t \in T_c \land b_t < b_{t-1}} (b_t - b_{t-1}) < \sum_{t \in T_c \land b_t \geq b_{t-1}} (b_t - b_{t-1}) + \sum_{t \in T_q \land b_t \geq b_{t-1}} (b_t - b_{t-1})
\]

For \(t \in T_q\), from the sequence definition (Def. 5), we have that \(b_t > b_{t-1}\), thus we can rewrite previous inequality as:

\[
\sum_{t \in T_c \land b_t < b_{t-1}} (b_t - b_{t-1}) < \sum_{t \in T_c \land b_t \geq b_{t-1}} (b_t - b_{t-1}) + 4\tau_q \cdot \nu_D + 4\sqrt{\nu_D} \sum_{t \in T_q} \sqrt{b_{t-1}}
\]

By applying step (2), we get:

\[
\sum_{t \in T_c \land b_t < b_{t-1}} (b_t - b_{t-1}) < \sum_{t \in T_c \land b_t \geq b_{t-1}} (b_t - b_{t-1}) + 4\nu_D \tau_q + 4\nu_D \tau_q (\sqrt{\tau_c} + \tau_q - 1)
\]
By subtracting the first sum from the right hand side we get:

$$\sum_{t \in T_c} z_{t-1} = \nu_D \cdot \tau_c + \sum_{t \in T_c} (b_{t-1} - b_t) < \nu_D \cdot (\tau_c + 4\tau_q^2 + 4\tau_q\sqrt{\tau_c})$$

Finally, by using the Cauchy-Schwarz inequality:

$$\sum_{t \in T_c} \sqrt{z_{t-1}} \leq \sqrt{\nu_D \cdot (\tau_c + 4\tau_q^2 + 4\tau_q\sqrt{\tau_c}) \cdot \sqrt{\tau_c}} \leq \sqrt{\nu_D \cdot (\tau_c + 2\tau_q\sqrt{\tau_c})}$$

(4) In the final step, we show that \(a_T \geq 1 - 4\nu_D(\sqrt{\tau_c} + \tau_q)^2\).

From the definition of \(a_t\) (Def. 5):

$$a_T = a_0 + \sum_{t=1}^{\tau} (a_t - a_{t-1})$$

$$= 1 - \sum_{t \in T_c} (2\nu_D + 2\sqrt{\nu_D} \cdot \sqrt{z_{t-1}}) - \sum_{t \in T_q} \left(4\nu_D + 4\sqrt{\nu_D} \cdot \sqrt{b_{t-1}}\right)$$

$$= 1 - 2\tau_c \nu_D - 4\tau_q \nu_D - 2\sqrt{\nu_D} \sum_{t \in T_c} \sqrt{z_{t-1}} - 4\sqrt{\nu_D} \sum_{t \in T_q} \sqrt{b_{t-1}}$$

Using the bounds derived in steps (2) and (3), we get:

$$a_T \geq 1 - 2\tau_c \nu_D - 4\tau_q \nu_D - 2\nu_D \cdot (\tau_c + 2\sqrt{\tau_c} \tau_q) - 4\nu_D \cdot \tau_q (\sqrt{\tau_c} + \tau_q - 1)$$

$$= 1 - 4\nu_D(\sqrt{\tau_c} + \tau_q)^2$$

2.3 Case Studies

In this section, we will apply our main result to two common function distributions. As a common ingredient, it will be helpful to consider the following indicator random variable:

$$\text{I}_f^x \overset{\text{def}}{=} \begin{cases} 1 & \text{if } f(x) = 1; \\ 0 & \text{if } f(x) = 0, \end{cases}$$

for all \(f \in \mathcal{F}\) and \(x \in X\). Then, for a distribution \(D\),

$$\mathbb{E}_{f \leftarrow D}(\text{I}_f^x) = \Pr_{f \leftarrow D}[f(x) = 1].$$
2.3.1 Grover-like Search

The first interesting case is a general Grover-type search. We consider a distribution $D_w$ which is uniform over functions that exactly map $w$ inputs to 1. In other words, drawing $f \leftarrow D_w$ is equivalent to sampling a subset $S \subseteq X$ with $|S| = w$ uniformly at random and set $f(x) = 1$ if and only if $x \in S$. We consider the resulting multi-uniform search problem:

**Multi-Uniform Search**

**Given:** $f \leftarrow D_w$, which maps a uniform size-$w$ subset to 1.

**Goal:** Find $x$ such that $f(x) = 1$.

**Theorem 2.** For any adversary $A$ making up to $\tau_c$ classical queries and $\tau_q$ quantum queries,

$$\text{Succ}_{A, D_w} \leq \frac{w}{M} \cdot (2\sqrt{\tau_c} + 2\tau_q + 1)^2,$$

where $M = |X|$ is the domain size.

**Proof.** We just need to show that $\nu_D = \sup_{\|\varphi\| \leq 1} \mathbb{E}_{f \leftarrow D_w}(\|\pi_f \varphi\|^2) \leq \frac{w}{M}$ in this case. Consider an arbitrary unit vector $\varphi = \sum_x \alpha_x |x\rangle$ with $\sum_x |\alpha_x|^2 = 1$.

$$\mathbb{E}_{f \leftarrow D_w}(\|\pi_f \varphi\|^2) = \mathbb{E}_{f \leftarrow D_w} \left( \left| \sum_x \alpha_x \mathbbm{1}_f^x \right|^2 \right)$$

$$= \sum_x |\alpha_x|^2 \cdot \mathbb{E}_{f \leftarrow D_w}(\mathbbm{1}_x^f)$$

$$= \sum_x |\alpha_x|^2 \cdot \Pr_{f \leftarrow D_w}[f(x) = 1]$$

$$= \frac{w}{M}.$$

We note two special scenarios. When $w = 1$, this reproduces Rosmanis’s result [Ros22], and when $\tau_c = 0$, our result reproduces the fully quantum query complexity of Grover search with multiple marked items (cf. [BBBV97, Zal99]).

2.3.2 Bernoulli Search

The second interesting case is what we call a Bernoulli distribution $D_\eta$ on $\mathcal{F}$, as specified below:

**Bernoulli Search**

**Given:** $f \leftarrow D_\eta$ drawn via the following sampling procedure:
For each $x \in X$, independently set
\[ f(x) = \begin{cases} 1, & \text{with probability } \eta \\ 0, & \text{otherwise} \end{cases}. \]

**Goal:** Find $x$ such that $f(x) = 1$.

**Theorem 3.** For any adversary $A$ making up to $\tau_c$ classical queries and $\tau_q$ quantum queries,
\[ \text{Succ}_{A,D_\eta} \leq \eta \cdot (2\sqrt{\tau_c} + 2\tau_q + 1)^2. \]

**Proof.** Consider an arbitrary unit vector $\varphi = \sum_x \alpha_x |x\rangle$ with $\sum_x |\alpha_x|^2 = 1$. Again, we just need to show that $E_{f \sim D_\eta}(\|\pi f \varphi\|^2) \leq \eta$. Similarly as above,
\[ E_{f \sim D_\eta}(\|\pi f \varphi\|^2) = \sum_x |\alpha_x|^2 \cdot \Pr_{f \sim D_\eta}[f(x) = 1] = \eta. \]

Note that when $\tau_c = 0$, this bound reproduces the complexity of Bernoulli search using fully quantum queries (cf. [HRS16, ARU14]).

3 Applications of Bernoulli Search

3.1 Generic Security of Hash Functions against Hybrid Adversaries

In this section we study the generic security of hash functions, i.e., security properties such as one-wayness, second-preimage resistance and extended target collision resistance [HRS16] against hybrid classical-quantum attacks.

The analysis of these generic security properties of hash functions against hybrid classical-quantum adversaries reduces to the study of a family of distributional search problems. Namely, the central problem is the Bernoulli Search problem, in which the target function to be queried is sampled from the Bernoulli distribution $D_\eta$, defined in Section 2.3.2.

To show the security of a hash function in the hybrid classical-quantum security model, we will adopt the strategy and proof techniques developed in [HRS16] against quantum adversaries, which proceeds as follows:

- Reduce the hardness of a hybrid classical-quantum adversary against security of hash functions to the hardness of hybrid classical-quantum strategies for the Bernoulli search problem. More concretely, show how an instance of the Bernoulli search problem can be turned into an instance of the security experiment.
- Determine the number of classical and quantum queries in the reduction.

- Apply the bound on the success probability of a hybrid classical-quantum algorithm to solve the Bernoulli search problem (Theorem 3) given the number of queries established in previous step. This gives us the bound on the success probability of breaking the security properties of hash functions.

We now introduce notation and security definitions of hash functions to be analyzed in the hybrid security model.

### 3.1.1 Hash Function Background

Let \( n \in \mathbb{N} \) be the security parameter, \( m = \text{poly}(n), k = \text{poly}(n) \), and \( \mathcal{H}_n := \{ H_K : \{0,1\}^m \rightarrow \{0,1\}^n \}_{K \in \{0,1\}^k} \) be a family of hash functions, where \( K \) denotes the index of the hash function. We will denote by \( M \) the input of the hash function.

**Definition 6 (OW).** For any QPT adversary \( A \), we define the probability of success of breaking the one-wayness (OW) of a family of hash functions \( \mathcal{H}_n \) as:

\[
\text{Succ}^\text{OW}_{\mathcal{H}_n}(A) = \Pr[K \leftarrow \{0,1\}^k, M \leftarrow \{0,1\}^m, Y \leftarrow H_K(M); M' \leftarrow A(K, Y) : Y = H_K(M')]
\]

Similarly, we define single-function, multi-target preimage resistance (SM) as:

\[
\text{Succ}^\text{SM}^m_{\mathcal{H}_n}(A) = \Pr[K \leftarrow \{0,1\}^k, M_i \leftarrow \{0,1\}^m, Y_i \leftarrow H_K(M_i) \quad 0 < i \leq p;
M' \leftarrow A(K, (Y_1, \ldots, Y_p)) : \exists 0 < i \leq p, Y_i = H_K(M')]
\]

And we also define multi-function, multi-target preimage resistance (MM) as:

\[
\text{Succ}^\text{MM}^m_{\mathcal{H}_n}(A) = \Pr[K_i \leftarrow \{0,1\}^k, M_i \leftarrow \{0,1\}^m, Y_i \leftarrow H_K(M_i) \quad 0 < i \leq p
(j, M') \leftarrow A((K_1, Y_1), \ldots, (K_p, Y_p)) : Y_j = H_K(M')]
\]

**Definition 7 (SPR).** For any QPT adversary \( A = (A_1, A_2) \), we define the probability of success of breaking the second-preimage resistance (SPR) of a family of hash functions \( \mathcal{H}_n \) as:

\[
\text{Succ}^\text{SPR}_{\mathcal{H}_n}(A) = \Pr[K \leftarrow \{0,1\}^k, M \leftarrow \{0,1\}^m;
M' \leftarrow A(K, M) : M' \neq M \text{ and } H_K(M) = H_K(M')]
\]

**Definition 8 (eTCR).** For any QPT adversary \( A \), we define the probability of success of breaking the extended target collision-resistance (eTCR) of a family of hash functions \( \mathcal{H}_n \) as:

\[
\text{Succ}^\text{TCR}_{\mathcal{H}_n}(A) = \Pr[M \leftarrow A_1(1^n), K \leftarrow \{0,1\}^k;
(M', K') \leftarrow A_2(K, M) : M' \neq M \text{ and } H_K(M) = H_K(M')]
\]

SM and MM definitions are defined analogously for second-preimage resistance and extended target collision-resistance as in the one-way definition case.
3.1.2 Hybrid Security of Hash Functions

First, we state the hybrid adversarial success as a function of its quantum/classical queries against the properties enumerated above, followed by the proof for OW. The proofs for the other security properties proceed similarly as in [HRS16].

**Lemma 10 (Hybrid Security of OW).** Let $m = cn$ for $c > 1$ constant and $p = o(2^n)$. For any hybrid classical-quantum algorithm $A$ with $\tau_c$ classical queries and $\tau_q$ quantum queries we have:

\[
\text{Succ}^{\text{OW}}_{H_n}(A) \leq \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2,
\]
\[
\text{Succ}^{\text{SM}_p - \text{OW}}_{H_n}(A) \leq p \cdot \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2,
\]
\[
\text{Succ}^{\text{MM}_p - \text{OW}}_{H_n}(A) \leq \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2.
\]

**Lemma 11 (Hybrid Security of SPR).** For any hybrid classical-quantum algorithm $A$ with $\tau_c$ classical queries and $\tau_q$ quantum queries we have:

\[
\text{Succ}^{\text{SPR}}_{H_n}(A) \leq \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2,
\]
\[
\text{Succ}^{\text{SM}_p - \text{SPR}}_{H_n}(A) \leq p \cdot \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2,
\]
\[
\text{Succ}^{\text{MM}_p - \text{SPR}}_{H_n}(A) \leq \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2.
\]

**Lemma 12 (Hybrid Security of eTCR).** For any hybrid classical-quantum algorithm $A$ with $\tau_c$ classical queries and $\tau_q$ quantum queries we have:

\[
\text{Succ}^{\text{eTCR}}_{H_n}(A) \leq \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2 + \frac{8(\tau_c + \tau_q)^2}{2^n},
\]
\[
\text{Succ}^{\text{MM}_p - \text{eTCR}}_{H_n}(A) \leq p \cdot \left( \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2 + \frac{8(\tau_c + \tau_q)^2}{2^n} \right).
\]

The results and the comparison with the quantum and classical adversary setting are summarized in the following table:
We want to argue that the output of the Bernoulli Analysis of the reduction.

Table 2: Security of hash functions $H_n := \{H_K : \{0,1\}^m \rightarrow \{0,1\}^n\}_{K \in \{0,1\}^k}$ against generic classical, quantum and hybrid adversaries. Entries represent the probability of success of classical adversaries equipped with $q$ classical queries, quantum adversaries equipped with $q$ quantum queries, respectively hybrid classical-quantum adversaries equipped with $\tau_c$ classical and $\tau_q$ quantum queries.

**Proof of Lemma 10 (OW).** Given an Bernoulli Search instance, we will show how to construct an instance of one-wayness (OW).

<table>
<thead>
<tr>
<th>Bernoulli Search to OW Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: <strong>Input</strong>: $f : {0,1}^m \rightarrow {0,1}$ sampled from distribution $D_q$. Set $\eta = \frac{1}{2^n}$;</td>
</tr>
<tr>
<td>2: Sample $y \in {0,1}^n$;</td>
</tr>
<tr>
<td>3: Let random function $g : {0,1}^m \rightarrow {0,1}^n - {y}$;</td>
</tr>
<tr>
<td>4: Construct function $G : {0,1}^m \rightarrow {0,1}^n$ defined as:</td>
</tr>
<tr>
<td>5: $G(x) = y$, if $f(x) = 1$</td>
</tr>
<tr>
<td>6: $G(x) = g(x)$, else</td>
</tr>
<tr>
<td>7: <strong>Output</strong>: OW instance $(y,G)$.</td>
</tr>
</tbody>
</table>

**OW Adversary**

| 1: **Input**: Given $y$ and oracle access to $G |
| 2: **Task**: Find $x \in \{0,1\}^m$ such that $G(x) = y$ |

**Analysis of the reduction.** We want to argue that the output of the Bernoulli Search to OW reduction (i.e., $(y,G)$) is negligibly close to the distribution of the OW experiment. The sketch of this claim proceeds as follows:

- The output $(y,G)$ is distributed identically to distribution $D_1 = \{(z,H)\}$, where $z$ is sampled uniformly at random from $\{0,1\}^n$ and $H : \{0,1\}^m \rightarrow \{0,1\}^n$ random function.
- Define distribution $D_0 := \{(H(x),H)\}$ where $H$ is sampled uniformly at random and $x$ is sampled uniformly at random from domain $\{0,1\}^m$. Distribution $D_0$ is the distribution in the OW experiment.
– Show that $D_1$ are $D_0$ are close:

$$\text{SD}(D_0, D_1) = \frac{1}{2} \sum_{z,H} \left| \Pr_{x,H}[z,H] - \Pr_{x,H}[H(x),H] \right|$$

$$= \frac{1}{2} \sum_z \sum_H \frac{1}{|H|} \left| \left| H^{-1}(z) \right| - \frac{1}{2^n} \right|$$

Using Jensen’s inequality we get that: $\text{SD}(D_0, D_1) \leq \frac{1}{2} \cdot \frac{1}{2^n}$. By setting $m \geq 2n$, the distributions are negligibly close.

**Implementation of $G$ using $f$.** Now, we need to see how oracle access to $G$ is implemented using oracle access to $f$ and knowledge of $g$ and $y$, as well as how many queries to $f$ are needed:

– Quantum query to $G$: $\sum_{x,z} a_{x,z}|x,z\rangle \xrightarrow{H} \sum_{x,z} a_{x,z}|x,z + H(x)\rangle$.

\[
\sum_{x,z} a_{x,z}|x|z\rangle|0\rangle \quad \text{(initial state to be queried)}
\]

$\mapsto \sum_{x,z} a_{x,z}|x|z\rangle|f(x)\rangle \quad \text{ (evaluate $f$)}$

$\mapsto \sum_{x,z} a_{x,z}|x|z + f(x)\cdot y + (1 - f(x))\cdot g(x)\rangle|f(x)\rangle$

$\mapsto \sum_{x,z} a_{x,z}|x|G(x)\rangle|f(x)\rangle$

$\mapsto \sum_{x,z} a_{x,z}|x|G(x)\rangle|0\rangle \quad \text{(uncompute $f$)}$

It is clear that a quantum query to $G$ requires two quantum queries to the Bernoulli function $f$.

– Classical query to $G$:

$$x \mapsto f(x)\cdot y + (1 - f(x))\cdot g(x) = G(x).$$

A classical query to $G$ requires a classical query to Bernoulli function $f$.

As a result, we have that the success of a hybrid adversary that has $\tau_c$ classical queries and $\tau_q$ quantum queries to break $\text{OW}$ is at most the success of a hybrid algorithm that has $\tau_c$ classical queries and $2 \cdot \tau_q$ quantum queries to solve the Bernoulli Search problem (Theorem 3, with $\eta = \frac{1}{2^n}$):

$$\text{Succ}_{\text{OW}}^{\tau_c}(A) \leq \frac{1}{2^n} \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2 \quad (10)$$

\[\square\]
3.2 The Bitcoin Blockchain against Hybrid Adversaries

A proof of work (PoW) enables a party to convince other parties that considerable effort has been invested in solving a computational task. In the blockchain setting, the objective of a PoW is to confirm new transactions to be included in the blockchain. To successfully create a PoW in Bitcoin, one needs to find a value ("witness") such that evaluating a hash function (SHA-256) on this value together with (the hash of) the last block and new transactions to be incorporated, yields an output below a threshold. A party who produces such a PoW gets to append a new block to the blockchain and is rewarded. A blockchain hence consists of a sequence of such blocks. Each party maintains such a blockchain, and attempts to extend it via solving a PoW.

**Definition 9 (Blockchain PoW—Informal).** Given a hash function $h$, a positive integer $T$, and a string $z$ representing the hash value of the previous block, the goal is to find a value $\text{ctr}$ such that:

$$h(\text{ctr}, z) \leq T.$$ 

In this section we revisit the following question:

*What is the complexity of PoW in the hybrid classical-quantum query model? Can we formally establish the hybrid security of the Bitcoin backbone protocol [GKL15] to properly work against hybrid classical-quantum adversaries in the random oracle model?*

Next, we show the hybrid classical-quantum query complexity of PoW, and then establish the hybrid security of the Bitcoin backbone protocol in the random oracle model.

3.2.1 The Bitcoin Backbone Protocol

It is shown in [GKL15] that the blockchain data structure built by the Bitcoin backbone protocol satisfies a number of basic properties. At a high level, the first property, called common prefix, has to do with the existence, as well as persistence in time, of a common prefix of blocks among the chains of honest parties. The second, called chain quality, stipulates the proportion of honest blocks in any portion of some honest party’s chain.

**Definition 10 (Common Prefix).** The common prefix property with parameter $k \in \mathbb{N}$, states that for any pair of honest players $P_1, P_2$ adopting chains $C_1, C_2$ at rounds $r_1 \leq r_2$, it holds that $C_1^{r_1 \leq k} \preceq C_2$ (the chain resulting from pruning the $k$ rightmost blocks of $C_1$ is a prefix of $C_2$).

**Definition 11 (Chain Quality).** The chain quality property with parameters $\mu \in \mathbb{R}$ and $l \in \mathbb{N}$, states that for any honest party $P$ with chain $C$, it holds that
for any $l$ consecutive blocks of $C$, the ratio of blocks created by honest players is at least $\mu$.

**Parameters and random variables.** Next, we recall some important notions in the Bitcoin backbone protocol setting.

- $\tau_c$ and $\tau_q$ denotes the number of adversarial classical queries respectively quantum queries per round;
- $f$ is the probability that at least one honest party generates a PoW in a round;
- $\epsilon$ will be used for the concentration quality of random variables;
- $\kappa$ denotes the security parameter;
- $k$ denotes the number of blocks for common prefix property and $\mu$ denotes the chain quality parameter;
- $s$ refers to the total number of rounds;
- $p = \frac{T}{2^\kappa}$, where $T$ denotes the difficulty parameter for solving a PoW. $p$ can be understood as the probability of success of generating a PoW using a single classical query;
- $f$ denotes the probability that at least one honest player generates a PoW in a single round (e.g., in the Bitcoin system, $f$ is about $2^{-3}$).

### 3.2.2 Hybrid Security of the Bitcoin Backbone Protocol

We will use the hybrid classical-quantum hardness of PoW to derive a quantum analogue of an honest-majority condition, under which the common prefix and chain quality properties occur with overwhelming probability. Intuitively, the hybrid-majority reflects a condition on the computational power of the hybrid adversary that needs to be imposed such that the security properties of the Bitcoin Backbone protocol would hold with overwhelming probability. The following definition and lemmas are adapted from [CGK+23].

**Definition 12 (Hybrid Honest-Majority).** We say that the hybrid honest majority condition holds if:

$$\sqrt{\tau_c} + 2\tau_q \leq \frac{1}{\sqrt{f(1-f)p}} \cdot \text{negl}(\kappa)$$

**Lemma 13.** Under the hybrid honest-majority condition (Def. 12), the desired properties of a blockchain hold with probability $1 - \text{negl}(\kappa)$:

- The common prefix property of the Bitcoin backbone protocol holds with parameter $k \geq 2sf$, for any $s \geq \frac{2}{f}$ consecutive rounds;
- the chain quality property holds with parameter $l \geq 2sf$ and ratio of honest blocks $\mu$ with $\mu = f$.  

27
Proof. From [CGK+23] it is known that the common prefix and chain quality properties hold as long as in any round, the number of solved PoWs using $\tau_c$ classical queries and $\tau_q$ quantum queries is at most $E := (1 - \epsilon)f(1 - f)$. It should be clear from Definition 9 that solving a single PoW is equivalent to solving the Bernoulli Search problem with distribution $D_\eta$, where we set $\eta = p = \frac{T}{2\pi}$. Then, the probability that a hybrid classical-quantum algorithm equipped with $\tau_c$ classical and $\tau_q$ quantum queries to solve $E$ PoWs is at most:

$$P_{\text{PoW Succ}} \leq E \cdot \text{Succ}_{A,D_\eta} \leq E \cdot p \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2.$$ 

As a result, the probability that the two security properties hold under the hybrid honest-majority is:

$$P_{\text{sec}} = 1 - P_{\text{PoW Succ}} \geq 1 - (1 - \epsilon)f(1 - f)p \cdot (2\sqrt{\tau_c} + 4\tau_q + 1)^2 \geq 1 - \text{negl}(\kappa)$$

\[ \square \]

4 Conclusions and Future Work

We believe that the hybrid query model is both of theoretical and practical importance. Since near-term quantum computers are likely to be limited and also expensive, it is to the interest of a party to supplement it with massive classical computational power. This also reflects the fact that those parties who have early access to quantum computers (e.g., big companies and government agencies) probably largely coincide with those who are capable of employing classical clusters and supercomputers. Next, we discuss a few future research directions worth exploring.

One immediate question is to study other problems in the hybrid query model. Recent work [HLS22] proves the hardness of the collision problem by generalizing the recording technique due to Zhandry [Zha19] in the hybrid query model. It would be interesting to develop other techniques and generally establish further query complexity results in this model.

Our applications to hash functions and Bitcoin blockchains can be seen as analyzing cryptographic constructions in the QRO model against hybrid adversaries. Many block ciphers rely on a different model, known as the ideal cipher model. As a simple example, the Even-Mansour cipher encrypts by $E_k : m \mapsto \sigma(k \oplus m) \oplus k$, where $\sigma$ is a random permutation given as an oracle. As it turns out, this classically secure cipher is completely broken when quantum queries are allowed to both $E_k$ and $\sigma$ [KM10]. Since the secret key $k$ is managed by honest users, it is debatable whether superposition access to $E_k$ is realistic. There has been progress in re-establishing the cipher’s security under a partially quantum adversary with quantum access to $\sigma$ but classical access to $E_k$ [JST21, ABKM22]. The hybrid query model we consider in this work suggests further relaxing the queries
to $\sigma$ to be a hybrid of classical and quantum ones, and it would be valuable to re-examine the security of such schemes in the ideal cipher model.

Querying an oracle is actually more commonplace in cryptography than the aforementioned scenarios. Security definitions often give some component of a cryptosystem as an oracle to the adversary, such as an encryption oracle in the chosen-plaintext-attack (CPA) game and a signing oracle in formalizing unforgeability of digital signatures. There has been a considerable effort of settling appropriate definitions and constructions (e.g., quantum-accessible pseudorandom functions, encryption and signatures) when quantum adversaries are granted superposition queries to these oracles (cf. [BZ13, Zha15, AMRS20, Zha21, CEV23]). Extending such efforts to the hybrid-adversary landscape would offer fine-grained security assessments of post-quantum cryptosystems.

Acknowledgement

J.G. was partially supported by NSF grants no. 2001082 and 2055694. F.S. was partially supported by NSF grant no. 1942706 (CAREER). J.G. and F.S. also thank SONY for a Faculty Innovation Award. A.C. acknowledges support from the National Science Foundation grant CCF-1813814 and from the AFOSR under Award Number FA9550-20-1-0108.
References


