

Enhancing One-Way to Hiding Theorems with Amplitude Amplification

Bohang Chen¹, Shuai Han¹, Geng Wang¹, and Xinyi Huang²

¹ School of Computer Science,
Shanghai Jiao Tong University, Shanghai 200240, China
{bohango918,dalen17,wanggxx}@sjtu.edu.cn

² Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
huangxinyi@nuaa.edu.cn

Abstract. The one-way to hiding (O2H) theorem and its variants, which bound the distinguishing advantage in terms of the one-way advantage, are widely used in security proofs in the quantum random oracle model (QROM), particularly for key encapsulation mechanisms (KEMs). However, existing O2H bounds typically incur a security loss depending on the adversary’s oracle query depth d (i.e. the number of sequential layers of parallel queries), which can make both computational and information-theoretic bounds in KEM security proofs less tight.

In this work, we establish a generic amplitude-amplification-based technique to many O2H variants to remove their depth-dependent factors in the advantage bounds. This covers the Semi-Classical O2H (SC-O2H) [Ambainis et al., CRYPTO 2019] and Measure-Rewind-Extract O2H (MRE-O2H) [Ge et al., ASIACRYPT 2024] theorems, in which the constructed one-way adversaries have access to an indicator oracle $\mathbf{1}_S$ that checks whether the input is a valid solution to the one-way game.

We identify conditions under which our enhanced O2H theorems can replace the original O2H theorems in existing security proofs. These conditions hold for a range of security proofs, including IND-CCA security proofs for KEMs obtained from variants of the U transformation in the Fujisaki–Okamoto (FO) framework.

Applying our enhanced theorems in these proofs yields the following improvements in the depth dependence of security bounds:

- When the one-way advantage is bounded information-theoretically, our technique eliminates the depth-dependent factors with only a constant-factor loss in the security bound.
- When the one-way advantage is bounded by computational hardness assumptions, our technique eliminates the depth-dependent factors d for SC-O2H and $\sqrt{d}$ for MRE-O2H, at the cost of increasing the constructed one-way adversary’s running time by a factor that is only of the order of the square roots of the eliminated losses, namely $O(\sqrt{d})$ for SC-O2H and $O(\sqrt[4]{d})$ for MRE-O2H.

Keywords: Post-quantum security, KEM, QROM, O2H

1 Introduction

When analyzing the post-quantum security of efficient cryptographic constructions based on random oracles, it has become standard to provide security proofs in the quantum random oracle model (QROM). The QROM allows an adversary to query the random oracle with a superposition as input, making it considerably harder to prove security in the QROM than in the classical ROM. To address this, a large body of works [3,7,11,20,19,1,2,15,10] has developed tools and techniques for QROM security proofs that are easy to use even without much background in quantum information.

Among these works, the One-Way to Hiding (O2H) theorems [19,1] are worth noting as a crucial branch of works providing tools for programming the quantum random oracles. With the original O2H theorem stated in [19], one can replace the initial oracle $H : \mathcal{X} \rightarrow \mathcal{Y}$ with a programmed oracle $G : \mathcal{X} \rightarrow \mathcal{Y}$ that differs only on inputs within a set $S \subset \mathcal{X}$. Then, the advantage for an adversary $\mathcal{A}_{\text{IND}}$ distinguishing between the oracles H and G will have an upper bound related to the advantage of a constructed adversary $\mathcal{B}_{\text{OW}}$, which has oracle access to either H or G and wins a game that requires it to output an element $x \in S$. If the resulting game of the constructed adversary $\mathcal{B}_{\text{OW}}$ can be further reduced from some concrete computational hardness problem (e.g. SIS, LWE, NTRU), then one can show the indistinguishability of the two oracles H and G . In some cases, the game of $\mathcal{B}_{\text{OW}}$ may even be hard for information-theoretic reasons, with no computational problem involved.

Since then, a sequence of works [2,15,10] has been establishing variants of the O2H theorems, providing improvements on their security loss by altering $\mathcal{B}_{\text{OW}}$'s oracle access and its concrete procedure. See Table 1 for more details.

Table 1: One-way to hiding (O2H) and its variants in the QROM. Here S is the set of inputs that the two oracles H and G differ on, $|S|$ is its size, $\mathcal{A}_{\text{IND}}$ makes parallel queries to its oracle with query depth d , and $\mathbf{1}_S$ denotes the indicator function of S , i.e., $\mathbf{1}_S(x) = 1$ for $x \in S$ and $= 0$ otherwise.

O2H Type	$ S $	$\text{Adv}(\mathcal{A}_{\text{IND}}) \leq$	$\mathcal{B}_{\text{OW}}$'s Oracle
Original [19]	Arbitrary	$2d \cdot \sqrt{\text{Adv}_{\mathcal{B}_{\text{OW}}}}$	H
SC-O2H [1]	Arbitrary	$2\sqrt{d} \cdot \text{Adv}_{\mathcal{B}_{\text{OW}}}$	$H, \mathbf{1}_S$ *
DS-O2H [2]	1	$2\sqrt{\text{Adv}_{\mathcal{B}_{\text{OW}}}}$	H, G
MRM-O2H [15]	Arbitrary	$4d \cdot \text{Adv}_{\mathcal{B}_{\text{OW}}}$	H, G
MRE-O2H [10]	Arbitrary	$4\sqrt{d} \cdot \text{Adv}_{\mathcal{B}_{\text{OW}}}$	$H, G, \mathbf{1}_S$

* The adversary $\mathcal{B}_{\text{OW}}$ in the SC-O2H actually requires oracle access to the punctured oracle $H \setminus S$. For simplicity, here we write their oracle access as $H, \mathbf{1}_S$, since $H \setminus S$ is by definition implemented with H and $\mathbf{1}_S$ (cf. Definition 1).

We classify the variants of O2H theorems into three categories based on the oracle access of the constructed adversary $\mathcal{B}_{\text{OW}}$, named one-sided variants, checkable variants and double-sided variants.

- The *one-sided variants* only have oracle access to one of the two oracles H and G . This includes the original O2H theorem in [19].
- The *checkable variants* have additional oracle access to the indicator function $\mathbf{1}_S$ that checks whether an input $x \in \mathcal{X}$ is in the set S . We classify the Semi-Classical (SC) O2H theorem in [1] in this category, since the punctured oracle $H \setminus S$ uses $\mathbf{1}_S$ to check whether an input $x \in \mathcal{X}$ is in S by definition.
- The *double-sided variants* have oracle access to both oracles H and G . This includes the Double-sided (DS) O2H theorem in [2], the Measure-rewind-measure (MRM) O2H theorem in [15], and the Measure-rewind-extract (MRE) O2H theorem in [10]. As discussed in [10], when having oracle access to both oracles H and G , one can simulate $\mathbf{1}_S$ by comparing the outputs of H and G . We therefore do not distinguish between whether $\mathcal{B}_{\text{OW}}$ has direct access to $\mathbf{1}_S$ in the double-sided variants.

These O2H theorems are widely used in security proofs of cryptographic schemes, among which most notably are the security proofs of the Fujisaki-Okamoto (FO) transformation and its variants [9,13], which are used to construct IND-CCA secure key encapsulation mechanism (KEM) schemes from OW-CPA secure public-key encryption (PKE) schemes. With these different variants of the O2H theorems, a sequence of work [14,2,15,10] has been tightening the security proof of the IND-CCA security of various FO transformations in the QROM.

Nonetheless, there is a notable drawback about the existing O2H theorems [19,1,2,15,10] regarding the tightness of these security proofs. Namely, the reduction between $\mathcal{A}_{\text{IND}}$ and $\mathcal{B}_{\text{OW}}$ generally suffers from a security loss dependent on the query depth d of the adversary $\mathcal{A}_{\text{IND}}$ ³ (except for the DS-O2H [2], which, however, suffers from a substantially larger square-root loss than MRM-O2H [15] and MRE-O2H [10]), as shown in Table 1. For an arbitrary adversary $\mathcal{A}_{\text{IND}}$, its query depth d can be as large as the number of its total queries q (that can be up to 2^{30} or even 2^{60} [17, 4.A.2]), in which case the existing O2H theorems would incur a considerably large security loss. Moreover, the advantage of $\mathcal{B}_{\text{OW}}$ is usually bounded via a sequence of hybrid games, each of which may introduce a loss term of its own. The factor depending on d introduced by the O2H theorems then multiplies every loss term in this sequence, degrading the tightness with respect to every underlying hardness assumption and information-theoretic bound.

However, compared with the result in the classical ROM, such a security loss seems rather weird for the checkable variants [1] and the double-sided variants [15,10]. In the classical random oracle model, one can avoid the loss dependent on the query depth d in the reduction between $\mathcal{A}_{\text{IND}}$ and $\mathcal{B}_{\text{OW}}$ by checking whether each input to the random oracle H is in the set S directly with the classical

³ Note that $\mathcal{A}_{\text{IND}}$ can make parallel queries to its oracle, and the query depth d is the number of sequential layers of parallel queries (cf. Subsect. 2.2 for the definition).

oracle access to $\mathbf{1}_S$, and outputting confidently an element $x \in S$ once such an input is found. This makes us wonder whether the factor dependent on d in the O2H theorems in the QROM for the checkable variants and the double-sided variants is inherent or not. Such intuition leads to the question:

Can we remove the factor dependent on the query depth d in the security loss of the variations of the O2H Theorems?

1.1 Our Contributions

In this work, we answer the above question affirmatively with a generic technique applicable to many O2H variants to reduce their security loss. We also show its impact on existing security proofs that apply the variations of O2H theorems.

More precisely, we established a general method based on quantum amplitude amplification [5], called *amplitude-amplification-based enhancement (AA-based enhancement)*, to boost the success probability of the one-way adversary $\mathcal{B}_{\text{OW}}$, for O2H variants where $\mathcal{B}_{\text{OW}}$ has oracle access to the indicator function $\mathbf{1}_S$, including the checkable variants [1] and the double-sided variants [10]. Specifically, we apply this method to the SC-O2H theorem in [1] and the MRE-O2H theorem in [10], and obtain our AA-enhanced SC-O2H theorem and AA-enhanced MRE-O2H theorem, where the security loss is now independent of the query depth d , thus providing the best-known bounds in their respective categories. Table 2 summarizes the impact of our technique on the best-known O2H theorems in all three categories of oracle access.

Table 2: Comparison of the existing O2H variants and our AA-enhanced ones. Here “Existing Bounds” shows the advantage and running time established in the existing O2H variants, and “Our Enhancement” gives the corresponding advantage and running time after applying our AA-based enhancement. The sub-column “Advantage” shows the upper bound on the distinguishing advantage of $\mathcal{A}_{\text{IND}}$ in terms of the one-way advantage ε of $\mathcal{B}_{\text{OW}}$, and “Time” shows the upper bound on the running time of $\mathcal{B}_{\text{OW}}$ in terms of the running time T of $\mathcal{A}_{\text{IND}}$.

O2H Type	$\mathcal{B}_{\text{OW}}$ ’s Oracle	Existing Bounds		Our Enhancement	
		Advantage	Time	Advantage	Time
Original O2H [19]	H	$O(d) \cdot \sqrt{\varepsilon}$	$O(1) \cdot T$	Inapplicable	
SC-O2H [1]	$H, \mathbf{1}_S$	$O(\sqrt{d}) \cdot \sqrt{\varepsilon}$	$O(1) \cdot T$	$O(1) \cdot \sqrt{\varepsilon}$	$O(\sqrt{d}) \cdot T$
MRE-O2H [10]	$H, G, \mathbf{1}_S$	$O(\sqrt{d}) \cdot \varepsilon$	$O(1) \cdot T$	$O(1) \cdot \varepsilon$	$O(\sqrt[4]{d}) \cdot T$

As for running time, our technique introduces extra time consumption to the one-wayness adversary $\mathcal{B}_{\text{OW}}$, also shown in Table 2. The impacts of this are:

- When the advantage of $\mathcal{B}_{\text{OW}}$ is further bounded via some *computational* hardness assumptions, this extra time may lead to a larger advantage when

solving the problem, offsetting the reduced security loss. In this case, our technique can be viewed as a trade-off between advantage and running time.

- When the advantage of $\mathcal{B}_{\text{OW}}$ is further bounded by some *statistical* terms information-theoretically, then the running-time budget is irrelevant, since such a bound holds even for computationally unbounded adversaries. In this case, our technique indeed eliminates the depth-dependent factors with only a constant-factor loss in the security bound.

In concrete applications of the O2H theorems, it is more common to bound the advantage in the one-wayness game by a *mixture* of computational hardness assumptions and information-theoretic bounds, using a sequence of hybrid games. In such case, both of the cases mentioned above appear. We will make a more detailed discussion of this in Subsect. 1.2 along with the impact of our AA-enhanced O2H theorems on concrete security proofs.

1.2 Applications to security proofs

Our amplitude-amplification-enhanced (AA-enhanced) SC-O2H and MRE-O2H theorems can be used as a direct replacement for a broad class of security proofs that use the original SC-O2H and MRE-O2H theorems, respectively, yielding improved security bounds.

In particular, we show the impact of our technique on the U transformation family [13], which is a building block of the Fujisaki-Okamoto (FO) transformation [9] that turns a deterministic PKE (DPKE) into a KEM. We present the results in Table 3, as both a concrete improvement on the security loss of the FO transformation and an example of how to use our AA-enhanced O2H theorems.

Specifically, we analyze two classes of security proofs for the U transformation family [13].

- The first class consists of the proofs of IND-CPA security of the $U_m^\perp$ and $U^\mathcal{L}$ transformations in [10] based on the MRE-O2H theorem, which act as components of the modular proof of their IND-CCA security. Applying our technique to this class of proofs improves the best known security bound of the IND-CCA security of the transformations.
- The second class consists of the proofs of IND-CCA security of the $U_m^\perp$ and $U^\mathcal{L}$ transformations in [10] based on the SC-O2H theorem. This class acts as a good example of how to use our AA-based enhancement on security proofs based on SC-O2H.

We highlight our improvement in the statistical terms when applying our technique instead of the existing SC-O2H and MRE-O2H theorems. In particular, for the U transformation family, this corresponds to the correctness error term δ . As shown in Table 3, the correctness loss bound obtained with our AA-based enhancement is tighter by a factor of $O(\sqrt{d})$ than the loss in the original proofs for both classes we are analyzing. Our result justifies that the $O(\sqrt{d})$ loss in the correctness error term appearing in prior results is not inherent.

Table 3: Comparison of the security bounds of several security proofs [14,10] of the U transformations $U_m^\perp$ and $U^\perp$ [13] (which turn a deterministic PKE (DPKE) into a KEM) of the FO transformation [9], obtained with the existing SC-O2H and MRE-O2H theorems, and our AA-enhanced SC and AA-enhanced MRE, respectively. Here OW-VA, OW-CPA, and OW-qPCA denote one-wayness of the underlying DPKE against validity-checking attacks, chosen-plaintext attacks, and quantum plaintext-checking attacks, respectively. δ denotes the correctness error of the underlying DPKE. d is the query depth of $\mathcal{A}$ to its oracle. q is the total query number of $\mathcal{A}$. $\mathcal{M}$ is the message space. For a security notion SEC, we use $\text{Adv}_{\mathcal{A}(T)}^{\text{SEC}}$ to denote the advantage of $\mathcal{A}$ when it runs in time T . We write C in the running time of $\mathcal{B}$ in each line for a different but fixed constant.

Transform	O2H type	Reduction	Security bound
$U_m^\perp$ [13]	SC	OW-VA $\Rightarrow$ IND-CCA	[14] $\text{Adv}_{\mathcal{A}(T)}^{\text{IND-CCA}} \leq \delta + 2\sqrt{(d+1)(2\delta + \text{Adv}_{\mathcal{B}(CT)}^{\text{OW-VA}})}$
	AA-enhanced SC	OW-VA $\Rightarrow$ IND-CCA	$\text{Adv}_{\mathcal{A}(T)}^{\text{IND-CCA}} \leq \delta + 4\sqrt{2\delta + \text{Adv}_{\mathcal{B}(Cd^{1/2}T)}^{\text{OW-VA}}}$
	MRE	OW-CPA $\Rightarrow$ IND-CPA	[10] $\text{Adv}_{\mathcal{A}(T)}^{\text{IND-CPA}} \leq 2\sqrt{d}\text{Adv}_{\mathcal{B}(CT)}^{\text{OW-CPA}} + 2\sqrt{d}\delta$
	AA-enhanced MRE	OW-CPA $\Rightarrow$ IND-CPA	$\text{Adv}_{\mathcal{A}(T)}^{\text{IND-CPA}} \leq 8\text{Adv}_{\mathcal{B}(Cd^{1/4}T)}^{\text{OW-CPA}} + 8\delta$
$U^\perp$ [13]	SC	OW-qPCA $\Rightarrow$ IND-CCA	[14] $\text{Adv}_{\mathcal{A}(T)}^{\text{IND-CCA}} \leq \frac{2q}{ \mathcal{M} } + 2\sqrt{(d+1)(2\delta + \text{Adv}_{\mathcal{B}(CT)}^{\text{OW-qPCA}})}$
	AA-enhanced SC	OW-qPCA $\Rightarrow$ IND-CCA	$\text{Adv}_{\mathcal{A}(T)}^{\text{IND-CCA}} \leq \frac{2q}{ \mathcal{M} } + 4\sqrt{2\delta + \text{Adv}_{\mathcal{B}(Cd^{1/2}T)}^{\text{OW-qPCA}}}$
	MRE	OW-CPA $\Rightarrow$ IND-CPA	[10] $\text{Adv}_{\mathcal{A}(T)}^{\text{IND-CPA}} \leq 2\sqrt{d}\text{Adv}_{\mathcal{B}(CT)}^{\text{OW-CPA}} + 2\sqrt{d}\delta$
	AA-enhanced MRE	OW-CPA $\Rightarrow$ IND-CPA	$\text{Adv}_{\mathcal{A}(T)}^{\text{IND-CPA}} \leq 8\text{Adv}_{\mathcal{B}(Cd^{1/4}T)}^{\text{OW-CPA}} + 8\delta$

In Sect. 6, we present a detailed discussion of the conditions for the direct replacement with our AA-enhanced O2H theorems and of the renewed proofs of the U transformations.

1.3 Technical Overview

As an overview, we focus on improving the algorithm from a simplified statement of the semi-classical O2H theorem (see Theorem 2 for the formal statement).

The semi-classical O2H theorem [1] concerns the distinguishability of a random oracle $H : \mathcal{X} \rightarrow \mathcal{Y}$ from its *punctured* version $H \setminus S$, where $S \subset \mathcal{X}$ is the set of punctured points. Upon input $|x\rangle_X |y\rangle_Y$, the punctured oracle $H \setminus S$ first evaluates the membership oracle $\mathbf{1}_S$ on $|x\rangle_X$, measuring and revealing the bit indicating whether $x \in S$; it then applies H to the registers X and Y exactly as an ordinary query to H would (cf. Definition 1).

Theorem 1 (Semi-Classical O2H, informal [1]). *Let $S \subset \mathcal{X}$ be a set, $H : \mathcal{X} \rightarrow \mathcal{Y}$ be a function, and $z \in \{0,1\}^*$ be a bit string. Suppose S, H, z are sampled from an arbitrary joint distribution $\mathcal{D}$. Let $\mathcal{A}^\mathcal{O}$ be a quantum algorithm that makes parallel queries to an oracle $\mathcal{O} \in \{H, H \setminus S\}$ with query depth d . Let*

Find denote the event that, in at least one of $\mathcal{A}$'s oracle queries, the measurement of the membership bit produced by $\mathbf{1}_S$ yields outcome 1. Let

$$\begin{aligned} P_{\text{left}} &:= \Pr[b = 1 : (S, H, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^H(z)], \\ P_{\text{right}} &:= \Pr[b = 1 : (S, H, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^{H \setminus S}(z)], \\ P_{\text{Find}} &:= \Pr[\text{Find} : (S, H, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^{H \setminus S}(z)]. \end{aligned}$$

Then

$$|P_{\text{left}} - P_{\text{right}}| \leq \sqrt{(d+1) \cdot P_{\text{Find}}} \text{ and } \left| \sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}} \right| \leq \sqrt{(d+1) \cdot P_{\text{Find}}}. \quad (1)$$

We note that when we restrict the distribution $\mathcal{D}$ to those that output a fixed tuple (S, H, z) deterministically, we obtain a special case of the SC-O2H called *fixed* SC-O2H, which turns out to be equivalent to SC-O2H as demonstrated in [1]. We write $P_{\text{Find}}^{S,H,z}, P_{\text{left}}^{S,H,z}, P_{\text{right}}^{S,H,z}$ for $P_{\text{Find}}, P_{\text{left}}, P_{\text{right}}$ respectively when fixing the tuple (S, H, z) output by $\mathcal{D}$.

Our target is to derive an algorithm $\mathcal{B}$, with oracle access specified later, whose success probability P_{succ} satisfies $|P_{\text{left}} - P_{\text{right}}| \leq C\sqrt{P_{\text{succ}}}$ for some constant C independent of d . In concrete applications, P_{succ} may then be bounded via an underlying one-wayness assumption or by some statistical terms. Since our construction may incur additional computational overhead, we will analyze its efficiency after presenting it.

We first illustrate the main idea through a warm-up construction based on independent repetitions. Its analysis uses an elementary probabilistic argument, providing an accessible starting point for readers unfamiliar with quantum amplitude amplification.

First Attempt: amplifying probability with repetitions. In order to eliminate the factor $\sqrt{d+1}$ in the bound (1) of SC-O2H, our first attempt is to construct a new adversary $\mathcal{B}^{H \setminus S}$ that triggers the event Find with probability $\Theta(d)$ times greater than that of the original adversary $\mathcal{A}^{H \setminus S}$. With such new adversary, the factor of the security loss during the reduction can be eliminated. To do this, our intuition is to do repetitions and trade the running time for a higher success probability.

This relies on our key observation that the semi-classical O2H theorem, in its fixed form, establishes a pointwise bound for every fixed instance. For an algorithm $\mathcal{A}^{H \setminus S}(z)$ with fixed (S, H, z) , we can construct a new algorithm $\mathcal{B}^{H \setminus S}(z)$ that runs $t := d+1$ repetitions of $\mathcal{A}^{H \setminus S}$ sequentially. Then, denoting $P'_{\text{Find}}^{S,H,z}$ as the probability of Find in $\mathcal{B}^{H \setminus S}(z)$ with fixed (S, H, z) , we have

$$P'_{\text{Find}}^{S,H,z} = 1 - (1 - P_{\text{Find}}^{S,H,z})^t. \quad ^4$$

⁴ We note that the equation holds for every fixed (S, H, z) , but may not be meaningful when the reduction only provides average-case guarantees on the probabilities, as commonly encountered in cryptographic statements. Specifically, if we only know about the expectation $P_{\text{Find}} = \mathbb{E}[P_{\text{Find}}^{S,H,z}]$, the expectation of the repeated probability will be $P'_{\text{Find}} = \mathbb{E}[1 - (1 - P_{\text{Find}}^{S,H,z})^t] \neq 1 - (1 - \mathbb{E}[P_{\text{Find}}^{S,H,z}])^t = 1 - (1 - P_{\text{Find}})^t$.

We observe that for cryptographic applications, the probability $P_{\text{Find}}^{S,H,z}$ should be substantially small, since it is usually related to the advantage of solving some hard problems regarding one-wayness.

We also observe that for a small $P_{\text{Find}}^{S,H,z}$, the probability of the event Find in $\mathcal{B}^{H \setminus S}$ admits the estimation that $P'_{\text{Find}}^{S,H,z} = 1 - (1 - P_{\text{Find}}^{S,H,z})^t \approx t \cdot P_{\text{Find}}^{S,H,z}$.

With such observations, our intuition is that for cryptographic applications, we are often working with negligible $P_{\text{Find}}^{S,H,z}$. Therefore, we may assume $P_{\text{Find}}^{S,H,z}$ to have an upper bound $\frac{1}{t}$ for polynomial-sized t . This then allows us to apply the estimation $P'_{\text{Find}}^{S,H,z} \geq Ct \cdot P_{\text{Find}}^{S,H,z}$ for some constant $C < 1$ to amplify the probability of Find in $\mathcal{A}^{H \setminus S}$ by a factor of $O(t)$. We suspect such a formulation is still capable of many applications of the SC-O2H.

However, this is not the case. In fact, one-wayness is usually stated as an average-case property, in which the advantage is defined as an expectation over all instances in the corresponding space. Consequently, an average-case one-wayness theorem does not guarantee the pointwise condition $P_{\text{Find}}^{S,H,z} \leq \frac{1}{t}$ needed for a uniform $\Theta(t)$ -fold amplification on the success probability using the repetition approach. On instances with larger $P_{\text{Find}}^{S,H,z}$, the repeated success probability $P'_{\text{Find}}^{S,H,z} = 1 - (1 - P_{\text{Find}}^{S,H,z})^t$ saturates towards 1 quickly instead of growing in proportion to $t \cdot P_{\text{Find}}^{S,H,z}$.

Observations on the O2H Theorems. Nonetheless, we note that our actual target is not to amplify the probability of Find, but to bound the distinguishing advantage with a new algorithm.

In particular, whenever $P_{\text{Find}}^{S,H,z} > \frac{1}{t} = \frac{1}{d+1}$, the upper bound $\sqrt{(d+1)P_{\text{Find}}^{S,H,z}}$ on the distinguishing advantage in (1) seems unnecessarily large, as the distinguishing advantage has a trivial upper bound of 1 because probabilities lie in the interval $[0, 1]$.

Therefore, we distinguish between two cases based on the value of $P_{\text{Find}}^{S,H,z}$ for each fixed tuple (S, H, z) .

- If $P_{\text{Find}}^{S,H,z}$ is bounded by $\frac{1}{t}$, then the algorithm $\mathcal{B}^{H \setminus S}$ constructed above satisfies $P'_{\text{Find}}^{S,H,z} \geq C_1 t \cdot P_{\text{Find}}^{S,H,z}$ for some constant $0 < C_1 < 1$.
- If $P_{\text{Find}}^{S,H,z}$ is larger than $\frac{1}{t}$, then the repetition approach yields a saturated probability satisfying the lower bound $P'_{\text{Find}}^{S,H,z} \geq C_2$ for some constant $0 < C_2 < 1$.

From these two cases, we conclude that $P'_{\text{Find}}^{S,H,z} \geq \min \{C_1 t \cdot P_{\text{Find}}^{S,H,z}, C_2\}$. We further define $C := 1/\min \{C_1, C_2\}$.⁵ Then, for $t = d+1$, given the trivial upper bound $|P_{\text{left}}^{S,H,z} - P_{\text{right}}^{S,H,z}| \leq 1$ and the upper bound $|P_{\text{left}}^{S,H,z} - P_{\text{right}}^{S,H,z}| \leq \sqrt{(d+1) \cdot P_{\text{Find}}}$ in (1) from the original semi-classical O2H theorem, we take the

⁵ As will be shown in the main body, the constants are $C_1 = C_2 = \frac{e-1}{e}$ and $C = \frac{e}{e-1}$, where e is Euler's number.

expectation over $(S, H, z) \leftarrow \mathcal{D}$ and obtain the new upper bound:

$$|P_{\text{left}} - P_{\text{right}}| \leq \sqrt{\min\{1, (d+1)P_{\text{Find}}\}} \leq \sqrt{C \cdot P'_{\text{Find}}}.$$

This successfully eliminates the factor $d+1$, improving the bound on the distinguishing advantage. The details of this approach are presented in Sect. 3.

Quantum speedup instead of repetitions. As we are working with the quantum random oracle model, all adversaries presented are quantum algorithms. In this case, the repetition approach does not provide an optimal trade-off between advantage and running time. We naturally start to think about whether quantum power can help with the efficiency of such algorithm.

Specifically, we consider applying the quantum amplitude amplification algorithm [5] as an alternative approach to repetition. The quantum amplitude amplification algorithm is a generalization of Grover algorithm [12] and can be viewed as a quantum analogue of independent classical repetitions achieving a quadratic speedup.

Let $\mathcal{A}$ be an algorithm with success probability p . Fixing an integer $t \geq 1$, our target is to derive an algorithm $\mathcal{B}$ with success probability $p' \geq \min\{C_1 t p, C_2\}$ for some constants $C_1, C_2 > 0$, but running in time $O(\sqrt{t})$ times the circuit size of $\mathcal{A}$, rather than $O(t)$ times.

Concretely, we use a standard variant of the amplitude amplification algorithm in which the number of generalized Grover iterations is sampled uniformly at random as $j \xleftarrow{\$} \{0, 1, \dots, m-1\}$, with the hard upper bound on the iteration count set to $m := 2^{\lceil \log_2 \sqrt{t} \rceil}$. Since $j < m < 2\sqrt{t}$, the algorithm performs $O(\sqrt{t})$ generalized Grover iterations in the worst case, and thus satisfies the circuit size restriction. Using the averaging bound established in [4, Lemma 1], we obtain the required upper bound of success probability.

This variant of the amplitude amplification algorithm is then a decent replacement of the repetition approach. The detail of this algorithm is presented in Subsect. 4.1.

Extracting $x \in S$ from quantum output. The application of the quantum amplitude amplification algorithm [5] is restricted to unitary quantum circuits. This is usually not a problem since a non-unitary quantum algorithm can be purified into a unitary circuit acting on additional workspace registers, with only a constant-factor overhead in the computational cost, provided the oracle calls and classical control can be implemented coherently and their inverses are available.

However, the direct applications of semi-classical O2H require one to extract $x \in S$ from the event Find. Usually, when one can simulate $H \setminus S$, this is achieved by halting immediately when the semi-classical oracle inside $H \setminus S$ measures to 1, and then measuring the outcome of the register X , i.e., the input register to $H \setminus S$.

If one directly translates the algorithm $\mathcal{A}^{H \setminus S}$ and the event Find into their unitary forms, such a way of extracting $x \in S$ is no longer feasible, since the

event Find is now detected by the measurements at the end of the circuit, where the register X has already been changed. In this case, it is non-trivial to construct an algorithm to extract $x \in S$ from a quantum state where the event Find is measured as happening. This shows that applying the amplitude amplifying algorithm to such algorithm directly induces unnecessary difficulties to our construction. It is better to trace an event that trivially leads to an extraction of $x \in S$.

To bypass this problem, we construct a unitary quantum oracle algorithm that directly outputs the extracted $x \in S$ explicitly. The construction is straightforward. We first change the oracle $H \setminus S$'s behavior of $\mathcal{A}^{H \setminus S}$ so that when the measurement outcome of the bit indicating whether $x \in S$ (i.e., the output of $\mathbf{1}_S$) is one, it immediately measures the registers X and halts with the measurement outcome as the output. This yields a non-unitary implementation of our desired algorithm. We then carefully implement its procedure in a coherent way and obtain the unitary version of the algorithm suitable for our amplitude amplification.

We then apply the amplitude amplification algorithm with this unitary quantum oracle algorithm and obtain our AA-enhanced SC-O2H theorem. The concrete theorem formulation is shown in Subsect. 4.2, with the proof and a detailed construction of its corresponding algorithm to extract $x \in S$ shown in Appendix A.2.

In the technical overview above, we mainly focus on SC-O2H and explain the high-level ideas about how we obtain our AA-enhanced SC-O2H theorem. In Sect. 5, we also extend our techniques to MRE-O2H [10] to get AA-enhanced MRE-O2H, and explain why our technique is inapplicable to the original O2H [19].

2 Preliminaries

For a set S , we denote $\mathbf{1}_S$ as the indicator function of S , which outputs 1 if $x \in S$ and 0 otherwise. For a linear operator A , we use $A^\dagger$ to denote its adjoint (i.e., conjugate transpose). We denote $\text{supp}(\cdot)$ as the support. For a discrete distribution D over a space $\mathcal{X}$, its support is defined as $\text{supp}(D) = \{x \in \mathcal{X} \mid D(x) > 0\}$. For a projector P over a Hilbert space $\mathcal{H}$ (see Subsect. 2.2), its support is defined as $\text{supp}(P) = \{|y\rangle = P|x\rangle \mid |x\rangle \in \mathcal{H}\}$.

For $r \in \mathbb{R}$, we write $\lceil r \rceil$ for the least integer greater than or equal to r , $\lfloor r \rfloor$ for the greatest integer less than or equal to r , and $\lfloor r \rfloor := \lfloor r + \frac{1}{2} \rfloor$ for the nearest integer to r . We make use of the rounding error bound $|\lfloor r \rfloor - r| \leq \frac{1}{2}$.

2.1 Mathematical Background

We use the following mathematical results in our work.

AM-GM inequality. For any set of real numbers $a_1, a_2, \dots, a_n$, we have the AM-GM inequality (i.e., the inequality of arithmetic and geometric means):

$$\frac{1}{n}(a_1 + a_2 + \dots + a_n) \geq (a_1 a_2 \dots a_n)^{1/n}. \quad (2)$$

Jensen's inequality. For a concave function f , non-negative weights $\alpha_1, \alpha_2, \dots, \alpha_n$ summing to 1, and real numbers $x_1, x_2, \dots, x_n$ in the domain of f , we have

$$\sum_{i=1}^n \alpha_i f(x_i) \leq f\left(\sum_{i=1}^n \alpha_i x_i\right). \quad (3)$$

The inequality reverses when f is convex.

Estimation of the natural constant e . For $x \geq 1$, we have the following inequalities:

$$\left(1 + \frac{1}{x}\right)^x \leq e \quad \text{and} \quad \left(1 - \frac{1}{x}\right)^x \leq \frac{1}{e}. \quad (4)$$

Sum of trigonometric functions [4, Lemma 1]. For any real number α and any integer $n > 0$, we have the sum

$$\sum_{j=0}^{n-1} \cos((2j+1)\alpha) = \frac{\sin(2n\alpha)}{2\sin\alpha}. \quad (5)$$

Now we state the bound of probability in a repeated independent trial and the bound of the probability in randomized Grover iterations.

Lemma 1 (Bound of Repeated Independent Trials). *Let $t \geq 1$ and $0 \leq p \leq 1$. Then*

$$1 - (1-p)^t \geq \frac{e-1}{e} \cdot \min\{1, tp\}.$$

Proof. We proceed by distinguishing three cases according to the value of p .

Case 1: $p = 0$: In this case, since $1 - (1-p)^t = tp = 0$, the inequality is trivial.

Case 2: $0 < p < \frac{1}{t}$: In this case, we consider the function $f(p) = \frac{1-(1-p)^t}{p}$. We observe that for $0 \leq p < 1$, its derivative

$$\begin{aligned} f'(p) &= \frac{tp(1-p)^{t-1} - 1 + (1-p)^t}{p^2} = \frac{(1-p)^{t-1}(1-p+tp) - 1}{p^2} \\ &\leq \frac{\left(\frac{(t-1)(1-p)+(1-p+tp)}{t}\right)^t - 1}{p^2} = 0. \end{aligned}$$

The inequality here is from (2) (i.e., the AM-GM inequality). This indicates that $f(p)$ is a decreasing function on $(0, 1)$. Therefore, for $0 \leq p < \frac{1}{t}$,

$$f(p) \geq f\left(\frac{1}{t}\right) = t - t\left(1 - \frac{1}{t}\right)^t \stackrel{(4)}{\leq} \left(1 - \frac{1}{e}\right)t.$$

This shows by definition of $f(p)$ that, for $0 \leq p < \frac{1}{t}$,

$$1 - (1-p)^t \geq \frac{e-1}{e}tp.$$

Case 3: $\frac{1}{t} \leq p \leq 1$: In this case, we observe that $1 - (1 - p)^t$ is an increasing function on $[0, 1]$ w.r.t. p . Therefore,

$$1 - (1 - p)^t \geq 1 - \left(1 - \frac{1}{t}\right)^t \stackrel{(4)}{\leq} 1 - \frac{1}{e} = \frac{e - 1}{e} \cdot 1.$$

By combining the above three cases, Lemma 1 follows. $\square$

Lemma 2 (Bound of Randomized Grover iterations). *Let $m \geq 1$ be an integer and let $\psi \in [0, \pi/4]$. If j is uniformly distributed over $\{0, 1, \dots, m - 1\}$, then*

$$\mathbb{E}_j [\sin^2((2j + 1)\psi)] \geq \min \left\{ \frac{1}{4}, \frac{4m^2}{\pi^2} \sin^2 \psi \right\}. \quad (6)$$

The proof of Lemma 2 is provided in Appendix A.1.

2.2 Quantum Computation

We rely on the common notation as in [18] for quantum computation. For completeness, we provide an introduction to the notations that we use.

Basic notations. Let $\mathcal{H}$ be a finite-dimensional complex Hilbert space, representing the state space of a quantum system. We represent the vectors in $\mathcal{H}$ and its dual space with the standard bra-ket notation.

Let X be a quantum register with its state space being $\mathcal{H}_X$. We use the register's name as subscripts for vectors and operators. Specifically, we denote $|\cdot\rangle_X$ and $\langle\cdot|_X$ as vectors in $\mathcal{H}_X$ and its dual space, respectively. Another way of describing the state of register X is using the density operator $\rho_X \in \mathcal{L}(\mathcal{H}_X)$. A density operator over the Hilbert space $\mathcal{H}_X$ is a positive semidefinite linear operator $\rho_X: \mathcal{H}_X \rightarrow \mathcal{H}_X$ satisfying $\text{Tr}(\rho) = 1$. If there are multiple registers' names written in the subscripts, it represents vectors or operators of a multi-register system.

For multi-register systems, the state space is the tensor product of the single-register spaces with an implicitly fixed register order. To simplify notation, we use subscripts to permute registers as needed, and the displayed tensor-product order is immaterial.

For a finite nonempty set $\mathcal{X}$, a register X over $\mathcal{X}$ means a binary quantum register encoding the elements of $\mathcal{X}$. We write $|x\rangle_X$ for the computational basis state encoding $x \in \mathcal{X}$.

Unitary quantum operations. Unitary quantum operations are unitary operators $U: \mathcal{H} \rightarrow \mathcal{H}$ acting on quantum states. We use subscripts to denote the register(s) on which a quantum operation acts. When a unitary operation U_X acts on register X , an initial state represented by a state vector $|\phi\rangle_X$ or a density operator ρ_X evolves to $U|\phi\rangle_X$ or $U\rho_X U^\dagger$, respectively.

Projective measurements. A projective measurement M is defined by the collection of orthogonal projectors $\{P_m\}$, where P_m is a projector onto the

eigenspace of $\mathbf{M}$ corresponding to the eigenvalue m . The projectors satisfy the completeness relation $\sum_m \mathbf{P}_m = I$, where I is the identity operator. When a quantum state $|\psi\rangle$ is measured using $\mathbf{M}$, the probability of obtaining result m is given by $p(m) = \langle\psi| \mathbf{P}_m |\psi\rangle$, and the post-measurement state collapses to $\frac{\mathbf{P}_m |\psi\rangle}{\sqrt{p(m)}}$ if outcome m is observed.

We abuse the eigenvalue m itself to represent the classical output of the measurement corresponding to $\mathbf{P}_m$.

Quantum algorithms. A quantum algorithm $\mathcal{A}$ is described with a quantum circuit that performs a mix of quantum and classical operations on its initial state, and outputs a (possibly mixed) quantum state.

In our applications, the output of the quantum algorithm can be represented alternatively as a tuple $(c, |\phi\rangle)$, where c is the classical part of the output, and $|\phi\rangle$ is guaranteed to be a pure state conditioned on c . Either of the two may be absent for certain algorithms presented.

Besides, we allow the quantum algorithm $\mathcal{A}$ to accept input $z = (z_1, |z_2\rangle_{Z_2})$ in the form of a mix of classical input and quantum pure state input. Specifically, when we feed the input $z = (z_1, |z_2\rangle_{Z_2})$ to the algorithm, we assume w.l.o.g. that $\mathcal{A}^\mathcal{O}(z)$ first encodes the input into a pure quantum state $|z\rangle_Z \otimes |0\rangle_W$ as the algorithm's initial state, where W represents the additional working register for $\mathcal{A}^\mathcal{O}$'s execution, and $|z\rangle_Z = |z_1\rangle_{Z_1} \otimes |z_2\rangle_{Z_2}$ encodes the encoded input with Z_1 being a fresh register for encoding the classical part z_1 .

We evaluate the computational cost of a quantum algorithm with its circuit size $\text{SIZE}(\mathcal{A})$, which counts the number of elementary gates performed in the quantum circuit. We evaluate the spacial cost of a quantum algorithm with its circuit width $\text{WIDTH}(\mathcal{A})$, which counts the number of qubits used in the quantum circuit.

Since each elementary gate acts on only a constant number of qubits, if $\text{WIDTH}(\mathcal{A}) = \omega(\text{SIZE}(\mathcal{A}))$, then the number of qubits ever touched by the circuit is $O(\text{SIZE}(\mathcal{A}))$ and the remaining qubits are not involved in the computation and thus can simply be discarded. We therefore assume throughout the paper that $\text{WIDTH}(\mathcal{A}) = O(1) \cdot \text{SIZE}(\mathcal{A})$ for every quantum algorithm $\mathcal{A}$ without loss of generality if not otherwise specified.

Quantum oracles. We model a quantum oracle $\mathcal{O}$ as a black-box quantum operation acting on a fixed group of designated registers specified in advance, called its *query registers* and denoted by R . The operation is not necessarily unitary. A query to $\mathcal{O}$ applies $\mathcal{O}_R$ to these registers while leaving all other registers unchanged.

For a classical function $F : \mathcal{X} \rightarrow \mathcal{Y}$, we reuse F to denote the quantum oracle acting on query registers X over $\mathcal{X}$ and Y over $\mathcal{Y}$ via the transformation

$$|x\rangle |y\rangle \rightarrow |x\rangle |y \oplus F(x)\rangle,$$

where $\oplus$ denotes bitwise XOR.

Quantum oracle algorithms. A quantum oracle algorithm $\mathcal{A}^\mathcal{O}$ is a quantum algorithm that is given black-box access to an oracle $\mathcal{O}$. It performs a mix of

quantum and classical operations between oracle queries (and prior to the first oracle query).

Although we treat the quantum oracle algorithm as performing a mix of classical and quantum operations, it is widely known that one can transform such operations into one unitary quantum circuit, with only a constant factor computational overhead. Formally, we state this fact as the following lemma.

Lemma 3. *For any quantum algorithm $\mathcal{A}^\mathcal{O}(z)$ that queries the oracle $\mathcal{O}$ at most q times, there exists a sequence of unitary quantum operations $\{\mathbf{U}_0, \mathbf{U}_1, \dots, \mathbf{U}_q\}$ and a projective measurement $\mathbf{M}_\mathcal{A}$, such that the normal form of the algorithm*

$$\mathcal{A}_u^\mathcal{O} := \mathbf{M}_\mathcal{A} \circ \mathbf{U}_q \circ \mathcal{O} \circ \dots \circ \mathbf{U}_1 \circ \mathcal{O} \circ \mathbf{U}_0$$

satisfies:

1. *The circuit size is $\text{SIZE}(\mathcal{A}_u^\mathcal{O}) = O(1) \cdot \text{SIZE}(\mathcal{A}^\mathcal{O})$.*
2. *For all inputs z , the outputs of $\mathcal{A}_u^\mathcal{O}(z)$ and $\mathcal{A}^\mathcal{O}(z)$ (in terms of mixed quantum states) are identical.*

Parallel queries and query depth. In some settings, such as those considered in [1,15,10], a quantum oracle algorithm may make several queries to $\mathcal{O}$ in parallel. Formally, $\mathcal{O}$ is replaced by the parallel oracle $\mathcal{O}_{R_1 R_2 \dots R_n}^{\otimes n}$, which acts as $\mathcal{O}$ on each group of query registers R_i , for $i \in \{1, 2, \dots, n\}$ in parallel. We call n the *query width*, and the total number of invocations to the parallel oracle the *query depth* d .

When writing a quantum oracle algorithm $\mathcal{A}^\mathcal{O}$, we implicitly allow it to make parallel queries and analyze it in terms of its query depth and query width. In particular, saying that $\mathcal{A}^\mathcal{O}$ has query width n means that we interpret its oracle access as access to $\mathcal{O}^{\otimes n}$.

3 Warm-up: Repetition-Enhanced O2H

3.1 Semi-classical O2H

Let us recall the semi-classical oracle and the punctured oracle, and then recall the semi-classical (SC) O2H lemma proposed in [1].

Definition 1 (Semi-Classical Oracle and Punctured Oracle). *Let $\mathbf{1}_S(x)$ be an indicator function for a set $S \subseteq \mathcal{X}$, which outputs 1 if $x \in S$ and 0 otherwise. A semi-classical oracle $\mathcal{O}_S^{\text{SC}}$ for a set S is defined as follows: on input $|x\rangle_X$, it computes and measures $\mathbf{1}_S(x)$ in an auxiliary qubit $|\mathbf{1}_S(x)\rangle$ indicating whether $x \in S$ or not. For an oracle H , the punctured oracle $H \setminus S$ is the oracle H punctured on S , which upon an input $|x\rangle_X |y\rangle_Y$ first queries $\mathcal{O}_S^{\text{SC}}$ on $|x\rangle_X$ and then queries H on $|x\rangle_X |y\rangle_Y$.*

Let Find denote the event that, in at least one of the queries made to $H \setminus S$, the measurement of the membership bit produced by $\mathbf{1}_S$ yields outcome 1. Then, we state the semi-classical O2H theorem by [1].

Theorem 2 (Semi-Classical O2H [1]). Let $S \subset \mathcal{X}$ be a random set. Let $H, G : \mathcal{X} \rightarrow \mathcal{Y}$ be random functions satisfying $\forall x \notin S, H(x) = G(x)$. Let $z \in \{0, 1\}^*$ be a random bit string. Suppose S, H, G, z are sampled from an arbitrary joint distribution $\mathcal{D}$. Let $\mathcal{A}$ be a quantum oracle algorithm of query depth d .

Let

$$P_{\text{left}} := \Pr[b = 1 : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^H(z)], \quad (7)$$

$$P_{\text{right}} := \Pr[b = 1 : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^G(z)], \quad (8)$$

$$\begin{aligned} P_{\text{Find}} &:= \Pr[\text{Find} : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, \mathcal{A}^{H \setminus S}(z)] \\ &= \Pr[\text{Find} : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, \mathcal{A}^{G \setminus S}(z)]. \end{aligned}$$

Then

$$|P_{\text{left}} - P_{\text{right}}| \leq 2\sqrt{(d+1) \cdot P_{\text{Find}}} \text{ and } \left| \sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}} \right| \leq 2\sqrt{(d+1) \cdot P_{\text{Find}}}.$$

Moreover, the theorem also holds with the bound $\sqrt{(d+1)P_{\text{Find}}}$ for the following alternative definitions of P_{right} .

$$P_{\text{right}} := \Pr[b = 1 : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^{H \setminus S}(z)], \quad (9)$$

$$P_{\text{right}} := \Pr[b = 1 \wedge \neg \text{Find} : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^{H \setminus S}(z)], \quad (10)$$

$$P_{\text{right}} := \Pr[b = 1 \wedge \neg \text{Find} : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^{G \setminus S}(z)], \quad (11)$$

$$P_{\text{right}} := \Pr[b = 1 \vee \text{Find} : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^{H \setminus S}(z)], \quad (12)$$

$$P_{\text{right}} := \Pr[b = 1 \vee \text{Find} : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^{G \setminus S}(z)], \quad (13)$$

As proved in [1], Theorem 2 with P_{right} defined as in (9) implies its other variations (8), (10)–(13). In the following, we will focus on this variant, henceforth referred to as the *asymmetric form* of Theorem 2, and denote it simply by Theorem 2 when there is no ambiguity. Moreover, as discussed in the introduction, Theorem 2 is proved via an equivalent proposition, which states that the theorem remains true pointwise for any instance (S, H, G, z) in the support of $\mathcal{D}$. The asymmetric form of this proposition is formalized in the following lemma.

Lemma 4 (Fixed SC-O2H [1]). Fix S, H, z . Let the symbols be as defined in Theorem 2. Let

$$\begin{aligned} P_{\text{left}}^{S, H, z} &:= \Pr[b = 1 : b \leftarrow \mathcal{A}^H(z)], \\ P_{\text{right}}^{S, H, z} &:= \Pr[b = 1 : b \leftarrow \mathcal{A}^{H \setminus S}(z)], \\ P_{\text{Find}}^{S, H, z} &:= \Pr[\text{Find} : \mathcal{A}^{G \setminus S}(z)] = \Pr[\text{Find} : \mathcal{A}^{H \setminus S}(z)]. \end{aligned}$$

Then

$$|P_{\text{left}}^{S, H, z} - P_{\text{right}}^{S, H, z}| \leq \sqrt{(d+1) \cdot P_{\text{Find}}^{S, H, z}} \text{ and } \left| \sqrt{P_{\text{left}}^{S, H, z}} - \sqrt{P_{\text{right}}^{S, H, z}} \right| \leq \sqrt{(d+1) \cdot P_{\text{Find}}^{S, H, z}}. \quad (14)$$

Remark 1. Suppose one can implement the semi-classical oracle $\mathcal{O}_S^{\text{SC}}$ locally, and the outcome of its membership measurement is exposed in the implementation. Then for any algorithm with access to this oracle, one can do modifications to make it output an element $x \in S$ whenever Find occurs.

Indeed, upon measuring the membership outcome 1, the modified algorithm aborts, measures the query register X in the computational basis, and outputs the result x . Since the membership measurement has projected X onto the subspace spanned by $\{|x\rangle : \mathbf{1}_S(x) = 1\}$, the resulting outcome satisfies $x \in S$ with probability 1.

In semi-classical O2H, if we modify the adversary $\mathcal{A}^{H \setminus S}$ using this approach, we then obtain an algorithm that outputs $x \in S$ with probability P_{Find} . This aligns with the form of a common adversary in a one-way security game.

3.2 Main Theorem from Repetition

We begin our statement with the fixed version of our main theorem.

Lemma 5 (Fixed SC-O2H, repetition-enhanced). *Fix S, H, z . Let the symbols be defined as in Lemma 4 and Theorem 2. Let $t = d + 1$. Let $\mathcal{B}_{\text{rep}}^{H, \mathbf{1}_S}(z)$ be a quantum algorithm that operates as follows:*

- $\mathcal{B}_{\text{rep}}^{H, \mathbf{1}_S}(z)$ simulates $H \setminus S$ with its oracles H and $\mathbf{1}_S$, and runs $\mathcal{A}^{H \setminus S}(z)$ repeatedly t times.
- $\mathcal{B}_{\text{rep}}^{H, \mathbf{1}_S}(z)$ outputs 1 whenever the event Find occurs in at least one round of the simulated $\mathcal{A}^{H \setminus S}(z)$, and outputs 0 otherwise.

Let $P_{\text{frep}}^{S, H, z} = \Pr[\mathcal{B}_{\text{rep}}^{H, \mathbf{1}_S}(z) = 1]$. Then

$$|P_{\text{left}}^{S, H, z} - P_{\text{right}}^{S, H, z}| \leq \sqrt{\frac{e}{e-1} \cdot P_{\text{frep}}^{S, H, z}} \text{ and } \left| \sqrt{P_{\text{left}}^{S, H, z}} - \sqrt{P_{\text{right}}^{S, H, z}} \right| \leq \sqrt{\frac{e}{e-1} \cdot P_{\text{frep}}^{S, H, z}}.$$

We note that $\mathcal{B}_{\text{rep}}^{H, \mathbf{1}_S}(z)$ is able to detect the occurrence of the event Find for each round of the simulated $\mathcal{A}^{H \setminus S}(z)$, as it is providing $\mathcal{A}$ with the punctured oracle $G \setminus S$. The Find event's occurring means that $\mathcal{B}$'s measurement of an output of the semi-classical oracle of function $\mathbf{1}_S$ returns 1. When $\mathcal{B}$ obtains this measurement outcome, it can immediately abort this round of repetition and conclude that the Find event occurs.

Proof (Lemma 5). As the parameters S, H, z are all fixed, the Find events in different rounds of repetition are independent. Therefore,

$$P_{\text{frep}}^{S, H, z} = 1 - (1 - P_{\text{Find}}^{S, H, z})^t.$$

By Lemma 1, we have

$$P_{\text{frep}}^{S, H, z} \geq \frac{e-1}{e} \min\{1, tP_{\text{Find}}^{S, H, z}\}.$$

Observe that $P_{\text{left}}^{S,H,z}$ and $P_{\text{right}}^{S,H,z}$ are probabilities, so

$$|P_{\text{left}}^{S,H,z} - P_{\text{right}}^{S,H,z}| \leq 1 \text{ and } \left| \sqrt{P_{\text{left}}^{S,H,z}} - \sqrt{P_{\text{right}}^{S,H,z}} \right| \leq 1. \quad (15)$$

With Lemma 4, this indicates that

$$|P_{\text{left}}^{S,H,z} - P_{\text{right}}^{S,H,z}| \leq \min \left\{ 1, \sqrt{t \cdot P_{\text{Find}}^{S,H,z}} \right\} \leq \sqrt{\frac{e}{e-1} P_{\text{frep}}^{S,H,z}}$$

and $\left| \sqrt{P_{\text{left}}^{S,H,z}} - \sqrt{P_{\text{right}}^{S,H,z}} \right| \leq \min \left\{ 1, \sqrt{t \cdot P_{\text{Find}}^{S,H,z}} \right\} \leq \sqrt{\frac{e}{e-1} P_{\text{frep}}^{S,H,z}}.$

This completes the proof of Lemma 5. $\square$

With Lemma 5, we are ready to state our theorem, the repetition-enhanced semi-classical O2H (SC-O2H) theorem.

Theorem 3 (SC-O2H, repetition-enhanced). *Let $S \subset \mathcal{X}$ be random. Let $H, G : \mathcal{X} \rightarrow \mathcal{Y}$ be random functions satisfying $\forall x \notin S, H(x) = G(x)$. Let $z \in \{0, 1\}^*$ be a random bit string. Suppose S, H, G, z are sampled from an arbitrary joint distribution $\mathcal{D}$.*

Let $\mathcal{A}$ be a quantum algorithm of query depth d .

Let $\mathcal{B}_{\text{rep}}^{H, 1_S}(z)$ be the quantum algorithm as described in Lemma 5.

Let P_{left} and P_{right} be defined as in (7) and (8), respectively, and let

$$P_{\text{frep}} := \Pr[b = 1 : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{B}_{\text{rep}}^{H, 1_S}(z)].$$

Then

$$|P_{\text{left}} - P_{\text{right}}| \leq 2\sqrt{\frac{e}{e-1} \cdot P_{\text{frep}}} \text{ and } \left| \sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}} \right| \leq 2\sqrt{\frac{e}{e-1} \cdot P_{\text{frep}}}. \quad (16)$$

Moreover, the theorem also holds with the bound $\sqrt{\frac{e}{e-1} \cdot P_{\text{frep}}}$ for the alternative definitions of P_{right} as in (9)–(13).

Proof (Theorem 3). As in the proof of Theorem 2, the theorem with P_{right} defined by (9) implies the versions with P_{right} defined by (8) or (10)–(13). Hence it suffices to prove the theorem under the definition of P_{right} in (9).

Under the definition in (9), the probabilities P_{left} , P_{right} , and P_{frep} depend only on the marginal distribution of (S, H, z) , which we denote by $\mathcal{D}'$. For each $(S, H, z) \in \text{supp}(\mathcal{D}')$, let

$$\alpha_{S,H,z} := \Pr_{(S', H', z') \xleftarrow{\$} \mathcal{D}'} [(S', H', z') = (S, H, z)].$$

Then

$$\begin{aligned}
|P_{\text{left}} - P_{\text{right}}| &= \left| \sum_{(S,H,z) \in \text{supp}(\mathcal{D}')} \alpha_{S,H,z} \cdot (P_{\text{left}}^{S,H,z} - P_{\text{right}}^{S,H,z}) \right| \\
&\leq \sum_{(S,H,z) \in \text{supp}(\mathcal{D}')} \alpha_{S,H,z} \cdot |P_{\text{left}}^{S,H,z} - P_{\text{right}}^{S,H,z}| \\
&\stackrel{\text{Lem. 5}}{\leq} \sum_{(S,H,z) \in \text{supp}(\mathcal{D}')} \alpha_{S,H,z} \cdot \sqrt{\frac{e}{e-1}} \cdot P_{\text{frep}}^{S,H,z} \\
&\stackrel{(*)}{\leq} \sqrt{\frac{e}{e-1}} \cdot \sum_{(S,H,z) \in \text{supp}(\mathcal{D}')} \alpha_{S,H,z} P_{\text{frep}}^{S,H,z} \\
&= \sqrt{\frac{e}{e-1}} \cdot P_{\text{frep}},
\end{aligned}$$

where the inequality $(*)$ follows from (3) (i.e., Jensen's inequality). Then we obtain the first inequality of (16).

For the difference of the square roots, we have

$$\left| \sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}} \right| = \left| \sqrt{\sum_{(S,H,z) \in \text{supp}(\mathcal{D}')} \alpha_{S,H,z} \cdot P_{\text{left}}^{S,H,z}} - \sqrt{\sum_{(S,H,z) \in \text{supp}(\mathcal{D}')} \alpha_{S,H,z} \cdot P_{\text{right}}^{S,H,z}} \right|.$$

We can treat the RHS as the difference between the Euclidean norms of two vectors $\mathbf{v}_{\text{left}}$ and $\mathbf{v}_{\text{right}}$, both indexed by $(S,H,z) \in \text{supp}(\mathcal{D}')$, whose entries are $(\mathbf{v}_{\text{left}})_{S,H,z} := \sqrt{\alpha_{S,H,z} \cdot P_{\text{left}}^{S,H,z}}$ and $(\mathbf{v}_{\text{right}})_{S,H,z} := \sqrt{\alpha_{S,H,z} \cdot P_{\text{right}}^{S,H,z}}$, respectively. With this notation, we write

$$\begin{aligned}
\left| \sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}} \right| &= \left| \|\mathbf{v}_{\text{left}}\| - \|\mathbf{v}_{\text{right}}\| \right| \leq \|\mathbf{v}_{\text{left}} - \mathbf{v}_{\text{right}}\| \\
&= \sqrt{\sum_{(S,H,z) \in \text{supp}(\mathcal{D}')} \alpha_{S,H,z} \cdot \left(\sqrt{P_{\text{left}}^{S,H,z}} - \sqrt{P_{\text{right}}^{S,H,z}} \right)^2} \\
&\stackrel{\text{Lem. 5}}{\leq} \sqrt{\sum_{(S,H,z) \in \text{supp}(\mathcal{D}')} \alpha_{S,H,z} \cdot \frac{e}{e-1} \cdot P_{\text{frep}}^{S,H,z}} \\
&= \sqrt{\frac{e}{e-1}} \cdot P_{\text{frep}}.
\end{aligned}$$

This completes the proof of Theorem 3. $\square$

4 Amplitude-Amplification-Enhanced O2H

In this section, we state our main contribution, the Amplitude-Amplification-enhanced Semi-Classical O2H (AA-enhanced SC-O2H) theorem. In Subsect. 4.1,

after recalling the Grover iteration, we present an adapted amplitude amplification algorithm to our needs. In Subsect. 4.2, we describe our AA-enhanced SC-O2H theorem.

4.1 Amplitude amplification with randomized iteration counts

In this subsection, we present an adapted amplitude amplification algorithm in [5] which restricts the number of times of running Grover iteration to have an upper bound.

We first recall Grover iteration.

Let U be a unitary quantum circuit and P be an orthogonal projector. Suppose $\psi = \arcsin \|PU|0\rangle\| \in (0, \frac{\pi}{2})$. Let $|\varphi\rangle = U|0\rangle$ be the initial state of the system and let $|\alpha\rangle = \frac{P|\varphi\rangle}{\|P|\varphi\rangle\|}$ and $|\beta\rangle = \frac{(I-P)|\varphi\rangle}{\|(I-P)|\varphi\rangle\|}$. Grover iteration is constructed with two reflections over the real plane spanned by $|\alpha\rangle$ and $|\beta\rangle$:

- A unitary operation representing the reflection about the vector $|\beta\rangle$

$$R = -P + (I - P) = I - 2P.$$

In other words, R reverses the phase of the component in the support of P .

- A unitary operation representing the reflection about the vector $|\varphi\rangle$:

$$\hat{U} = 2|\varphi\rangle\langle\varphi| - I = U(2|0\rangle\langle 0| - I)U^\dagger.$$

One round of Grover iteration applies the product $Q := \hat{U}R$ of the two reflections, rotating a vector on the real plane by 2ψ .

The following lemma states the effect of one iteration of Grover search algorithm on the state of the system.

Lemma 6 (Grover iteration). *After t rounds of Grover iteration on the initial state $|\varphi\rangle$, the final state of the system becomes*

$$\left(\hat{U}R\right)^t |\varphi\rangle = \sin((2t+1)\psi) |\alpha\rangle + \cos((2t+1)\psi) |\beta\rangle.$$

Proof. We have $|\varphi\rangle = \sin(\psi) |\alpha\rangle + \cos(\psi) |\beta\rangle$. On the real plane spanned by $|\alpha\rangle$ and $|\beta\rangle$, the product $Q = \hat{U}R$ of the two reflections acts as a rotation by 2ψ . Hence the angle after j iterations is $(2j+1)\psi$, which gives the claimed evolution of the system.

We now state the concrete algorithm adapted from the amplitude amplification algorithm in [5] as the algorithm below. This adaptation gives an upper bound on the resulting algorithm's circuit size and a lower bound on its success probability analogous to that of the repetitive approach in Sect. 3. The algorithm's procedure is given in the proof.

Theorem 4 (Amplitude amplification, adapted). *Let U be a unitary quantum circuit, let P be an orthogonal projector, and let $k \in \mathbb{N}$ with $k \geq 1$. There exists a randomized quantum algorithm $\mathcal{A}_{U,P,k}$ such that*

$$\Pr[|\phi\rangle \in \text{supp}(P) : (j, |\phi\rangle) \leftarrow \mathcal{A}_{U,P,k}] \geq \min \left\{ \frac{1}{4}, \frac{4}{\pi^2} k \|\text{PU}|0\rangle\|^2 \right\}.$$

Moreover, the circuit size is

$$\text{SIZE}(\mathcal{A}_{U,P,k}) = O(\sqrt{k}) \cdot (\text{SIZE}(U) + \text{SIZE}(R) + \text{WIDTH}(U)), \quad (17)$$

where $R = I - 2P$.

Proof (Theorem 4). Let $Q = \hat{U}R$ be the operation of Grover iteration. Denote $m := \lceil \sqrt{k} \rceil$. Let the projective measurement that measures the vectors in the support of P to 1 be

$$M := \{P_0 = I - P, P_1 = P\}.$$

The algorithm proceeds as follows.

1. Run $U|0\rangle$. Then measure the resulting state with the projective measurement M . If the measurement outcome is one, output $(-1, |\phi\rangle)$ and halt, where $|\phi\rangle$ is the post-measurement state.
2. Otherwise, sample j uniformly from $\{0, 1, \dots, m-1\}$ and run $(Q^j \circ U)|0\rangle$. Then measure the resulting state with M and output $(j, |\phi\rangle)$, where $|\phi\rangle$ is the post-measurement state.

Let $p = \|\text{PU}|0\rangle\|^2$; we distinguish three cases w.r.t. p .

Case 1: $p = 0$: In this case, the claim is immediate since $\frac{4}{\pi^2} k \|\text{PU}|0\rangle\|^2 = 0$.

Case 2: $p \geq \frac{1}{2}$: In this case, consider the success probability in the first step. The projective measurement M measures $U|0\rangle$ to 1 with probability $\|\text{PU}|0\rangle\|^2 = p \geq \frac{1}{2}$. Note that the post-measurement state of M naturally lies in $\text{supp}(P)$ by definition, if the measurement outcome is 1. Therefore, in this case,

$$\Pr[|\phi\rangle \in \text{supp}(P) : (j, |\phi\rangle) \leftarrow \mathcal{A}_{U,P,k}] \geq p \geq \frac{1}{2}.$$

Case 3: $0 \leq p \leq \frac{1}{2}$: In this case, we denote F_1 as the event that the algorithm fails to halt in the first step and runs into the second step. We consider the situation conditioned on the event F_1 .

Let $\psi = \arcsin \sqrt{p} \in (0, \frac{\pi}{4})$. Let $|\varphi\rangle = U|0\rangle$ be the initial state before applying Grover iteration. Let $|\alpha\rangle = \frac{P|\varphi\rangle}{\|P|\varphi\rangle\|}$ and $|\beta\rangle = \frac{(I-P)|\varphi\rangle}{\|(I-P)|\varphi\rangle\|}$. Then, Grover iteration Q rotates the vector $|\varphi\rangle$ on the real plane spanned by $|\alpha\rangle$ and $|\beta\rangle$.

By Lemma 6, the resulting state after applying j rounds of Grover iteration is

$$Q^j \circ U|0\rangle = \sin((2j+1)\psi) |\alpha\rangle + \cos((2j+1)\psi) |\beta\rangle.$$

Therefore, for uniformly sampled $j \xleftarrow{\$} \{0, 1, \dots, m-1\}$, the probability of measuring the resulting state to 1 is

$$\mathbb{E}_j \left[\left\| \mathbf{P}(\mathbf{Q}^j \circ \mathbf{U} | 0) \right\|^2 \right] = \mathbb{E}_j \left[\sin^2((2j+1)\psi) \right] \geq \min \left\{ \frac{1}{4}, \frac{4m^2}{\pi^2} \sin^2 \psi \right\},$$

where the final inequality is from Lemma 2.

Therefore,

$$\begin{aligned} & \Pr[|\phi\rangle \in \text{supp}(\mathbf{P}) : (j, |\phi\rangle) \leftarrow \mathcal{A}_{\mathbf{U}, \mathbf{P}, k}] \\ &= \Pr[F_1] + \Pr[\neg F_1] \Pr[|\phi\rangle \in \text{supp}(\mathbf{P}) \mid \neg F_1 : (j, |\phi\rangle) \leftarrow \mathcal{A}_{\mathbf{U}, \mathbf{P}, k}] \\ &= p + (1-p) \mathbb{E}_j \left[\left\| \mathbf{P}(\mathbf{Q}^j \circ \mathbf{U} | 0) \right\|^2 \right] \\ &\geq p + (1-p) \min \left\{ \frac{1}{4}, \frac{4m^2}{\pi^2} \sin^2 \psi \right\} \\ &\geq \min \left\{ \frac{1}{4}, \frac{4m^2}{\pi^2} \sin^2 \psi \right\}. \end{aligned}$$

By the fact that $\sin^2 \psi = p$ and $m^2 \geq k$, we conclude that

$$\Pr[|\phi\rangle \in \text{supp}(\mathbf{P}) : (j, |\phi\rangle) \leftarrow \mathcal{A}_{\mathbf{U}, \mathbf{P}, k}] \geq \min \left\{ \frac{1}{4}, \frac{4}{\pi^2} kp \right\}.$$

With all three cases above, we obtain the claimed bound on the probability as in Theorem 4.

For the circuit size, recall that $\mathbf{Q} = \hat{\mathbf{U}}\mathbf{R} = \mathbf{U}(2|0\rangle\langle 0| - I)\mathbf{U}^\dagger$. The operation $\mathbf{U}^\dagger$ can be constructed from the implementation of $\mathbf{U}$ and uses the same amount of basic quantum gates, while the operation $(2|0\rangle\langle 0| - I)$ is a reflection about $|0\rangle$ that can be implemented with $O(1) \cdot \text{WIDTH}(\mathbf{U})$ basic quantum gates.

As the algorithm applies at most $m-1$ Grover iterations $\mathbf{Q}$, along with some cheap classical operations, it follows the stated circuit size in (17).

This completes the proof of Theorem 4. $\square$

In our applications, the algorithm is allowed to access some quantum oracles. The quantum operation $\mathbf{U}$ and the quantum operation $\mathbf{R} = I - 2\mathbf{P}$ might be implemented with oracle invocations. We also want to apply the amplitude amplification algorithm on such implementations of quantum operations.

It is not always possible to apply the same technique as in Theorem 4 to extend the probabilities in the presence of quantum oracles $\mathcal{O}$, as it might be hard to implement $\mathcal{O}^\dagger$ required in the construction of $\hat{\mathbf{U}}$. However, for a unitary oracle, if it is also Hermitian (i.e., $\mathcal{O}^\dagger = \mathcal{O}$), invoking $\mathcal{O}^\dagger$ is equivalent to invoking $\mathcal{O}$ itself. Therefore, for a quantum algorithm with access to such oracle, we have the following corollary.

Corollary 1. *Let the notation be as in Theorem 4. Let $\mathcal{O}$ be a unitary and Hermitian quantum oracle. Suppose U and $R = I - 2P$ are quantum oracle circuits whose query width is n . Let their query depths be d_u and d_r , respectively. Then the constructed $\mathcal{A}_{U,P,k}$ is a quantum oracle circuit with query width n and query depth at most $O(\sqrt{k}) \cdot (d_u + d_r)$. Moreover, its circuit size is*

$$\text{SIZE}(\mathcal{A}_{U,P,k}) = O(\sqrt{k}) (\text{SIZE}(U) + \text{SIZE}(R) + \text{WIDTH}(U)).$$

We further note that a standard oracle of a classical function $F : \mathcal{X} \rightarrow \mathcal{Y}$ that performs the transform $|x\rangle_X |y\rangle_Y \rightarrow |x\rangle_X |y \oplus F(x)\rangle_Y$ is naturally a Hermitian quantum oracle. Therefore, for an implementation with oracle access to a standard oracle of a classical function, the above corollary holds.

4.2 Main Theorem from Amplitude Amplification

With amplitude amplification, we construct a new algorithm that achieves the same bound as in Theorem 3 up to a constant factor, but much more efficiently.

Theorem 5 (SC-O2H enhanced with Amplitude Amplification). *Let $S \subset \mathcal{X}$ be a random set. Let $H, G : \mathcal{X} \rightarrow \mathcal{Y}$ be random functions satisfying $\forall x \notin S, H(x) = G(x)$. Let $z \in \{0, 1\}^*$ be a random bit string. Suppose S, H, G, z are sampled from an arbitrary joint distribution $\mathcal{D}$. Let $\mathcal{A}$ be a quantum oracle algorithm with query depth d and query width n . Let $\mathcal{B}_{aa}^{H, 1_S}$ be the quantum algorithm whose construction is described later in the proof (cf. Appendix A.2). Let P_{left} and P_{right} be defined as in (7) and (8), respectively, and let*

$$P_{\text{fgs}} := \Pr[x^\circ \in S : (S, H, z) \xleftarrow{\$} \mathcal{D}, x^\circ \leftarrow \mathcal{B}_{aa}^{H, 1_S}(z)].$$

Then

$$|P_{\text{left}} - P_{\text{right}}| \leq 2\sqrt{4P_{\text{fgs}}} \text{ and } \left| \sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}} \right| \leq 2\sqrt{4P_{\text{fgs}}},$$

Moreover, the theorem also holds with the bound $\sqrt{4 \cdot P_{\text{frep}}}$ for the alternative definitions of P_{right} as in (9)–(13).

Besides, $\mathcal{B}_{aa}^{H, 1_S}$ has circuit size

$$\text{SIZE}(\mathcal{B}_{aa}^{H, 1_S}) = O(\sqrt{d}) \cdot \text{SIZE}(\mathcal{A}^{H \setminus S}) + O(d^{3/2} n \log |\mathcal{X}|),$$

and, fixing its query width to n , queries both the H and 1_S oracles with query depth $O(d\sqrt{d})$.

Similar to Theorem 3, Theorem 5 is derived from a lemma stating its fixed version.

Lemma 7 (Fixed SC-O2H, AA-enhanced). *Fix S, H, z . Let the symbols be as defined in Lemma 4. Denote $k = d + 1$. Let $\mathcal{B}_{aa}^{H, 1_S}$ be the quantum algorithm whose construction is described later in the proof (cf. Appendix A.2). Let*

$$P_{\text{fgs}}^{S, H, z} := \Pr[x^\circ \in S : x \leftarrow \mathcal{B}_{aa}^{H, 1_S}(z)].$$

Then

$$|P_{\text{left}}^{S,H,z} - P_{\text{right}}^{S,H,z}| \leq \sqrt{4P_{\text{fgs}}^{S,H,z}} \text{ and } \left| \sqrt{P_{\text{left}}^{S,H,z}} - \sqrt{P_{\text{right}}^{S,H,z}} \right| \leq \sqrt{4P_{\text{fgs}}^{S,H,z}}. \quad (18)$$

Moreover, $\mathcal{B}_{\text{aa}}^{H,1_S}$ has circuit size

$$\text{SIZE}(\mathcal{B}_{\text{aa}}^{H,1_S}) = O(\sqrt{d}) \cdot \text{SIZE}(\mathcal{A}^{H \setminus S}) + O(d^{3/2} n \log |\mathcal{X}|),$$

and, fixing its query width to n , queries both the H and 1_S oracles with query depth $O(d\sqrt{d})$.

The proof of Theorem 5 from Lemma 7 is identical to how we prove Theorem 3 from Lemma 5, so we are left with proving Lemma 7. We refer to the technical overview in Subsect. 1.3 for a high-level overview, and postpone the formal proof of Lemma 7 to Appendix A.2.

5 Extending Other Variants of O2H

In this section, we discuss how our techniques can be applied to other variants of the O2H theorem. First, we show our technique is applicable to the “double-sided” variants of O2H theorems in Subsect. 5.1. By “double-sided” variants, we refer to the variants of O2H theorems in which the adversary has oracle access to both G and H , which include the initial DS-O2H theorem [2], the MRM-O2H theorem [15] and the MRE-O2H theorem [10]. Then, we show that our technique is inapplicable to the original O2H theorem [19] in Subsect. 5.2.

5.1 Applicability to Double-Sided Variants

We show that our technique can be applied to the Measure-Rewind-Extract (MRE) O2H theorem [10], which is the most recent and tightest variant of the “double-sided” variants of O2H theorems.

The MRE-O2H theorem constructs an algorithm that has access to the oracle 1_S , which aligns with the requirement of our technique. We therefore state an analogous extended version of the MRE-O2H theorem with our technique.

We first recall the Fixed MRE-O2H lemma from [10].

Lemma 8 (Fixed MRE-O2H [10]). *Let z be a fixed bit string and $S \subset \mathcal{X}$ be a fixed set. Let $H, G : \mathcal{X} \rightarrow \mathcal{Y}$ be fixed functions such that $H(x) = G(x)$ for all $x \notin S$. Let $\mathcal{A}$ be a quantum algorithm with query depth d and query width n . There exists a quantum algorithm $\mathcal{B}^{H,G,1_S}$ such that*

$$|P_{\text{left}} - P_{\text{right}}| \leq 4\sqrt{d}P_{\text{find}},$$

where

$$\begin{aligned} P_{\text{left}}^{S,H,G,z} &:= \Pr[b = 1 : b \leftarrow \mathcal{A}^H(z)], \\ P_{\text{right}}^{S,H,G,z} &:= \Pr[b = 1 : b \leftarrow \mathcal{A}^G(z)], \\ P_{\text{find}}^{S,H,G,z} &:= \Pr[T_B \cap S \neq \emptyset : T_D \leftarrow \mathcal{B}^{H,G,1_S}(z)]. \end{aligned}$$

Moreover, $\mathcal{B}^{H,G,1_S}$ has a circuit size of $O(1) \cdot \text{SIZE}(\mathcal{A})$, its query depths to H , G and 1_S oracles are at most $O(d)$ with query width n , and $|T_D| \leq 2n$.

Unlike Theorem 2 (i.e., the SC-O2H theorem [1]), the MRE-O2H theorem [10] and its fixed-input version explicitly construct a quantum algorithm that outputs a list T_B satisfying $T_B \cap S \neq \emptyset$. This makes our technique easier to apply.

Intuitively, we can use Lemma 3 to convert the quantum algorithm $\mathcal{B}^{H,G,1_S}$ from Lemma 8 into its unitary form, and then apply Theorem 4 in the same manner as in the proof of Lemma 7. This yields the fixed-input version of an extended MRE-O2H lemma with Grover search. Taking the expectation over the distribution $\mathcal{D}$ then gives the theorem stated below.

Theorem 6 (MRE-O2H with Grover Search). *Let $S \subset \mathcal{X}$ be random. Let $H, G : \mathcal{X} \rightarrow \mathcal{Y}$ be random functions such that $H(x) = G(x)$ for all $x \notin S$. Let $z \in \{0, 1\}^*$ be a random bit string. Suppose S, H, G, z are sampled from an arbitrary joint distribution $\mathcal{D}$. Let $\mathcal{A}$ be a quantum algorithm with query depth d . There exists a quantum algorithm $\mathcal{B}_{aa}^{H,G,1_S}$ such that*

$$|P_{\text{left}} - P_{\text{right}}| \leq 16P_{\text{fgs}}, \quad (19)$$

where

$$\begin{aligned} P_{\text{left}} &:= \Pr[b = 1 : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^H(z)], \\ P_{\text{right}} &:= \Pr[b = 1 : (S, H, G, z) \xleftarrow{\$} \mathcal{D}, b \leftarrow \mathcal{A}^G(z)], \\ P_{\text{fgs}} &:= \Pr[x^\circ \in S : (S, H, z) \xleftarrow{\$} \mathcal{D}, x^\circ \leftarrow \mathcal{B}_{aa}^{H,G,1_S}(z)]. \end{aligned}$$

Moreover, $\mathcal{B}_{aa}^{H,G,1_S}$ has a circuit size of $O\left(d^{\frac{1}{4}}\right) \cdot \text{SIZE}(\mathcal{A})$, and its query depths to H , G and 1_S oracles are at most $O\left(d^{\frac{5}{4}}\right)$.

Since the proof of Theorem 6 follows the same structure as that of Theorem 5, we omit the full details here.

As for the earlier variants of DS-O2H and MRM-O2H, we note that the constructed adversaries in both the DS-O2H theorem and the MRM-O2H theorem don't have access to 1_S , and applying our technique will additionally require the resulting algorithm to query the oracle 1_S .

However, as discussed in [10], the requirement of oracle access to 1_S is not essential in the double-sided variants, as one can simulate 1_S by querying H and G . For intuition, if an algorithm can simulate H and G simultaneously, then for the set S that H and G differ on, it can compute $1_S(x)$ efficiently on an input x by checking whether $H(x) = G(x)$.

This observation shows that our technique can likewise be applied to the DS-O2H and MRM-O2H theorems, yielding variants with tighter probability loss while retaining the full range of applications of the original results.

Nonetheless, MRE-O2H and our extension thereof already cover every application of MRM-O2H and provide a more efficient algorithm. Consequently, improving the probability loss in the DS-O2H and MRM-O2H theorems offers no practical benefit.

5.2 Inapplicability to the Original O2H theorem

As the resulting algorithm of our technique must have access to the oracle $\mathbf{1}_S$, our technique cannot be applied directly to the original O2H theorem, whose constructed algorithm has no access to $\mathbf{1}_S$.

Nonetheless, as discussed in [1], the original O2H theorem [19] is implied by the semi-classical O2H theorem. The implication relies on the following theorem.

Theorem 7 (Search in semi-classical oracle [1]). *Let $\mathcal{A}$ be a quantum algorithm with query depth d to a semi-classical oracle with domain $\mathcal{X}$. Let $S \subseteq \mathcal{X}$ and $z \in \{0,1\}^*$ be random with an arbitrary joint distribution.*

Let $\mathcal{B}$ be an algorithm that, on input z , picks $i \xleftarrow{\$} \{1, \dots, d\}$, runs $\mathcal{A}^{\text{O}_\emptyset^{\text{SC}}}$ until just before the i -th query to the semi-classical oracle, measures all the input registers of the i -th parallel query and outputs the measurement outcomes as a list T . Then

$$\Pr[\text{Find} : \mathcal{A}^{\text{O}_S^{\text{SC}}}(z)] \leq 4d \cdot \Pr[T \cap S \neq \emptyset : T \leftarrow \mathcal{B}(z)].$$

By definition, the semi-classical oracle $\text{O}_\emptyset^{\text{SC}}$ acts as the identity on its input. So instead of querying an oracle, $\mathcal{B}$ can also simulate $\text{O}_\emptyset^{\text{SC}}$ locally by essentially doing nothing to the oracle's input. This indicates that using this theorem, one can extract the element $x \in S$ found during queries to the semi-classical oracle, without having to decide whether an input x is in S .

One might suspect applying our AA-based enhancement to the SC-O2H theorem can yield the AA-enhanced version of the original O2H theorem with the help of Theorem 7. However, this is not the case.

Theorem 7 indeed relies on the fact that the semi-classical oracle is non-unitary and performs measurement within the oracle. However, our AA-based enhancement requires us to implement the semi-classical oracle coherently, with the inverse of that coherent implementation also applied to the system in the last half of a Grover iteration. This does not align with the requirement of Theorem 7.

In fact, replacing the coherent implementation of O_S^{SC} with that of $\text{O}_\emptyset^{\text{SC}}$ in the algorithm $\mathcal{B}_{\text{aa}}^{H,1_S}$ of Theorem 5 is of no use for obtaining an AA-enhanced version of the original O2H theorem, since this replacement removes the amplification itself. To see this, the replacement changes the projector $\text{P}_{\mathcal{A},H,S}$ to $\text{P}_{\mathcal{A},H,\emptyset}$, obtained by setting $S = \emptyset$ in (25). This projector has empty support, so $\text{P}_{\mathcal{A},H,\emptyset} = \mathbf{0}$ and the corresponding reflection becomes $\text{R} = I - 2\text{P}_{\mathcal{A},H,\emptyset} = I$.

Let $|\varphi\rangle = \text{U}|0\rangle$ be the state prepared before the Grover iterations in the modified algorithm. Since $\hat{\text{U}} = 2|\varphi\rangle\langle\varphi| - I$ is the reflection about $|\varphi\rangle$, we have

$$(\hat{\text{U}}\text{R})^t |\varphi\rangle = \hat{\text{U}}^t |\varphi\rangle = |\varphi\rangle.$$

Thus, every Grover iteration leaves the prepared state unchanged, and increasing the number of iterations cannot improve the success probability.

In fact, our AA-enhanced SC-O2H theorem (Theorem 5) does not have access to the semi-classical oracle. Instead, it can access the unitary oracle $\mathbf{1}_S$ directly. This does not align with the requirement of Theorem 7.

Remark 2. We classified the SC-O2H theorem as a *checkable variant* in the introduction because, by definition, one can simulate the oracle $H \setminus S$ with the oracles $\mathbf{1}_S$ and H and this is also the most direct way of simulating $H \setminus S$. This type of simulation is seen in various security proofs, including the proofs of IND-CCA security of the $\mathbf{U}^\perp$, $\mathbf{U}_m^\perp$, $\mathbf{U}^\times$, and $\mathbf{U}_m^\times$ transformations in [10].

However, as we have discussed, one can also use Theorem 7 (i.e., the search in the semi-classical oracle theorem) to complete the reduction without having to simulate $\mathbf{1}_S$, at the cost of introducing an extra security loss factor of $O(d)$. Since this approach requires essentially only oracle access to H , and implies a security loss at the same order as the original O2H theorem, it is more natural to treat such application of the SC-O2H theorem as a one-sided variant of the O2H theorem.

We also note that our amplitude-amplification-based enhancement doesn't apply to this type of SC-O2H usage, since no oracle access to $\mathbf{1}_S$ is provided after using Theorem 7.

6 Applications to Existing Security Proofs

In this section, we discuss how to replace the use of SC-O2H and MRE-O2H in the existing security proofs with our AA-enhanced O2H theorems. We first briefly recall how to use the O2H theorems in typical security proofs. Then, we state the conditions under which our AA-enhanced O2H theorems can replace the original theorems, and show a (probably incomplete) list of existing proofs that satisfy the requirements.

Typical usage of the O2H theorems in a hybrid argument consists of the following steps:

1. For a pair of hybrid games that differs only on the oracle used, compose the game into one algorithm $\mathcal{A}(z)$ that has oracle access to either oracle $\mathcal{O} \in \{H, G\}$, with input z containing both global inputs to the hybrid games, and inputs prepared by the challenger in the hybrid game before the challenger's first query to the oracle.
2. Apply the O2H theorem to $\mathcal{A}(z)$ to construct an adversary $\mathcal{B}_{\text{OW}}(z)$ to find the element in the set S , which has oracle access according to the theorem's variant.
3. Bound the advantage of the adversary $\mathcal{B}_{\text{OW}}(z)$ via the underlying hardness assumption(s) and/or information-theoretic arguments, possibly through a further sequence of hybrid games. Doing so typically requires simulating the oracle access of $\mathcal{B}_{\text{OW}}(z)$, since the underlying hardness does not provide such oracle access.

For proofs using the SC-O2H theorem and the MRE-O2H theorem and following such paradigm (excluding those proofs that rely on the *search in the semi-classical oracle theorem* in [1]), our enhanced O2H theorems can be used to replace their corresponding original O2H theorems in the second step directly

without affecting the rest of the proof, if the reduction in the third step is performed with a hybrid argument such that each transition between consecutive hybrid games satisfies either of the following conditions:

- *The reduction step is performed in a black-box manner.* By black-box, we mean that the reduction does not use the internal structure of $\mathcal{B}_{\text{OW}}$ during the reduction, but only manipulates its input z and the oracle access of $\mathcal{B}_{\text{OW}}$ according to the O2H theorem’s variant.
- *The reduction step does not affect success probability.* In this case, the hybrid game may change the internal structure of $\mathcal{B}_{\text{OW}}$, under the restriction that such a change must not affect its success probability.

Such conditions might seem restrictive; however, they indeed fit into a broad class of existing proofs using the checkable variants and the double-sided variants of O2H theorems. We provide a list of examples where the proofs satisfy the above conditions in Table 4. As we discussed above, we can apply our AA-enhanced SC-O2H theorem and AA-enhanced MRE-O2H theorem in these proofs instead of the original SC-O2H theorem and MRE-O2H theorem and obtain new bounds for the security loss. See also Table 3 in Subsect. 1.2.

Table 4: A (probably incomplete) list of security proofs in which our AA-enhanced O2H theorems can be used as a direct replacement. Here, CKS denotes the Cash–Kiltz–Shoup security model for non-interactive key exchange (NIKE) as defined in [6], and DS-IND denotes the ciphertext indistinguishability requirement of disjoint simulatability [16].

O2H Type	Scheme	Primitive	Target Security
SC-O2H	$\mathcal{U}^\mathcal{X}$ [14, Theorem 6]	KEM	IND-CCA
	$\mathcal{U}^\perp$ [14, Theorem 7]		
	$\mathcal{U}_m^\mathcal{X}$ [14, Theorem 8]		
	$\mathcal{U}_m^\perp$ [14, Theorem 9]		
	GA-HDH [8, Theorem 5]	NIKE	CKS
MRE-O2H	$\mathcal{U}^\mathcal{X}$ [10, Theorem 6]	KEM	IND-CPA
	$\mathcal{U}_m^\perp$ [10, Theorem 9]		
MRM-O2H*	KC [16, Theorem 1]	KEM	DS-IND
	GA-HEG [8, Theorem 3]	NIKE	CKS

* For the listed proofs based on MRM-O2H, we use the technique stated in [10] to lift them to using MRE-O2H, and then use our technique to apply amplitude-amplification-based enhancement.

References

1. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva, A., Micciancio, D. (eds.) *Advances in Cryptology – CRYPTO 2019, Part II. Lecture Notes in Computer Science*, vol. 11693, pp. 269–295. Springer, Cham, Switzerland, Santa Barbara, CA, USA (Aug 18–22, 2019). https://doi.org/10.1007/978-3-030-26951-7_10
2. Bindel, N., Hamburg, M., Hövelmanns, K., Hülsing, A., Persichetti, E.: Tighter proofs of CCA security in the quantum random oracle model. In: Hofheinz, D., Rosen, A. (eds.) *TCC 2019: 17th Theory of Cryptography Conference, Part II. Lecture Notes in Computer Science*, vol. 11892, pp. 61–90. Springer, Cham, Switzerland, Nuremberg, Germany (Dec 1–5, 2019). https://doi.org/10.1007/978-3-030-36033-7_3
3. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) *Advances in Cryptology – ASIACRYPT 2011. Lecture Notes in Computer Science*, vol. 7073, pp. 41–69. Springer Berlin Heidelberg, Germany, Seoul, South Korea (Dec 4–8, 2011). https://doi.org/10.1007/978-3-642-25385-0_3
4. Boyer, M., Brassard, G., Høyer, P., Tapp, A.: Tight bounds on quantum searching. *Fortschritte der Physik* **46**(4-5), 493–505 (1998). [https://doi.org/https://doi.org/10.1002/\(SICI\)1521-3978\(199806\)46:4/5<493::AID-PROP493>3.0.CO;2-P](https://doi.org/https://doi.org/10.1002/(SICI)1521-3978(199806)46:4/5<493::AID-PROP493>3.0.CO;2-P), <https://onlinelibrary.wiley.com/doi/abs/10.1002/%28SICI%291521-3978%28199806%2946%3A4/5%3C493%3A%3AAID-PROP493%3E3.0.CO%3B2-P>
5. Brassard, G., Høyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. *AMS Contemporary Mathematics Series* **305** (06 2000). <https://doi.org/10.1090/conm/305/05215>
6. Cash, D., Kiltz, E., Shoup, V.: The twin Diffie-Hellman problem and applications. *Journal of Cryptology* **22**(4), 470–504 (Oct 2009). <https://doi.org/10.1007/s00145-009-9041-6>
7. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Online-extractability in the quantum random-oracle model. In: Dunkelman, O., Dziembowski, S. (eds.) *Advances in Cryptology – EUROCRYPT 2022, Part III. Lecture Notes in Computer Science*, vol. 13277, pp. 677–706. Springer, Cham, Switzerland, Trondheim, Norway (May 30 – Jun 3, 2022). https://doi.org/10.1007/978-3-031-07082-2_24
8. Duman, J., Hartmann, D., Kiltz, E., Kunzweiler, S., Lehmann, J., Riepel, D.: Group action key encapsulation and non-interactive key exchange in the QROM. In: Agrawal, S., Lin, D. (eds.) *Advances in Cryptology – ASIACRYPT 2022, Part II. Lecture Notes in Computer Science*, vol. 13792, pp. 36–66. Springer, Cham, Switzerland, Taipei, Taiwan (Dec 5–9, 2022). https://doi.org/10.1007/978-3-031-22966-4_2
9. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M.J. (ed.) *Advances in Cryptology – CRYPTO’99. Lecture Notes in Computer Science*, vol. 1666, pp. 537–554. Springer Berlin Heidelberg, Germany, Santa Barbara, CA, USA (Aug 15–19, 1999). https://doi.org/10.1007/3-540-48405-1_34
10. Ge, J., Liao, H., Xue, R.: Measure-rewind-extract: Tighter proofs of one-way to hiding and CCA security in the quantum random oracle model. In: Chung, K.M., Sasaki, Y. (eds.) *Advances in Cryptology – ASIACRYPT 2024, Part IV. Lecture Notes in Computer Science*, vol. 15487, pp. 3–34. Springer, Singapore, Singapore, Kolkata, India (Dec 9–13, 2024). https://doi.org/10.1007/978-981-96-0894-2_1

11. Grilo, A.B., Hövelmanns, K., Hülsing, A., Majenz, C.: Tight adaptive reprogramming in the QROM. In: Tibouchi, M., Wang, H. (eds.) *Advances in Cryptology – ASIACRYPT 2021, Part I. Lecture Notes in Computer Science*, vol. 13090, pp. 637–667. Springer, Cham, Switzerland, Singapore (Dec 6–10, 2021). https://doi.org/10.1007/978-3-030-92062-3_22
12. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325–328 (Jul 1997). <https://doi.org/10.1103/PhysRevLett.79.325>, <https://link.aps.org/doi/10.1103/PhysRevLett.79.325>
13. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. In: Kalai, Y., Reyzin, L. (eds.) *TCC 2017: 15th Theory of Cryptography Conference, Part I. Lecture Notes in Computer Science*, vol. 10677, pp. 341–371. Springer, Cham, Switzerland, Baltimore, MD, USA (Nov 12–15, 2017). https://doi.org/10.1007/978-3-319-70500-2_12
14. Jiang, H., Zhang, Z., Ma, Z.: Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model. In: Ding, J., Steinwandt, R. (eds.) *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019*, pp. 227–248. Springer, Cham, Switzerland, Chongqing, China (May 8–10, 2019). https://doi.org/10.1007/978-3-030-25510-7_13
15. Kuchta, V., Sakzad, A., Stehlé, D., Steinfeld, R., Sun, S.: Measure-rewind-measure: Tighter quantum random oracle model proofs for one-way to hiding and CCA security. In: Canteaut, A., Ishai, Y. (eds.) *Advances in Cryptology – EUROCRYPT 2020, Part III. Lecture Notes in Computer Science*, vol. 12107, pp. 703–728. Springer, Cham, Switzerland, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45727-3_24
16. Liu, X., Wang, M.: QCCA-secure generic key encapsulation mechanism with tighter security in the quantum random oracle model. In: Garay, J. (ed.) *PKC 2021: 24th International Conference on Theory and Practice of Public Key Cryptography, Part I. Lecture Notes in Computer Science*, vol. 12710, pp. 3–26. Springer, Cham, Switzerland, Virtual Event (May 10–13, 2021). https://doi.org/10.1007/978-3-030-75245-3_1
17. National Institute of Standards and Technology (NIST): Post-quantum cryptography pqc - security (evaluation criteria). NIST Computer Security Resource Center (CSRC) (2025), [https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-\(evaluation-criteria\)](https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria))
18. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press (2010)
19. Unruh, D.: Revocable quantum timed-release encryption. In: Nguyen, P.Q., Oswald, E. (eds.) *Advances in Cryptology – EUROCRYPT 2014. Lecture Notes in Computer Science*, vol. 8441, pp. 129–146. Springer Berlin Heidelberg, Germany, Copenhagen, Denmark (May 11–15, 2014). https://doi.org/10.1007/978-3-642-55220-5_8
20. Yamakawa, T., Zhandry, M.: Classical vs quantum random oracles. In: Canteaut, A., Standaert, F.X. (eds.) *Advances in Cryptology – EUROCRYPT 2021, Part II. Lecture Notes in Computer Science*, vol. 12697, pp. 568–597. Springer, Cham, Switzerland, Zagreb, Croatia (Oct 17–21, 2021). https://doi.org/10.1007/978-3-030-77886-6_20

Appendix

A Postponed Proofs

A.1 Proofs of Lemma 2

We distinguish between three cases w.r.t. ψ .

Case 1: $\psi = 0$: The claim is immediate since $\sin^2((2j+1)\psi) = 0$.

Case 2: $0 < m\psi < \frac{\pi}{4}$: For every $0 \leq j \leq m-1$, we have $(2j+1)\psi < \frac{\pi}{2}$. Then, it holds that

$$\mathbb{E}_j [\sin^2((2j+1)\psi)] \geq \frac{4\psi^2}{m\pi^2} \sum_{j=0}^{m-1} (2j+1)^2 \quad (20)$$

$$\begin{aligned} &= \frac{4(4m^2-1)}{3\pi^2} \psi^2 \\ &\geq \frac{4m^2}{\pi^2} \sin^2 \psi. \end{aligned} \quad (21)$$

Here, (20) is by the fact that $\sin x \geq \frac{2}{\pi}x$ for $x \in [0, \frac{\pi}{2}]$ and (21) is from the fact that $x \geq \sin x$ for all $x \geq 0$.

Case 3: $m\psi \geq \frac{\pi}{4}$: In this case, with (5), we have

$$\frac{1}{m} \sum_{j=0}^{m-1} \sin^2((2j+1)\psi) = \frac{1}{2m} \sum_{j=0}^{m-1} (1 - \cos 2(2j+1)\psi) = \frac{1}{2} - \frac{\sin(4m\psi)}{4m \sin(2\psi)}. \quad (22)$$

Since $\psi \leq \pi/4$, concavity of the sine function gives $\sin(2\psi) \geq 4\psi/\pi$. Therefore $4m \sin(2\psi) \geq \frac{16m\psi}{\pi} \geq 4$. Then, (22) yields

$$\mathbb{E}_j [\sin^2((2j+1)\psi)] \geq \frac{1}{2} - \frac{1}{4m \sin(2\psi)} \geq \frac{1}{4}.$$

By combining the above three cases, Lemma 2 follows. $\square$

A.2 Proof of Lemma 7

We will describe the construction of $\mathcal{B}_{aa}^{H,1s}$ and show that it satisfies the claimed bounds in Lemma 7. In a nutshell, our construction extends the quantum algorithm $\mathcal{A}^{H \setminus S}(z)$ defined in Lemma 4 using the technique of quantum amplitude amplification [5].

Proof (Lemma 7). As $\mathcal{A}^{H \setminus S}(z)$ queries the punctured oracle $H \setminus S$ with query width n , we treat it as having access to the parallel oracle $(H \setminus S)^{\otimes n}$.

By Lemma 3, we transform $\mathcal{A}^{H \setminus S}(z)$ to its normal form $\mathcal{C}_{\mathcal{A},z}^{H \setminus S}$ as shown in Fig. 1. Here, $X = X_1 \cdots X_n$ and $Y = Y_1 \cdots Y_n$ are the joint input and output

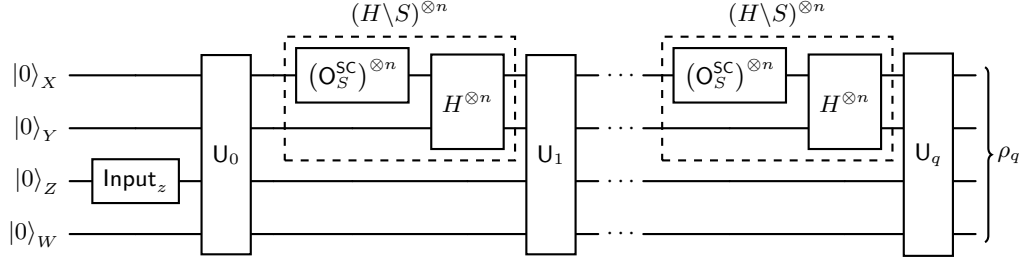


Fig. 1: A quantum circuit $C_{A,z}^{H\setminus S}$ representing $\mathcal{A}^{(H\setminus S)^{\otimes n}}(z)$. Here Input_z transforms $|0\rangle_Z$ to $|0 \oplus z\rangle_Z$, preparing the input z onto the register Z . $U_0, U_1, \dots, U_q$ are unitary operators. One of the qubits within W measures to the output of $\mathcal{A}^{H\setminus S}(z)$. $H\setminus S$ is the punctured oracle as defined in Definition 1, represented by a non-unitary quantum operation. ρ_q is the density operator of $\mathcal{A}$'s final state.

registers of $(H\setminus S)^{\otimes n}$, where the j -th component query applies $H\setminus S$ on the registers X_j and Y_j for each $j \in \{1, \dots, n\}$. We note that $C_{A,z}^{H\setminus S}$ as a whole is not unitary, since the punctured oracle $H\setminus S$ is not unitary.

In order to apply the amplitude amplification technique, i.e., Theorem 4, we construct a unitary quantum oracle circuit $C_{A,z}'^{H,1_S}$ along with a projector $P_{A,H,S}$.

Construction of $C_{A,z}'^{H,1_S}$. For $i \in \{1, 2, \dots, d\}$ and $j \in \{1, 2, \dots, n\}$, denote the operation CCX as the transform on the computational basis:

$$\text{CCX}_{T_{ij}X_jX'_{ij}} : |t_{ij}\rangle_{T_{ij}} |x_j\rangle_{X_j} |x'_{ij}\rangle_{X'_{ij}} \rightarrow \begin{cases} |t_{ij}\rangle_{T_{ij}} |x_j\rangle_{X_j} |x'_{ij}\rangle_{X'_{ij}} & , t_{ij} = 0 \\ |t_{ij}\rangle_{T_{ij}} |x_j\rangle_{X_j} |x'_{ij} \oplus x_j\rangle_{X'_{ij}} & , t_{ij} = 1 \end{cases} \quad (23)$$

The circuit $C_{A,z}'^{H,1_S}$ runs identically to $C_{A,z}^{H\setminus S}$ except for the following modifications:

1. $C_{A,z}'^{H,1_S}$ introduces $2dn$ additional registers: for each $1 \leq i \leq d$ and $1 \leq j \leq n$, it introduces a 1-qubit register T_{ij} and a register X'_{ij} over the set $\mathcal{X}$. All the additional registers are initialized to $|0\rangle$;
2. When $C_{A,z}^{H\setminus S}$ queries the oracle $(H\setminus S)^{\otimes n}$ for the i -th time, $C_{A,z}'^{H,1_S}$ instead applies the unitary transform $\mathcal{S}_i^{H,1_S}$ shown in Fig. 2.

The unitary operation $\mathcal{S}_i^{H,1_S}$ is implemented with queries to the unitary oracles H and 1_S . So all operations and oracle calls in the circuit $C_{A,z}'^{H,1_S}$ are unitary. Therefore, $C_{A,z}'^{H,1_S}$ is a unitary quantum circuit. We also show the concrete representation of the circuit $C_{A,z}'^{H,1_S}$ in Fig. 3.

Definition of $P_{A,H,S}$. Let the circuit $C_{A,z}'^{H,1_S}$ work on the Hilbert space $\mathcal{H}_\Sigma$ spanned by

$$\Sigma := \left\{ |\mathbf{x}'\rangle_{X'} |\mathbf{t}\rangle_T |x\rangle_X |y\rangle_Y |z\rangle_Z |w\rangle_W \mid \begin{array}{l} \mathbf{x}' \in \mathcal{X}^{d \times n}, \mathbf{t} \in \{0, 1\}^{d \times n}, \\ x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}, w \in \mathcal{W} \end{array} \right\},$$

$\mathcal{S}_i^{H,1_S} \mathbf{x}\rangle_X \mathbf{y}\rangle_Y \mathbf{t}_i\rangle_{T_i} \mathbf{x}'_i\rangle_{X'_i}$
01: Apply $\mathbf{1}_S \left(x_j\rangle_{X_j} 0\rangle_{T_{ij}} \right)$ for $1 \leq j \leq n$
02: Apply $H \left(x_j\rangle_{X_j} Y_j\rangle_{Y_j} \right)$ for $1 \leq j \leq n$
03: Apply $\text{CCX} \left(t_{ij}\rangle_{T_{ij}} x_j\rangle_{X_j} 0\rangle_{X'_{ij}} \right)$ for $1 \leq j \leq n$

Fig. 2: The unitary simulation of the i -th oracle query to $H \setminus S$. Each line is performed in parallel for $1 \leq j \leq n$. The quantum operation CCX is defined in (23).

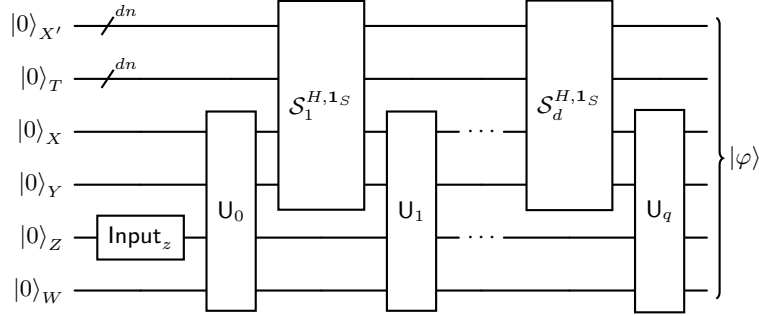


Fig. 3: The unitary quantum circuit $\mathcal{C}'_{\mathcal{A},z}{}^{H,1_S}$. Here the operation Input_z transforms $|0\rangle_Z$ to $|0 \oplus z\rangle_Z$, preparing the input z onto the register Z . $U_0, U_1, \dots, U_q$ are unitary operations. $\mathcal{S}_i^{H,1_S}$ for $i = 1, \dots, d$ are the unitary operations defined in Fig. 2.

where $\mathcal{Z}$ and $\mathcal{W}$ are collections of vectors as the computational basis of the registers Z and W , respectively.

Let

$$(i^*(\mathbf{t}), j^*(\mathbf{t})) := \min \{(i, j) \mid t_{ij} = 1\}, \quad (24)$$

where the minimum is taken w.r.t. the lexicographic order.

We define the projector

$$\mathbf{P}_{\mathcal{A},H,S} = \sum_{\psi \in \Sigma'} |\psi\rangle\langle\psi|, \quad (25)$$

where

$$\Sigma' = \left\{ |\mathbf{x}'\rangle_{X'} |\mathbf{t}\rangle_T |x\rangle_X |y\rangle_Y |z\rangle_Z |w\rangle_W \in \Sigma \mid \begin{array}{l} \exists 1 \leq i \leq q, \ t_i = 1 \wedge \\ x'_{i^*(\mathbf{t})j^*(\mathbf{t})} \in S \end{array} \right\}.$$

For a pure state $|\varphi\rangle \in \mathcal{H}_\Sigma$, let $\text{Extract}_{|\varphi\rangle}$ denote the event that measuring the registers T and X' in the computational basis yields outcomes $\mathbf{t}$ and $\mathbf{x}'$ satisfying $\mathbf{t} \neq \mathbf{0}$ and $x'_{i^*(\mathbf{t})j^*(\mathbf{t})} \in S$. Then by the definition of $\mathbf{P}_{\mathcal{A},H,S}$, we have

$$\Pr [\text{Extract}_{|\varphi\rangle}] = \|\mathbf{P}_{\mathcal{A},H,S} |\varphi\rangle\|^2. \quad (26)$$

We also state the properties of $C'_{\mathcal{A},z}{}^{H,1s}$ and $P_{\mathcal{A},H,S}$ in the following lemma.

Lemma 9. *When we apply the projector $P_{\mathcal{A},H,S}$ on the output of the circuit $C'_{\mathcal{A},z}{}^{H,1s}$, we have*

$$\Pr \left[\text{Find} : \mathcal{A}^{H \setminus S}(z) \right] = \Pr \left[\text{Extract}_{|\varphi\rangle} : |\varphi\rangle := C'_{\mathcal{A},z}{}^{H,1s} |0\rangle \right]. \quad (27)$$

A formal proof of Lemma 9 is given in Appendix A.3.

Construction of $R_{\mathcal{A},H,S} := I - 2P_{\mathcal{A},H,S}$. To implement the reflection operator $R_{\mathcal{A},H,S}$, we introduce ancilla registers C_0, C_1, C, X° , i.e., temporary registers initialized to fixed states and discarded after being disentangled from the system. Here C_0, C_1, C are 1-qubit registers, and X° is a register over $\mathcal{X}$. C_0, C_1, X° are initialized to $|0\rangle$ and C is initialized to $|-\rangle_C = \frac{1}{\sqrt{2}}(|0\rangle_C - |1\rangle_C)$.

Let measuring the output states of all the registers X', T in the computational basis yield outcomes $\mathbf{t} \in \{0, 1\}^{dn}$ and $\mathbf{x}' \in \mathcal{X}^{dn}$, respectively. There exists a trivial classical circuit that, on input $\mathbf{t}$ and $\mathbf{x}'$, outputs $(x^\circ, c_0) \in \mathcal{X} \times \{0, 1\}$ that satisfies: x° . Moreover, the classical circuit is of size $O(q \log |\mathcal{X}|)$.

This implies a quantum circuit, denoted by CK, whose size is $\text{SIZE}(\text{CK}) = O(q \log |\mathcal{X}|)$, that implements the operation

$$\begin{aligned} |\mathbf{x}'\rangle_{X'} |\mathbf{t}\rangle_T |c_0\rangle_{C_0} |x^\circ\rangle_{X^\circ} \mapsto & \\ & \begin{cases} |\mathbf{x}'\rangle_{X'} |\mathbf{t}\rangle_T |c_0^\circ \oplus 1\rangle_{C_0} |x^\circ \oplus x_k\rangle_{X^\circ}, & \mathbf{t} \neq \mathbf{0}; \\ |\mathbf{x}'\rangle_{X'} |\mathbf{t}\rangle_T |c_0\rangle_{C_0} |x^\circ\rangle_{X^\circ}, & \text{otherwise,} \end{cases} \end{aligned} \quad (28)$$

where C_0 and X° act as output registers.

With this subcircuit in place, we implement $R_{\mathcal{A},H,S}$ as a unitary operation, as shown in Fig. 4. Note that this implementation only applies a phase to the quantum state and therefore leaves the ancilla registers C_0, C_1, C, X° unentangled with the rest of the system. We may thus safely discard them afterwards.

With the construction of $C'_{\mathcal{A},z}{}^{H,1s}$ and $R = I - 2P_{\mathcal{A},H,S}$ and their properties, we are ready to show our construction of the algorithm $\mathcal{B}_{\text{aa}}^{H,1s}$.

Construction of $\mathcal{B}_{\text{aa}}^{H,1s}$. Applying Theorem 4 with $C'_{\mathcal{A},z}{}^{H,1s}$ as the unitary quantum circuit U , $P_{\mathcal{A},H,S}$ as the projection P and $k = d+1$ yields a unitary quantum circuit, denoted by $\mathcal{B}_{\mathcal{A},z}^{H,1s}$, such that

$$\begin{aligned} \Pr \left[\mathcal{B}_{\mathcal{A},z}^{H,1s} |0\rangle \in \text{supp}(P_{\mathcal{A},H,S}) \right] &\geq \min \left\{ \frac{1}{4}, \frac{4}{\pi^2} (d+1) \cdot \left\| P_{\mathcal{A},H,S} C'_{\mathcal{A},z}{}^{H,1s} |0\rangle \right\|^2 \right\} \\ &\geq \frac{1}{4} \cdot \min \left\{ 1, (d+1) \cdot \left\| P_{\mathcal{A},H,S} C'_{\mathcal{A},z}{}^{H,1s} |0\rangle \right\|^2 \right\}. \end{aligned} \quad (29)$$

Then, let the algorithm $\mathcal{B}_{\text{aa}}^{H,1s}(z)$ run as follows:

1. Run $(j, |\phi\rangle) \leftarrow \mathcal{B}_{\mathcal{A},z}^{H,1s}$ to obtain the final state $|\phi\rangle$.

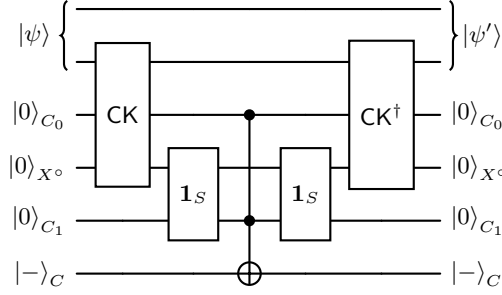


Fig. 4: The circuit of the reflection $R_{A,H,S} = I - 2P_{A,H,S}$. Here the top wire carries the registers $XYZW$ and the second wire the registers $X'T$; together they hold the system state $|\psi\rangle$. The bottom four wires are ancilla registers, initialized in $|0\rangle_{C_0} |0\rangle_{X^\circ} |0\rangle_{C_1} |-\rangle_C$ and discarded afterwards. The subcircuit CK computes the unitary operation defined in (28).

2. Measure registers T and X' of the final state $|\phi\rangle$ w.r.t. the computational basis to obtain classical outcomes $\mathbf{t} \in \{0, 1\}^{dn}$ and $\mathbf{x}' \in \mathcal{X}^{dn}$.
3. If $\mathbf{t} = 0$, halt immediately.
4. Otherwise, compute $(i^*(\mathbf{t}), j^*(\mathbf{t}))$ and return $x^\circ := x_{i^*(\mathbf{t})j^*(\mathbf{t})}$.

With this definition of $\mathcal{B}_{aa}^{H,1_S}$, we write

$$\begin{aligned}
P_{\text{fgs}}^{S,H,z} &= \Pr [x^\circ \in S : x^\circ \leftarrow \mathcal{B}_{aa}^{H,1_S}] \\
&\geq \Pr [\text{Extract}_{|\phi\rangle} : (j, |\phi\rangle) \leftarrow \mathcal{B}_{A,z}^{H,1_S}] \stackrel{(26)}{=} \mathbb{E}_{(j, |\phi\rangle) \leftarrow \mathcal{B}_{A,z}^{H,1_S}} \|\mathcal{P}_{A,H,S} |\phi\rangle\|^2 \\
&\geq \Pr [|\phi\rangle \in \text{supp}(\mathcal{P}_{A,H,S}) : (j, |\phi\rangle) \leftarrow \mathcal{B}_{A,z}^{H,1_S}] \\
&\stackrel{(29)}{\geq} \frac{1}{4} \cdot \min \left\{ 1, (d+1) \cdot \left\| \mathcal{P}_{A,H,S} \mathcal{C}'_{A,z}{}^{H,1_S} |0\rangle \right\|^2 \right\} \\
&\stackrel{\text{Lem. 91}}{\geq} \frac{1}{4} \cdot \min \left\{ 1, (d+1) \cdot P_{\text{find}}^{S,H,z} \right\}.
\end{aligned}$$

Now, recall (15) and (14), which state two upper bounds of the distinguishing advantage; we conclude that

$$\begin{aligned}
\left| P_{\text{left}}^{S,H,z} - P_{\text{right}}^{S,H,z} \right| &\leq \min \left\{ 1, \sqrt{(d+1) \cdot P_{\text{find}}^{S,H,z}} \right\} \leq \sqrt{4P_{\text{frep}}^{S,H,z}} \\
\text{and } \left| \sqrt{P_{\text{left}}^{S,H,z}} - \sqrt{P_{\text{right}}^{S,H,z}} \right| &\leq \min \left\{ 1, \sqrt{(d+1) \cdot P_{\text{find}}^{S,H,z}} \right\} \leq \sqrt{4P_{\text{frep}}^{S,H,z}}.
\end{aligned}$$

Circuit Size of $\mathcal{B}_{aa}^{H,1_S}$. Let L be the total number of qubits used by $\mathcal{A}^{H \setminus S}$'s registers in (qu)bits. To analyze the circuit size, we first recall that, by Theorem 4, the circuit size of $\mathcal{B}_{A,z}^{H,1_S}$ is

$$\text{SIZE}(\mathcal{B}_{A,z}^{H,1_S}) = O(\sqrt{d+1}) \cdot \left(\text{SIZE}(\mathcal{C}'_{A,z}{}^{H,1_S}) + \text{SIZE}(R_{A,H,S}) + \text{WIDTH}(\mathcal{C}'_{A,z}{}^{H,1_S}) \right).$$

By the construction of $C'_{\mathcal{A},z}{}^{H,1_S}$ and $R_{\mathcal{A},H,S}$, we write

$$\begin{aligned} \text{SIZE}(C'_{\mathcal{A},z}{}^{H,1_S}) &= O(1)\text{SIZE}(\mathcal{A}^{H\setminus S}) + O(dn \log |\mathcal{X}|) \\ \text{WIDTH}(C'_{\mathcal{A},z}{}^{H,1_S}) &= O(1) \cdot \left(\text{WIDTH}(\mathcal{A}^{H\setminus S}) + \text{SIZE}(\mathcal{A}^{H\setminus S}) + O(dn \log |\mathcal{X}|) \right) \\ &= O(1) \cdot \text{SIZE}(\mathcal{A}^{H\setminus S}) + O(dn \log |\mathcal{X}|) \\ \text{SIZE}(R_{\mathcal{A},H,S}) &= O(dn \log |\mathcal{X}|). \end{aligned}$$

Therefore, we conclude that

$$\text{SIZE}(B_{\mathcal{A},z}^{H,1_S}) = O(\sqrt{d}) \cdot \text{SIZE}(\mathcal{A}^{H\setminus S}) + O(d^{3/2}n \log |\mathcal{X}|).$$

This completes the proof of Lemma 7. $\square$

A.3 Proof of Lemma 9

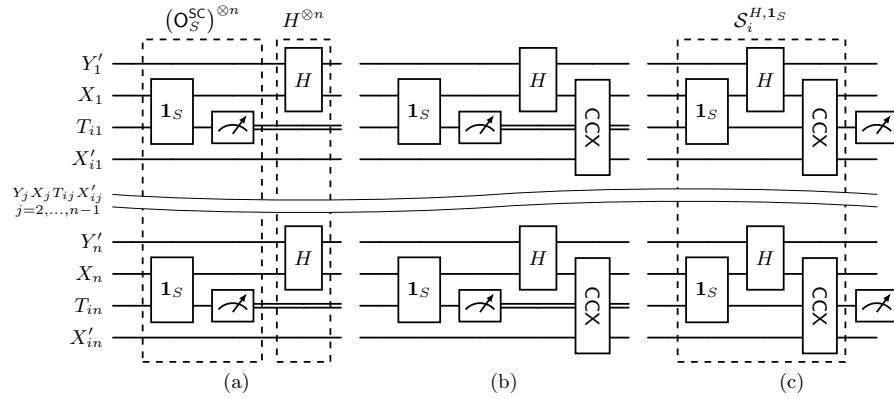


Fig. 5: The i -th query to the punctured oracle $H\setminus S$ and its replacement with the unitary operation $\mathcal{S}_i^{H,1_S}$. The operation CCX is defined as in (23). The registers $Y_j X_j T_{ij} X'_{ij}$ with $j = 2, \dots, n-1$ are omitted in the figure, but the same operation sequences are applied. The registers T_{ij} and X_{ij} for $j = 2, \dots, n-1$ are all initialized to $|0\rangle$.

We apply hybrid arguments to replace $(H\setminus S)^{\otimes n}$ with $\mathcal{S}_i^{H,1_S}$ defined in Fig. 2, and obtain our required equation.

First, we represent the algorithm $\mathcal{A}^{H\setminus S}$ with its normal form $C_{\mathcal{A},z}^{H\setminus S}$. Then we have

$$\Pr [\text{Find} : \mathcal{A}^{H\setminus S}(z)] = \Pr [\text{Find} : C_{\mathcal{A},z}^{H\setminus S} | 0\rangle].$$

Fig. 5(a) shows an equivalent representation of $(H\setminus S)^{\otimes n}$'s functionality for the i -th oracle query. This representation introduces two sets of internal registers

T_{ij} and X'_{ij} for $1 \leq i \leq d$ and $1 \leq j \leq n$, all of which are initialized to $|0\rangle$ and only touched during the i -th query to the oracle.

Fixing i , let Find_i be the event that at least one of the registers T_{ij} for $1 \leq j \leq n$ contains 1. Then we have

$$\begin{aligned} \Pr \left[\text{Find} : \mathcal{C}_{\mathcal{A},z}^{H \setminus S} |0\rangle \right] &= \Pr \left[\bigvee_{i=1}^d \text{Find}_i : \mathcal{C}_{\mathcal{A},z}^{H \setminus S} |0\rangle \right] \\ &= 1 - \prod_{i=1}^d \Pr \left[\neg \text{Find}_i : \mathcal{C}_{\mathcal{A},z}^{H \setminus S} |0\rangle \left| \bigwedge_{i'=1}^{i-1} \neg \text{Find}_{i'} \right. \right]. \end{aligned}$$

In Fig. 5(b), we add a series of parallel operations $\text{CCX}_{T_{ij}X_jX'_{ij}}$ for $1 \leq j \leq n$. We denote $\mathcal{S}_o$ as the oracle interface to $\mathcal{A}$ of the operation in Fig. 5(b), where the registers X_jY_j for $1 \leq j \leq n$ are the registers under $\mathcal{A}$'s control, and write $\mathcal{S}_{o,i}$ for the actual operation performed within the i -th query to $\mathcal{S}_o$.

In the first hybrid game, we replace the oracle $H \setminus S$ by $\mathcal{S}_o$. By the definition of $\text{CCX}_{T_{ij}X_jX'_{ij}}$ shown in (23), if T_{ij} has been measured to 0 before applying CCX , the corresponding operation $\text{CCX}_{T_{ij}X_jX'_{ij}}$ operates just as the identity. This means that, conditioned on the fact that none of the events $\text{Find}_{i'}$ for $i' \leq i$ happen, the state of the system just after the i -th query to $H \setminus S$ is identical between $\mathcal{A}^{H \setminus S}$ and $\mathcal{A}^{\mathcal{S}_o}$. Therefore,

$$\Pr \left[\neg \text{Find}_i : \mathcal{C}_{\mathcal{A},z}^{H \setminus S} |0\rangle \left| \bigwedge_{i'=1}^{i-1} \neg \text{Find}_{i'} \right. \right] = \Pr \left[\neg \text{Find}_i : \mathcal{C}_{\mathcal{A},z}^{\mathcal{S}_o} |0\rangle \left| \bigwedge_{i'=1}^{i-1} \neg \text{Find}_{i'} \right. \right].$$

Moreover, for $1 \leq i \leq d$ and $1 \leq j \leq n$, given that X'_{ij} is initialized to $|0\rangle$, when T_{ij} has been measured to 1, the operation $\text{CCX}_{T_{ij}X_jX'_{ij}}$ is in fact copying the input $|x\rangle_{X_j}$ into the register X'_{ij} . Therefore, in case T_{ij} measures to 1, with probability one, the corresponding register X'_{ij} measures to some $x \in S$ at the end of the circuit.

Following the definitions in the main body, let measuring the output states of all the registers X', T in the computational basis yield outcomes $\mathbf{t} \in \{0, 1\}^{dn}$ and $\mathbf{x}' \in \mathcal{X}^{dn}$, respectively. And let $(i^*(\mathbf{t}), j^*(\mathbf{t}))$ denote the smallest pair of (i, j) in lexicographic order such that $t_{ij} = 1$, as defined in (24). Then we have

$$\Pr \left[\left(\bigvee_{i=1}^d \text{Find}_i \right) \wedge \left(x'_{i^*(\mathbf{t})j^*(\mathbf{t})} \in S \right) : \mathcal{C}_{\mathcal{A},z}^{\mathcal{S}_o} |0\rangle \right] = \Pr \left[\bigvee_{i=1}^d \text{Find}_i : \mathcal{C}_{\mathcal{A},z}^{\mathcal{S}_o} |0\rangle \right].$$

Now we get into the second (and also the last) hybrid game, which changes the oracle implementation to that shown in Fig. 5(c). For $1 \leq i \leq d$ and $1 \leq j \leq n$, Fig. 5(c) moves the measurement performed on registers T_{ij} to the end of the circuit. Or more precisely, it commutes the measurement with the corresponding operation $\text{CCX}_{T_{ij}X_jX'_{ij}}$. We write the oracle interface of Fig. 5(c) to $\mathcal{A}$ as $\mathcal{S}^{H,1S}$ and write its actual operation performed within the i -th query as $\mathcal{S}_i^{H,1S}$.

From the definition (23), we see that $\text{CCX}_{T_{ij}X_jX'_{ij}}$ can be treated as a controlled operation with T_{ij} being the controlling qubit. Therefore, it commutes with the measurement on T_{ij} with respect to the computational basis. Such commutation won't change the measurement outcome at the end of the circuit. Therefore,

$$\begin{aligned} \Pr \left[\left(\bigvee_{i=1}^d \text{Find}_i \right) \wedge \left(x'_{i^*(\mathbf{t})j^*(\mathbf{t})} \in S \right) : \mathcal{C}_{\mathcal{A},z}^{\mathcal{S}_o} |0\rangle \right] \\ = \Pr \left[\left(\bigvee_{i=1}^d \text{Find}_i \right) \wedge \left(x'_{i^*(\mathbf{t})j^*(\mathbf{t})} \in S \right) : \mathcal{C}_{\mathcal{A},z}^{\mathcal{S}^{H,1S}} |0\rangle \right]. \end{aligned}$$

We note that the operation $\mathcal{S}_i^{H,1S}$ performed in Fig. 5(c) is identical to that defined in Fig. 2. Treating registers T and X' as input to the circuit, instead of the internal states of the oracle, the resulting circuit is identical to $\mathcal{C}'_{\mathcal{A},z}{}^{H,1S}$. Moreover, $\bigvee_{i=1}^d \text{Find}_i$ indicates that the register T in $\mathcal{C}'_{\mathcal{A},z}{}^{H,1S} |0\rangle$ measures to a non-zero outcome $\mathbf{t}$. Therefore, we write

$$\begin{aligned} \Pr \left[\left(\bigvee_{i=1}^d \text{Find}_i \right) \wedge \left(x'_{i^*(\mathbf{t})j^*(\mathbf{t})} \in S \right) : \mathcal{C}_{\mathcal{A},z}^{\mathcal{S}^{H,1S}} |0\rangle \right] \\ = \Pr \left[\mathbf{t} \neq 0 \wedge x'_{i^*(\mathbf{t})j^*(\mathbf{t})} \in S : |\varphi\rangle := \mathcal{C}'_{\mathcal{A},z}{}^{H,1S} |0\rangle \right] \end{aligned}$$

By definition of $\text{Extract}_{|\varphi\rangle}$, we obtain the claimed (27) and complete the proof of Lemma 9. $\square$