# 1 Preliminaries

Let $\mathcal{X}$ and $\mathcal{Y}$ be two sets such that $\mathcal{X}$ is finite. Given a distribution $D$ over $\mathcal{Y}$, we use $D^{\mathcal{X}}$ do denote the distribution over $\mathcal{X} \mapsto \mathcal{Y}$, where the values associated to each $x \in \mathcal{X}$ are sampled independently following the distribution $D$. We use $x \hookleftarrow D$ for sampling a value $x$ according to distribution $D$. We denote by $\mathbb{B}_\lambda$ the Bernoulli distribution over a single bit $\{0,1\}$; sampling a bit from $\mathbb{B}_\lambda$ returns 1 with fixed probability $\lambda$. Observe that sampling a function $f$ from $\mathbb{B}_\lambda^{\mathcal{X}}$ fixes a set $X_f := \{\, x \in X \,:\, O(x) = 1 \,\} \subseteq \mathcal{X}$. We will overload notation and denote this by $X \hookleftarrow \mathbb{B}_\lambda^{\mathcal{X}}$. When $A$ is a quantum algorithm with access to an oracle $H$, we write $r \hookleftarrow A^H$ to denote the measurement of classical output $r$ after a quantum interaction with $H$, possibly involving many queries.

# 2 Finding collisions in a random function

**Theorem 2.1.** *[4, Theorem 4.9] Any algorithm making $q$ quantum queries to a random function $f : [M] \to [N]$ outputs a collision for $f$ with probability at most $27(q+2)^3/N$.*

# 3 Adversary's output distribution

**Theorem 3.1.** *[4, Theorem 3.1] Let $A$ be a quantum algorithm making $q$ quantum queries to an oracle $H : \mathcal{X} \mapsto \mathcal{Y}$ and $z$ a constant bit string. There exists a function $C : \mathcal{X}^{2q} \times \mathcal{Y}^{2q} \times \{0,1\}^* \mapsto \mathbb{R}$ such that, for all distributions $D$:*

$$\Pr[\, r = z \,:\, H \hookleftarrow D^{\mathcal{X}}; r \hookleftarrow A^H \,] = \sum_{\substack{\vec{x} \in \mathcal{X}^{2q} \\ \vec{y} \in \mathcal{Y}^{2q}}} C(\vec{x}, \vec{y}, z) \cdot \Pr[\, \forall i, H(x_i) = y_i \,:\, H \hookleftarrow D \,]$$

# 4 Semi-Constant Distributions

**Definition 4.1** (Semi-Constant Distribution)**.** *Fix a function $H : \mathcal{X} \mapsto \mathcal{Y}$, a set $X \subseteq \mathcal{X}$, and a constant $y \in \mathcal{Y}$. We denote by $SC_{X,y,H}(x)$ the function returning $y$ if $x \in X$ and $H(x)$ otherwise.*

*For any $\lambda$ and distribution $D$, the semi-constant distribution over $\mathcal{X} \leftarrow \mathcal{Y}$ samples $X \hookleftarrow \mathbb{B}_\lambda^{\mathcal{X}}$, $y \hookleftarrow D$, and $H \hookleftarrow D^{\mathcal{X}}$ and returns $SC(X, y, H)$. We abbreviate this to $SC_X$, to highlight the conditioning on a pre-sampled set $X$.*

Fix $\lambda$ and distribution $D$ over $\mathcal{Y}$. We will consider two games $G_i$, for $i \in \{0,1\}$, where we restrict our attention to quantum algorithms $A$ placing at most $q$ queries to their oracle and that output a bit $c$, together with some additional information $x \in \mathcal{X}$, $l \in \mathcal{X}^*$. The games are defined as

$$G_i := X \hookleftarrow \mathbb{B}_\lambda^{\mathcal{X}}; H \hookleftarrow F_i(X); (c, x, l) \hookleftarrow A^H$$

where $F_0(X) := D^{\mathcal{X}}$, which ignores $X$, and $F_1(X) := \mathrm{SC}_X$. We are interested in *good* executions, which we capture via the following predicate parameterized by an integer $k$

$$\mathsf{good}_k(X, x, l) := |l| \leqslant k \wedge x \in X \wedge l \cap X = \varnothing$$

and we define $P_i := \Pr[\, c \wedge \mathsf{good}_k(X, x, l) \,:\, G_i \,]$.

The following theorem, which extends [4, Corollary 4.8], is proved in [2].

**Theorem 4.1.** *Let $A$ be a quantum algorithm making $q$ quantum queries to an oracle $H : \mathcal{X} \mapsto \mathcal{Y}$ returning $(c, x, l)$ where $c$ is a boolean, $x \in \mathcal{X}$ and $l$ is a list of at most $k$ elements in $\mathcal{X}$. We have:*

$$|P_1 - P_0| \leqslant \frac{(2q + k + 1)^4}{6} \lambda^2$$

# 5 Small-Range Distributions

Given a distribution $D$ on $\mathcal{Y}$, define the small range distribution $\mathsf{SR}_r^D(\mathcal{X})$ as the following distribution on functions $H : \mathcal{X} \to \mathcal{Y}$:

- For each $i \in [r]$, chose a random value $y_i \in \mathcal{Y}$ according to the distribution $D$.
- For each $x \in \mathcal{X}$, pick a random $i \in [r]$ and set $H(x) = y_i$.

**Theorem 5.1.** *[4, Corollary 4.15] The output distributions of a quantum algorithm making $q$ quantum queries to an oracle either drawn from $\mathsf{SR}_r^D(\mathcal{X})$ or $D^{\mathcal{X}}$ are $27q^3/r$-close.*

**Theorem 5.2.** *[4, Theorem 4.16] Consider two distributions $D_1$ and $D_2$ on oracles from $\mathcal{X}$ into $[r] \times \mathcal{Y}$:*

- *$D_1$: generate a random oracle $f : \mathcal{X} \to [r]$ and a random oracle $h : \mathcal{X} \to \mathcal{Y}$, and output the oracle that maps $x$ to $(f(x), h(x))$.*
- *$D_2$: generate a random oracle $f : \mathcal{X} \to [r]$ and a random oracle $g : [r] \to \mathcal{Y}$, and output the oracle that maps $x$ to $(f(x), g(f(x)))$.*

*Then the probability that any $q$-quantum query algorithm distinguishes $D_1$ from $D_2$ is at most $54(q + 2)^3/r$.*

# 6 Distinct outputs

**Theorem 6.1.** *(Specialized version of [4, Theorem 3.8]) Fix sets $\mathcal{X}$ and $\mathcal{Y}$, and distribution $D$ on $\mathcal{Y}$. Then any quantum algorithm making $q$ quantum queries to $H$ drawn from $D^{\mathcal{X}}$ can only produce $q + 1$ input/output pairs of $H$ with probability at most $(q + 1)/2^{H_\infty(D)}$.*

# 7 One-Way to Hiding (OW2H)

## 7.1 Semi-Classical OW2H

**Definition 7.1.** *[3, Definition 1][1] Let $H : \mathcal{X} \to \mathcal{Y}$ be any function, and $S \subseteq \mathcal{X}$ be a set. The oracle $H \setminus S$ ("$H$ punctured on $S$") takes as input a value $X$. It first computes whether $x \in S$ into an auxilliary qubit $p$, and measures $p$. Then it runs $H(X)$ and returns the result. Let $\mathsf{Find}$ be the event that any of the measurements of $p$ returns 1.*

**Lemma 7.1.** *[1, Lemma 1][3, Lemma 2] Let $(S, G, H, z)$ have arbitrary joint distribution satisfying the following conditions: $S \subseteq \mathcal{X}$ is a set, $G, H : \mathcal{X} \to \mathcal{Y}$ are functions such that $\forall X \notin S, G(X) = H(X)$, and $z$ is a bit string. Let $\mathcal{A}$ be a quantum oracle algorithm and $\mathsf{Ev}$ an arbitrary classical event. Then*

$$\Pr[\, \mathsf{Ev} \wedge \neg\mathsf{Find} \,:\, \mathcal{A}^{H \setminus S}(z) \,] = \Pr[\, \mathsf{Ev} \wedge \neg\mathsf{Find} \,:\, \mathcal{A}^{G \setminus S}(z) \,] \tag{1}$$

**Theorem 7.1.** *[1, Theorem 1][3, Lemma 3] Let $(S, G, H, z)$ have arbitrary joint distribution satisfying the following conditions: $S \subseteq \mathcal{X}$ is a set, $G, H : \mathcal{X} \to \mathcal{Y}$ are functions such that $\forall x \notin S, G(x) = H(x)$, and $z$ is a bit string. Let $\mathcal{A}$ be a quantum oracle algorithm of query depth at most $d$ and $\mathsf{Ev}$ an arbitrary classical event. Let*

$$\begin{array}{lll} P_{\text{left}} & := & \Pr[\,\mathsf{Ev} : \mathcal{A}^{H}(z)\,] \\ P_{\text{right}} & := & \Pr[\,\mathsf{Ev} : \mathcal{A}^{G}(z)\,] \\ P_{\text{find}} & := & \Pr[\,\mathsf{Find} : \mathcal{A}^{H\setminus S}(z)\,] = \Pr[\,\mathsf{Find} : \mathcal{A}^{G\setminus S}(z)\,] \end{array} \tag{2}$$

*Then,*

$$|\,P_{\text{left}} - P_{\text{right}}\,| \leqslant 2\sqrt{d \cdot P_{\text{find}}} \qquad \left|\sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}}\right| \leqslant 2\sqrt{d \cdot P_{\text{find}}}$$

*The theorem also holds with bound $\sqrt{(d+1) \cdot P_{\text{find}}}$ for the following alternative definitions of $P_{\text{right}}$:*

$$P_{\text{right}} := \Pr[\,\mathsf{Ev} : \mathcal{A}^{H\setminus S}(z)\,] \tag{3}$$

$$P_{\text{right}} := \Pr[\,\mathsf{Ev} \wedge \neg\mathsf{Find} : \mathcal{A}^{H\setminus S}(z)\,] = \Pr[\,\mathsf{Ev} \wedge \neg\mathsf{Find} : \mathcal{A}^{G\setminus S}(z)\,] \tag{4}$$

$$P_{\text{right}} := \Pr[\,\mathsf{Ev} \wedge \mathsf{Find} : \mathcal{A}^{H\setminus S}(z)\,] = \Pr[\,\mathsf{Ev} \wedge \mathsf{Find} : \mathcal{A}^{G\setminus S}(z)\,] \tag{5}$$

**Theorem 7.2.** *[1, Theorem 2][3, Lemma 4] Let $\mathcal{A}$ be any quantum oracle algorithm of query depth at most $d$. Let $H : \mathcal{X} \to \mathcal{Y}$ be a function, $S \subset \mathcal{X}$ be a set and $z$ a bit string with an arbitrary joint distribution. Then, there exists an algorithm $\mathcal{B}$ that runs in essentially the same time, has the same query depth as $\mathcal{A}$ and outputs a set $T \subseteq \mathcal{X}$ such that*

$$\Pr[\,\mathsf{Find} : \mathcal{A}^{H\setminus S}(z)\,] \leqslant 4d \cdot \Pr[\,S \cap T \neq \varnothing : T \leftarrow B^{H}(z)] \tag{6}$$

Let $H : \mathcal{X} \to \mathcal{Y}$ be a function and $C_H$ denote the classical oracle that provides access to $H$. Let also $L \subseteq \mathcal{X}$ denote the list of queries placed to $C_H$.

**Theorem 7.3.** *Let $(S, G, H, z)$ have arbitrary joint distribution satisfying the following conditions: $S \subseteq \mathcal{X}$ is a set, $G, H : \mathcal{X} \to \mathcal{Y}$ are functions such that $\forall x \notin S, G(x) = H(x)$, and $z$ is a bit string. Let $\mathcal{A}$ be a quantum oracle algorithm with classical output $w$, of query depth at most $d$ (we count the aggregate number of queries to both oracles) and $\mathsf{Ev}(w)$ an arbitrary classical event computed over the output of $\mathcal{A}$. Let*

$$\begin{array}{lll} P_{\text{left}} & := & \Pr[\,\mathsf{Ev}(w) : w \leftarrow \mathcal{A}^{H,C_H}(z)\,] \\ P_{\text{right}} & := & \Pr[\,\mathsf{Ev}(w) \,\wedge\, S \cap L = \varnothing : w \leftarrow \mathcal{A}^{G,C_G}(z)\,] \end{array} \tag{7}$$

*Then, there exists an algorithm $\mathcal{B}$ that runs in essentially the same time, has the same query depth as $\mathcal{A}$ and outputs a set $T \subseteq \mathcal{X}$ such that*

$$\left|\sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}}\right| \leqslant 4(d+1) \cdot \sqrt{\Pr[\,S \cap T \neq \varnothing : T \leftarrow B^{G,C_G}(z)]}$$

*Proof.* For any oracle $H$, let $\mathcal{A}'^{H}$ be the algorithm that runs $\mathcal{A}$ internally and simulates $C_H$ trivially by querying $H$ and performing the required measurements. Let also $\mathcal{A}'$ output the list $L$ of queries placed by $\mathcal{A}$ to $C_H$ along with the output of $\mathcal{A}$. Then, we have that $\mathcal{A}'$ has query depth at most $d$ and

$$P_{\text{left}} = \Pr[\,\mathsf{Ev}(w) : (w, L) \leftarrow \mathcal{A}'^{H}(z)\,]$$

$$\Pr[\,\mathsf{Ev}(w)\,:\,w \hookleftarrow \mathcal{A}^{G,C_G}(z)\,] = \Pr[\,\mathsf{Ev}(w)\,:\,(w,L) \hookleftarrow \mathcal{A}'^{G}(z)\,]$$

Now, setting $\epsilon := \sqrt{(d+1)\cdot \Pr[\,\mathsf{Find}\,:\,\mathcal{A}'^{G\setminus S}(z)\,]}$ we can apply Theorem 7.1 and derive that

$$\left|\sqrt{\Pr[\,\mathsf{Ev}(w)\,:\,(w,L) \hookleftarrow \mathcal{A}'^{H}(z)\,]} - \sqrt{\Pr[\,\mathsf{Ev}(w)\,\wedge\,\neg\mathsf{Find}\,:\,(w,L) \hookleftarrow \mathcal{A}'^{G\setminus S}(z)\,]}\right| \leqslant \epsilon \tag{8}$$

Now define $\mathsf{Ev}'(w,L) := \mathsf{Ev}(w) \wedge S \cap L = \varnothing$. We have

$$\Pr[\,\mathsf{Ev}(w)\,\wedge\,\neg\mathsf{Find}\,:\,(w,L) \hookleftarrow \mathcal{A}'^{G\setminus S}(z)\,] = \Pr[\,\mathsf{Ev}'(w,L)\,\wedge\,\neg\mathsf{Find}\,:\,(w,L) \hookleftarrow \mathcal{A}'^{G\setminus S}(z)\,]$$

since, by construction, $\neg\mathsf{Find} \Rightarrow S \cap L = \varnothing$. We now apply Theorem 7.1 again, but this time using $H = G$ and $\mathsf{Ev} = \mathsf{Ev}'$, to obtain

$$\left|\sqrt{\Pr[\,\mathsf{Ev}'(w,L)\,:\,(w,L) \hookleftarrow \mathcal{A}'^{G}(z)\,]} - \sqrt{\Pr[\,\mathsf{Ev}'(w,L)\,\wedge\,\neg\mathsf{Find}\,:\,(w,L) \hookleftarrow \mathcal{A}'^{G\setminus S}(z)\,]}\right| \leqslant \epsilon \tag{9}$$

Adding Equations 8 and 9 and applying the triangular inequality, we obtain:

$$\left|\sqrt{\Pr[\,\mathsf{Ev}(w)\,:\,(w,L) \hookleftarrow \mathcal{A}'^{H}(z)\,]} - \sqrt{\Pr[\,\mathsf{Ev}'(w,L)\,:\,(w,L) \hookleftarrow \mathcal{A}'^{G}(z)\,]}\right| \leqslant 2\epsilon$$

Applying the definitions of $\mathcal{A}'$ and $\mathsf{Ev}'$ we get

$$\left|\sqrt{\Pr[\,\mathsf{Ev}(w)\,:\,w \hookleftarrow \mathcal{A}^{H,C_H}(z)\,]} - \sqrt{\Pr[\,\mathsf{Ev}(w)\,\wedge\,S \cap L = \varnothing\,:\,w \hookleftarrow \mathcal{A}^{G,C_G}(z)\,]}\right| \leqslant 2\epsilon$$

Finally, plugging in Theorem 7.2 we know there exists an algorithm $\mathcal{B}$ that runs in essentially the same time, has the same query depth as $\mathcal{A}$ and outputs a set $T \subseteq \mathcal{X}$ such that

$$2\epsilon = 2\sqrt{(d+1)\cdot \Pr[\,\mathsf{Find}\,:\,\mathcal{A}'^{G\setminus S}(z)\,]} \leqslant 2\sqrt{(d+1)\cdot 4d \cdot \Pr[\,S \cap T \neq \varnothing\,:\,T \hookleftarrow \mathcal{B}^{G}(z)]}$$

$$2\epsilon \leqslant 4(d+1)\cdot\sqrt{\Pr[\,S \cap T \neq \varnothing\,:\,T \hookleftarrow \mathcal{B}^{G}(z)]}$$

Finally, observe that any $\mathcal{B}$ that satisfies the equation above implies an algorithm $\mathcal{B}$ that is also provided access to $C_G$ and simply does not use it, which completes the proof. □

**Theorem 7.4.** *[3, Lemma 5] Let $(S, G, H, z)$ have arbitrary joint distribution satisfying the following conditions: $S = \{X^\star\} \subseteq \mathcal{X}$ is a singleton set, $G, H : \mathcal{X} \to \mathcal{Y}$ are functions such that $\forall x \notin S, G(x) = H(x)$, and $z$ is a bit string. Let $\mathcal{A}$ be a quantum oracle algorithm of query depth at most $d$ and $\mathsf{Ev}$ an arbitrary classical event. Let*

$$\begin{array}{rcl} P_{\text{left}} & := & \Pr[\,\mathsf{Ev}\,:\,\mathcal{A}^{H}(z)\,] \\ P_{\text{right}} & := & \Pr[\,\mathsf{Ev}\,:\,\mathcal{A}^{G}(z)\,] \end{array} \tag{10}$$

*Then, there exists an algorithm $\mathcal{B}$ that runs in essentially the same time, has the same query depth as $\mathcal{A}$ in queries both to $H$ and $G$ and outputs a value $X \in \mathcal{X}$ such that*

$$|\,P_{\text{left}} - P_{\text{right}}\,| \leqslant 2\sqrt{\Pr[\,X = X^\star\,:\,X \hookleftarrow \mathcal{B}^{H,G}(z)]}$$

$$\left|\sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}}\right| \leqslant 2\sqrt{\Pr[\,X = X^\star\,:\,X \hookleftarrow \mathcal{B}^{H,G}(z)]}$$

## References


[1] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 269–295, Cham, 2019. Springer International Publishing.

[2] Manuel Barbosa, Gilles Barthe, Xiong Fan, Benjamin Grégoire, Shih-Han Hung, Jonathan Katz, Pierre-Yves Strub, Xiaodi Wu, and Li Zhou. EasyPQC: Verifying post-quantum cryptography. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, CCS '21, page 2564–2586, New York, NY, USA, 2021. Association for Computing Machinery.

[3] Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. Tighter proofs of cca security in the quantum random oracle model. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography*, pages 61–90, Cham, 2019. Springer International Publishing.

[4] Mark Zhandry. *Cryptography in the Age of Quantum Computers (PhD Thesis)*. PhD thesis, Stanford University, 2015.