On the necessity of collapsing

Marcel Dall'Agnol
msagnol@pm.me
University of Warwick

Nicholas Spooner
nicholas.spooner@warwick.ac.uk
University of Warwick

June 18, 2022

Abstract

Collapsing and collapse binding were proposed by Unruh (Eurocrypt '16) as post-quantum strengthenings of collision resistance and computational binding (respectively). These notions have been very successful in facilitating the "lifting" of classical security proofs to the quantum setting. A natural question remains, however: is collapsing is the *weakest* notion that suffices for such lifting?

In this work we answer this question in the affirmative by giving a classical commit-and-open protocol which is post-quantum secure if and only if the commitment scheme (resp. hash function) used is collapse binding (resp. collapsing). This result also establishes that a variety of "weaker" post-quantum computational binding notions (sum binding, CDMS binding and unequivocality) are in fact *equivalent* to collapse binding.

Finally, we establish a "win-win" result, showing that a post-quantum collision resistant hash function that is not collapsing can be used to build an equivocal hash function (which can, in turn, be used to build one-shot signatures and other useful quantum primitives). This strengthens a result due to Zhandry (Eurocrypt '19) showing that the same object yields quantum lightning. For this result we make use of recent quantum rewinding techniques.

1 Introduction

The advent of quantum computing has led to a deep reevaluation of central ideas in cryptography. Most prominently, the hardness assumptions upon which many widely-used cryptographic schemes are based do not hold with respect to quantum computation. The past two decades have seen a great deal of progress in tackling this issue, by devising new schemes based on "post-quantum" assumptions.

This is, however, only part of the picture. Quantum computation is not only *more powerful* than classical, it is *fundamentally different* in nature. Quantum information exhibits properties like *superposition* and *unclonability* that have no classical analogue. As such, we must also revisit another key ingredient in the study of cryptography: definitions. A number of works explore the implications of quantum information for security definitions; some examples include random oracles [BDF+11], message authentication codes [BZ13a, GYZ17], and signatures and CCA-secure encryption [BZ13b].

This work focuses on the related notions of *collision resistance* and *computational binding*; for the present discussion we focus on the former. While a natural quantum analogue of collision resistance asserts that it is infeasible for a quantum computer to find a hash collision, [ARU14] demonstrated that this definition is not sufficient for many applications of hash functions. The key issue is that while collision resistance rules out finding two distinct preimages *simultaneously*, it does not rule out being able to "choose" the preimage that is obtained. Note that this is an exclusively quantum problem: a classical algorithm that can make such a choice can be used to break collision resistance via rewinding.

Unruh [Unr16b] proposed a strengthening of collision resistance called *collapsing* (and an analogous strengthening of computational binding called *collapse binding*). This has since become a central notion in post-quantum cryptography: a sequence of works [Unr16b, LZ19, ACP21, CCY21, CMSZ22, LMS21] have demonstrated that this strengthening is sufficient to prove post-quantum security for various protocols.

Collapsing hash functions can be built from LWE [Unr16a]; additionally, any CRH that satisfies a certain regularity property is collapsing, which includes constructions from LPN and isogenies, and plausibly functions like SHA [Zha22, CX22]. Nonetheless, in general there remains a gap between collapsing and collision resistance. [Zha19] shows that the existence of a hash function in this gap implies the existence of *quantum lightning* which (among other things) yields public-key quantum money.

1.1 Results

In this work we investigate the collapsing property and show that it is equivalent to other proposed notions of post-quantum security for hash functions and commitments.

1.1.1 Chosen-bit binding commitments

We introduce a new binding notion called *chosen-bit binding*, defined in terms of a classical interaction with a (potentially quantum) adversary Adv. Let $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ be a commitment scheme for messages of length $\ell(\lambda)$. The chosen-bit binding game is as follows.

1. Choose $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. Obtain $(\mathsf{com}, i) \leftarrow \mathsf{Adv}(\mathsf{ck})$, where $i \in [\ell(\lambda)]$.
3. Choose $b \leftarrow \{0,1\}$ uniformly at random.
4. Obtain $(m, \omega) \leftarrow \mathsf{Adv}(b)$. Output 1 if $\mathsf{Commit}(m, \omega) = \mathsf{com}$ and $m_i = b$.

We say that COM is classical (resp. post-quantum) chosen-bit binding (CBB) if for every efficient classical (resp. quantum) Adv, the above experiment outputs 1 with probability $1/2 + \mathsf{negl}(\lambda)$. It is straightforward to show (via rewinding) that classical CBB is equivalent to computational binding. Our first result is an equivalence between post-quantum CBB and collapsing.

Lemma 1.1. *A commitment scheme is collapse binding if and only if it is post-quantum chosen-bit binding.*

We note that the "only if" direction already follows from a result of Unruh [Unr16a]: CBB is a special case of "CDMS binding", which Unruh shows is implied by collapsing. We discuss this in more detail shortly.

1.1.2 Connections to existing notions

Note that, when $\ell = 1$, CBB is identical to "sum binding" [Unr16b]. [Unr16a] shows that collapse binding implies sum binding; combining this with Lemma 1.1 we obtain the following corollary.

Corollary 1.2. *(Post-quantum) sum binding is equivalent to collapse binding (for bit commitments).*

For general ℓ, chosen-bit binding is a special case of so-called "CDMS binding" [CDMS04, Unr16b]. Informally, a commitment is CDMS-binding with respect to a function class F if for every $f\colon X \to Y$ in F and every efficient adversary Adv,

$$\Pr_y[\mathsf{Adv}(y) \text{ opens } \mathsf{com} \text{ to } m \text{ s.t. } f(m) = y] \leq \frac{1}{|Y|} + \mathsf{negl}(\lambda) \ ,$$

where above com is a fixed commitment previously output by Adv and y is chosen uniformly at random from Y. [Unr16a] shows that collapsing implies CDMS binding for all function classes where $|Y|$ is polynomial. CBB is easily seen to be equivalent to CDMS binding for F being the class of one-bit projection functions; we hence obtain the following corollary.

Corollary 1.3. *(Post-quantum) CDMS binding is equivalent to collapse binding.*

It also follows that CDMS binding for one-bit projections implies CDMS binding for all function classes with polynomial range.

1.1.3 Collapsing and equivocal hash functions

We define an analogous notion of chosen-bit binding for hash functions. Let $\mathcal{H}_\lambda \subseteq \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}$ be a hash function family. The chosen-bit binding game for hash functions proceeds as follows.

1. Choose $h \leftarrow \mathcal{H}_\lambda$.
2. Obtain $(y, i) \leftarrow \mathsf{Adv}(h)$, where $y \in \{0,1\}^{n(\lambda)}$ and $i \in [m(\lambda)]$.
3. Choose $b \leftarrow \{0,1\}$ uniformly at random.
4. Obtain $x \leftarrow \mathsf{Adv}(b)$. Output 1 if $x_i = b$.

We say that $\mathcal{H}$ is classical (resp. post-quantum) chosen-bit binding (CBB) if for every efficient classical (resp. quantum) Adv, the above experiment outputs 1 with probability $1/2 + \mathsf{negl}(\lambda)$. Classical CBB is equivalent to collision resistance. By an essentially identical argument to Lemma 1.1, we show that post-quantum CBB is equivalent to collapsing.

Lemma 1.4. *A hash family $\mathcal{H}$ is collapsing if and only if it is post-quantum chosen-bit binding.*

An *equivocal* CRH [AGKZ20] is a post-quantum CRH with an additional functionality EqGen which produces a tuple (ρ, y, p) where ρ is a quantum "secret key" and p is a predicate. Given ρ, the user is able to (later) produce x such that $h(x) = y$ and $p(x) = b$ for any bit b of its choice (with probability close to 1).[1]

We observe first that what [AGKZ20] call "unequivocality" — roughly, that achieving the above with any nontrivial advantage is computationally infeasible — implies CBB, and hence collapsing. This resolves an open question of [AGKZ20].

However, we are able to show something much stronger, in the spirit of the "win-win" results of [Zha19]. In particular, we show that if a CRH is (almost everywhere) *not* collapsing then it is equivocal. Note that this is a much stronger notion than being "not unequivocal" since equivocation must succeed with probability close to 1. More formally, we obtain the following.[2]

Theorem 1.5. *Let $\mathcal{H}$ be a hash family that is post-quantum collision resistant but not collapsing. Then there exists a polynomial r such that the r-fold parallel repetition of $\mathcal{H}$, $\mathcal{H}^r$, is (infinitely often) equivocal.*

The proof uses recent quantum rewinding techniques [CMSZ22] to amplify success probability.

Finally, we use the chosen-bit binding definition to give a "fully classical" proof of the (folklore) result that somewhere-statistically binding (SSB) hash functions are collapsing.

Lemma 1.6. *Any somewhere-statistically binding hash function is chosen-bit binding; in particular, post-quantum SSB hash functions are collapsing.*

1.2 Discussion

Our results establish that collapsing is a "minimal" assumption which allows one to prove post-quantum security for the important class of "commit-and-open" sigma protocols. Indeed, it was shown in [LMS21] that any classically secure commit-and-open protocol is post-quantum secure when instantiated with a collapse binding commitment. Our first result (Lemma 1.1) gives a sort of converse: there is a commit-and-open protocol which is insecure when instantiated with a commitment that is *not* collapse binding.

Unlike collapse binding, which is defined in terms of a quantum interaction, chosen-bit binding is defined in terms of a classical interaction with a (potentially quantum) adversary. This may make it easier to connect with other classical binding notions (as we demonstrate by proving that SSB implies collapsing). The definition also implies a method by which a quantum falsifier can convince a classical party that a hash function is *not* collapsing.

[1] Note that while these functions are referred to as "hash functions", it is not necessary that they be compressing in order to be nontrivial, due to the equivocality property.

[2] It is claimed in [AGKZ20] that if $\mathcal{H}$ is "not unequivocal" then its parallel repetition $\mathcal{H}^r$ is equivocal for large enough r. This is in fact true, but their argument is flawed; see Remark 4.3 for a discussion.

2 Preliminaries

We denote by $\lambda \in \mathbb{N}$ the security parameter. For $n \in \mathbb{N}$, we write $[n]$ to denote the set $\{1, \ldots, n\}$. For a set S, we write $i \leftarrow S$ to denote that i is chosen uniformly from S. For a distribution D we write $i \leftarrow D$ to denote that i is chosen according to D.

We make use of the following simple fact, a consequence of Markov's inequality.

Proposition 2.1. *Let X be a random variable supported on $[0,1]$. Then for all $\alpha \geq 0$, $\Pr[X \geq \alpha] \geq E[X] - \alpha$.*

2.1 Quantum information

We recall the basics of quantum information. Most of the following is taken almost verbatim from [CMSZ22]. A (pure) *quantum state* is a vector $|\psi\rangle$ in a complex Hilbert space $\mathcal{H}$ with $\||\psi\rangle\| = 1$; in this work, $\mathcal{H}$ is finite-dimensional. We denote by $\mathbf{S}(\mathcal{H})$ the space of Hermitian operators on $\mathcal{H}$. A *density matrix* is a positive semi-definite operator $\rho \in \mathbf{S}(\mathcal{H})$ with $\mathrm{Tr}(\rho) = 1$. A density matrix represents a probabilistic mixture of pure states (a mixed state); the density matrix corresponding to the pure state $|\psi\rangle$ is $|\psi\rangle\langle\psi|$. Typically we divide a Hilbert space into *registers*, e.g. $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. We sometimes write, e.g., $\rho^{\mathcal{H}_1}$ to specify that $\rho \in \mathbf{S}(\mathcal{H}_1)$.

A unitary operation is a complex square matrix U such that $UU^\dagger = \mathbf{I}$. The operation U transforms the pure state $|\psi\rangle$ to the pure state $U|\psi\rangle$, and the density matrix ρ to the density matrix $U\rho U^\dagger$.

A *projector* Π is a Hermitian operator ($\Pi^\dagger = \Pi$) such that $\Pi^2 = \Pi$. A *projective measurement* is a collection of projectors $\mathsf{P} = (\Pi_i)_{i \in S}$ such that $\sum_{i \in S} \Pi_i = \mathbf{I}$. The application of P to a pure state $|\psi\rangle$ yields outcome $i \in S$ with probability $p_i = \||\Pi_i|\psi\rangle\|^2$; in this case the post-measurement state is $|\psi_i\rangle = \Pi_i|\psi\rangle / \sqrt{p_i}$. We refer to the post-measurement state $\Pi_i|\psi\rangle / \sqrt{p_i}$ as the result of applying P to $|\psi\rangle$ and *post-selecting* (conditioning) on outcome i. A state $|\psi\rangle$ is an *eigenstate* of P if it is an eigenstate of every Π_i. A two-outcome projective measurement is called a *binary projective measurement*, and is written as $\mathsf{P} = (\Pi, \mathbf{I} - \Pi)$, where Π is associated with the outcome 1, and $\mathbf{I} - \Pi$ with the outcome 0.

General (non-unitary) evolution of a quantum state can be represented via a *completely-positive trace-preserving (CPTP)* map $T \colon \mathbf{S}(\mathcal{H}) \to \mathbf{S}(\mathcal{H}')$. We omit the precise definition of these maps in this work; we only use the facts that they are trace-preserving (for every $\rho \in \mathbf{S}(\mathcal{H})$ it holds that $\mathrm{Tr}(T(\rho)) = \mathrm{Tr}(\rho)$) and linear. For every CPTP map $T \colon \mathbf{S}(\mathcal{H}) \to \mathbf{S}(\mathcal{H})$ there exists a *unitary dilation* U that operates on an expanded Hilbert space $\mathcal{H} \otimes \mathcal{K}$, so that $T(\rho) = \mathrm{Tr}_{\mathcal{K}}(U(\rho \otimes |0\rangle\langle 0|^{\mathcal{K}})U^\dagger)$. This is not necessarily unique; however, if T is described as a circuit then there is a dilation U_T represented by a circuit of size $O(|T|)$.

For Hilbert spaces $\mathcal{A}, \mathcal{B}$ the *partial trace* over $\mathcal{B}$ is the unique CPTP map $\mathrm{Tr}_{\mathcal{B}} \colon \mathbf{S}(\mathcal{A} \otimes \mathcal{B}) \to \mathbf{S}(\mathcal{A})$ such that $\mathrm{Tr}_{\mathcal{B}}(\rho_A \otimes \rho_B) = \mathrm{Tr}(\rho_B)\rho_A$ for every $\rho_A \in \mathbf{S}(\mathcal{A})$ and $\rho_B \in \mathbf{S}(\mathcal{B})$.

A *general measurement* is a CPTP map $\mathsf{M} \colon \mathbf{S}(\mathcal{H}) \to \mathbf{S}(\mathcal{H} \otimes \mathcal{O})$, where $\mathcal{O}$ is an ancilla register holding a classical outcome. Specifically, given measurement operators $\{M_i\}_{i=1}^N$ such that $\sum_{i=1}^N M_i M_i^\dagger = \mathbf{I}$ and a basis $\{|i\rangle\}_{i=1}^N$ for $\mathcal{O}$, $\mathsf{M}(\rho) = \sum_{i=1}^N (M_i \rho M_i^\dagger \otimes |i\rangle\langle i|^{\mathcal{O}})$. We sometimes implicitly discard the outcome register. A projective measurement is a general measurement where the M_i are projectors. A measurement induces a probability distribution over its outcomes given by $\Pr[i] = \mathrm{Tr}\Big(|i\rangle\langle i|^{\mathcal{O}}\, \mathsf{M}(\rho)\Big)$; we denote sampling from this distribution by $i \leftarrow \mathsf{M}(\rho)$.

2.2 Commitment schemes

For the purposes of this work, a *commitment scheme* consists of a pair of PPT algorithms $(\mathsf{Gen}, \mathsf{Commit})$ with the following binding property.

Computational binding. For an adversary Adv, define the experiment $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{bind}}(\lambda)$ as follows.

1. The challenger generates $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. $\mathsf{Adv}(\mathsf{ck})$ sends $(m_0, \omega_0, m_1, \omega_1)$ to the challenger.
3. The experiment outputs 1 if $m_0 \neq m_1$ and $\mathsf{Commit}(\mathsf{ck}, m_0, \omega_0) = \mathsf{Commit}(\mathsf{ck}, m_1, \omega_1)$.

We say that $(\mathsf{Gen}, \mathsf{Commit})$ is classically (resp. post-quantum) computationally binding if for all PPT (resp. QPT) adversaries Adv,

$$\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{bind}}(\lambda) = 1\right] = \mathsf{negl}(\lambda) \ .$$

Typically, in order to be non-trivial, commitment schemes should also satisfy a notion of hiding. We omit the definition of hiding since it is not relevant to the current work. Next, we recall the notion of collapse binding [Unr16b].

Collapse binding. For an adversary Adv, define the experiment $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cl}}(\lambda)$ as follows.

1. The challenger generates $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. $\mathsf{Adv}(\mathsf{ck})$ sends a commitment com and the registers $\mathcal{M} \otimes \mathcal{O}$ of a quantum state ρ.
3. The challenger flips a coin $b \in \{0,1\}$. If $b = 0$, the challenger does nothing. Otherwise, the challenger measures $\mathcal{M}$ in the computational basis.
4. The challenger returns registers $\mathcal{M} \otimes \mathcal{O}$ to the adversary, who outputs a bit b'. The experiment outputs 1 if $b = b'$.

We say that Adv is valid if measuring the output of $\mathsf{Adv}(\mathsf{ck})$ in the computational basis yields, with probability 1, $(\mathsf{com}, m, \omega)$ such that $\mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{com}$. (Equivalently, $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ where all $|\psi_i\rangle$ have zero amplitude on computational basis states $|m, \omega\rangle$ where $\mathsf{Commit}(\mathsf{ck}, m, \omega) \neq \mathsf{com}$.)

We say that $(\mathsf{Gen}, \mathsf{Commit})$ is collapse-binding if for all *valid* non-uniform QPT adversaries Adv,

$$\left|\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cl}}(\lambda) = 1\right] - \frac{1}{2}\right| = \mathsf{negl}(\lambda) \ .$$

Sum binding. For an adversary Adv, define the experiment $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{sum}}(\lambda)$ as follows.

1. The challenger generates $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. $\mathsf{Adv}(\mathsf{ck})$ sends a commitment com.
3. The challenger flips a coin $b \leftarrow \{0,1\}$ and sends it to Adv.
4. Adv returns an opening ω. The experiment outputs 1 if $\mathsf{Commit}(\mathsf{ck}, b, \omega) = \mathsf{com}$.

We say that COM is sum-binding if for all non-uniform QPT adversaries Adv,

$$\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{sum}}(\lambda) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda) \ .$$

Somewhere statistical binding (SSB). Finally, we recall the notion of somewhere statistical binding, introduced by [HW15] in the context of hash functions. Here we present the equivalent notion for commitments; note this is different to the more sophisticated notion of SSB commitments given by [FLPS21].

Definition 2.2 (Somewhere statistical binding)**.** Let ℓ be a polynomial. A commitment scheme $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ is said to be somewhere-statistically binding (SSB) if:

- For all $i, j \in [\ell(\lambda)]$, the distributions $\mathsf{Gen}(1^\lambda, i)$ and $\mathsf{Gen}(1^\lambda, j)$ are computationally indistinguishable.
- For all $i \in [\ell(\lambda)]$ and all ck_i in the support of $\mathsf{Gen}(1^\lambda, i)$, let m, m' be such that there exist ω, ω' satisfying $\mathsf{Commit}(\mathsf{ck}_i, m, \omega) = \mathsf{Commit}(\mathsf{ck}_i, m', \omega')$. Then $m_i = m'_i$.

"Honest" key generation is by (e.g.) choosing a random $j \in [\ell(\lambda)]$ and running $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda, j)$; note however that this is indistinguishable from any other way of choosing the index. We find it useful to restate the indistinguishability property as follows. For all QPT adversaries Adv:

$$\Pr\left[i = j \;\middle|\; \begin{array}{r} j \leftarrow [\ell(\lambda)] \\ \mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda, j) \\ i \leftarrow \mathsf{Adv}(\mathsf{ck}) \end{array}\right] \leq \frac{1}{\ell(\lambda)} + \mathsf{negl}(\lambda) \ .$$

Collision-resistant hash functions. For our purposes, a collision-resistant hash function is a binding (but not hiding) commitment scheme where the length of the randomness is zero. We will henceforth only discuss commitment schemes; all of our results extend to CRHs *mutatis mutandis*.

3 Chosen-bit binding

In this section we define the notion of chosen-bit binding for commitment schemes and show that post-quantum chosen-bit binding is equivalent to collapse binding.

The chosen-bit binding experiment. Given a commitment scheme COM we define the experiment $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda)$, parameterised by $\lambda \in \mathbb{N}$.

1. The challenger samples $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$ and sends ck to Adv.
2. Adv responds with a commitment com and index $i \in [\ell]$.
3. The challenger sends a random bit $b \leftarrow \{0,1\}$.
4. Adv responds with (m, ω).

The experiment outputs 1 if $\mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{com}$ and $m_i = b$.

Definition 3.1. We say that a commitment scheme is classical (resp. post-quantum) **chosen-bit binding** if for all efficient classical (resp. quantum) adversaries Adv,

$$\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda) \ .$$

The proof of the following lemma is straightforward and hence omitted.

Lemma 3.2. *A commitment scheme is chosen-bit binding against classical adversaries if and only if it is computationally binding.*

We now prove the main result of this section, that chosen-bit binding is equivalent to collapse binding.

Lemma 3.3. *A commitment scheme is chosen-bit binding against quantum adversaries if and only if it is collapse binding.*

We first prove (via the contrapositive) that collapsing implies chosen-bit binding; this is included only for completeness as it follows from [Unr16a, Theorem 32].

Proof (collapsing ⇒ CBB). Let Adv be an adversary that achieves advantage ε in the chosen-bit binding game. We may assume, without loss of generality, that the adversary's action in step 4 consists of the application of a unitary U followed by a computational basis measurement of $\mathcal{M} \otimes \mathcal{O}$. We construct an adversary Adv' for the collapse binding experiment as follows.

- Run $\mathsf{Adv}(\mathsf{ck})$ to obtain $i \in [\ell], \mathsf{com}$ and residual state ρ. Apply U to $\sigma = |+\rangle\langle+| \otimes \rho$ followed by the binary projective measurement $\mathsf{M} = (\Pi, I - \Pi)$ where

$$\Pi := \sum_{\substack{b \in \{0,1\}, m, \omega \\ \mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{com} \\ m_i = b}} |b, m, \omega\rangle\langle b, m, \omega| \ .$$

  If the outcome is 1, send the registers $\mathcal{M}, \mathcal{O}$ along with $i \in [\ell]$ to the challenger. Otherwise, send an arbitrary valid (classical) commitment.

- Upon receipt of $\mathcal{M}, \mathcal{O}$ from the challenger:
  - If the outcome in the previous step was 0, output a random bit.
  - Otherwise, apply $U^\dagger$ to $\mathcal{B}, \mathcal{M}, \mathcal{O}$ and measure $\mathcal{B}$ in the $\{|+\rangle, |-\rangle\}$ basis. If the result is $|+\rangle$, output 0; otherwise output 1.

Note that, since Adv' always sends (part of) a state in the image of Π, it is a valid adversary. Moreover, if either the challenger measures or the outcome of the first measurement by the adversary is 0, the experiment outputs a uniformly random bit.

For the case where the challenger does not measure, we use the following proposition:

Proposition 3.4. *Let P, Q be projectors and ρ a density matrix such that $\rho Q = \rho$. Then*

$$\mathrm{Tr}(QP\rho P) \geq \mathrm{Tr}(P\rho)^2 \ .$$

Using the proposition, we lower bound the probability that the first measurement outcome of the adversary is 1 and the second is 0 (so the experiment outputs 1): since $\sigma\left|+\right\rangle\!\left\langle+\right| = \sigma$,

$$\mathrm{Tr}\left(\left|+\right\rangle\!\left\langle+\right|\Pi\sigma\Pi\right) \geq \mathrm{Tr}(\Pi\sigma)^2 = \left(\frac{1}{2}+\varepsilon\right)^2 .$$

The probability that the experiment outputs 1 is thus

$$\begin{aligned}\frac{1}{4}+\frac{1}{2}\left(\mathrm{Tr}(\left|+\right\rangle\!\left\langle+\right|\Pi\sigma\Pi)+\frac{1}{2}(1-\mathrm{Tr}(\Pi\sigma))\right) &= \frac{1}{4}+\frac{1}{2}\left(\mathrm{Tr}(\left|+\right\rangle\!\left\langle+\right|\Pi\sigma\Pi)+\frac{1}{2}\left(\frac{1}{2}-\varepsilon\right)\right)\\ &\geq \frac{1}{4}+\frac{1}{2}\left(\left(\frac{1}{2}+\varepsilon\right)^2+\frac{1}{2}\left(\frac{1}{2}-\varepsilon\right)\right)\\ &\geq \frac{1}{2}+\frac{\varepsilon}{2}\ .\end{aligned}$$

□

Before proving the reverse implication, we show a basic fact about non-commuting projective measurements. Let M be some projective measurement and $\mathsf{B} = (D, I-D)$ a binary projective measurement. Consider the following experiment applied to a state ρ:

1. Measure $i \leftarrow \mathsf{M}$.
2. Apply B (and ignore the result).
3. Measure $j \leftarrow \mathsf{M}$.

The claim gives a lower bound on the probability that $i \neq j$ in terms of how well B distinguishes ρ from $\mathsf{M}(\rho)$ (which is a measure of how "non-commuting" B and M are). Variants of this claim have appeared independently and concurrently in [Zha22, CX22].

Claim 3.5. *Let D be a projector, $\mathsf{M} = (\Pi_i)_{i\in[N]}$ be a projective submeasurement and ρ be a state such that $\sum_i \mathrm{Tr}(\Pi_i\rho) = \mathrm{Tr}(\rho)$. Then*

$$\sum_j \sum_{i\neq j} \mathrm{Tr}(\Pi_i D \Pi_j \rho \Pi_j D) \geq \frac{\mathrm{Tr}(D(\rho - \mathsf{M}(\rho)))^2}{N\cdot\mathrm{Tr}(\rho)} \ .$$

Proof. Inserting resolutions of the identity, and since $(I - \sum_i \Pi_i)\rho = 0$,

$$\mathrm{Tr}(D\rho) = \sum_i \mathrm{Tr}(D\Pi_i\rho\Pi_i) + \sum_{i\neq j}\mathrm{Tr}(\Pi_i D\Pi_j\rho) = \mathrm{Tr}(D\mathsf{M}(\rho)) + \sum_j \mathrm{Tr}(\Pi_{\neq j} D\Pi_j\rho) \ ,$$

where $\Pi_{\neq j} \coloneqq \sum_{i\neq j}\Pi_i$. By Cauchy-Schwarz, $|\mathrm{Tr}(\Pi_{\neq j}D\Pi_j\rho)| \leq \sqrt{\mathrm{Tr}(\Pi_{\neq j}D\Pi_j\rho\Pi_j D)}\sqrt{\mathrm{Tr}(\rho)}$. Substituting into the above equation and applying Cauchy-Schwarz again yields the claim. □

We now prove the reverse implication.

Proof (CBB ⇒ collapsing). Let Adv be an adversary that achieves ε collapsing advantage. We design an adversary Adv' for the chosen-bit binding game as follows.

- Run $\mathsf{Adv}(\mathsf{ck})$ to obtain com and residual state ρ. Send com and a random index $i \leftarrow [\ell]$.
- Upon receipt of b from the challenger, measure the first i bits of $\mathcal{M}$, obtaining outcomes $b_1, \ldots, b_i$. If $b_i \neq b$, apply Adv's (projective) distinguishing measurement $(D, I-D)$ to ρ.
- Measure $\mathcal{M}, \mathcal{O}$, and reply with outcome (m, ω).

Let $\mathsf{M}_j(\rho)$ be the map corresponding to measuring the j^{th} bit of ρ. Let $\mathsf{M}_{[i]} \coloneqq \mathsf{M}_1(\cdots \mathsf{M}_{j-1}(\mathsf{M}_j(\rho))\cdots)$ be the map corresponding to measuring the *first* j bits of ρ, where $\mathsf{M}_{[0]}$ is the identity map. We have that

$$\rho - \mathsf{M}_{[\ell]}(\rho) = \sum_{j=0}^{n-1} \mathsf{M}_{[j]}(\rho) - \mathsf{M}_{[j+1]}(\rho) = \sum_{j=0}^{n-1} \rho_j - \mathsf{M}_{j+1}(\rho_j)$$

where $\rho_j \coloneqq \mathsf{M}_{[j]}(\rho)$.

The adversary's success probability γ in the chosen-bit binding experiment can be written as

$$\frac{1}{2\ell} \sum_{i\in[\ell]} \sum_{b\in\{0,1\}} \operatorname{Tr}(\Pi_{i,b}\rho_{i-1}) + \operatorname{Tr}(\Pi_{i,b} D \Pi_{i,1-b}\rho_{i-1}\Pi_{i,1-b} D),$$

where

$$\Pi_{i,b} \coloneqq \sum_{\substack{m,\omega \\ m_i = b \\ \mathsf{Commit}(\mathsf{ck},m,\omega)=\mathsf{com}}} |m,\omega\rangle\langle m,\omega|_{\mathcal{M},\mathcal{O}} \quad .$$

Note that the validity of Adv ensures ρ_{i-1} is in the span of $\Pi_{i,0} + \Pi_{i,1}$, which simplifies the first term of the sum: $\sum_{i\in[\ell]} \sum_{b\in\{0,1\}} \operatorname{Tr}(\Pi_{i,b}\rho_{i-1}) = \sum_{i\in[\ell]} \operatorname{Tr}(\rho_{i-1}) = \ell$. Applying Claim 3.5 and Cauchy-Schwarz, we obtain that

$$\begin{aligned}\gamma &\geq \frac{1}{2} + \frac{1}{4\ell} \sum_{i\in[\ell]} \operatorname{Tr}(D(\rho_i - \mathsf{M}_{i+1}(\rho_i)))^2 \geq \frac{1}{2} + \frac{1}{4\ell^2} \left(\sum_{i\in[\ell]} \operatorname{Tr}(D(\rho_i - \mathsf{M}_{i+1}(\rho_i))) \right)^2 \\ &= \frac{1}{2} + \frac{1}{4\ell^2} \big(\operatorname{Tr}(D(\rho - \mathsf{M}(\rho)))\big)^2 = \frac{1}{2} + \left(\frac{\varepsilon}{2\ell}\right)^2\end{aligned}$$

where the final equality follows by assumption on Adv. This completes the proof. □

Somewhere statistical binding. Using chosen-bit binding, we give a "fully classical" proof that somewhere-statistical binding commitments (resp. hash functions) are collapse binding (resp. collapsing).

Lemma 3.6. *Any post-quantum somewhere statistically binding commitment scheme (resp. hash function) is chosen-bit binding against quantum adversaries (and therefore collapse binding (resp. collapsing)).*

Proof. Let Adv be an adversary satisfying $\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1\right] = 1/2 + \varepsilon$.

We construct an adversary Adv for the SSB experiment as follows: simulate the CBB experiment with the key ck, obtaining $(\mathsf{com}, i, b, m, \omega)$. If $m_i \neq b$ or $\mathsf{Commit}(\mathsf{ck}, m, \omega) \neq \mathsf{com}$ (i.e., if the adversary loses), output $k \leftarrow [\ell]$; otherwise, output $k \leftarrow [\ell] \setminus \{i\}$. We denote by j the (uniformly sampled) binding index.

The success probability of this adversary is

$$\Pr[k = j] = \frac{1}{\ell} \cdot \Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 0\right] + \frac{1}{\ell - 1} \cdot \Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1 \wedge j \neq i\right] \quad . \tag{1}$$

Observe that the experiment outputs 1 with probability at most $1/2$ when conditioned on $j = i$ (since one of the choices for b is such that no winning pair (m, ω) exists); that is, $\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1 \;\middle|\; j = i\right] \leq 1/2$. Hence

$$\frac{1}{2} + \varepsilon = \Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1 \;\middle|\; j = i\right] \Pr[j = i] + \Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1 \wedge j \neq i\right] \quad .$$

If $\Pr[j = i] \geq (1 + \varepsilon)/\ell$ (infinitely often) then we can instead construct an adversary against SSB by simply outputting i as the guess. So we will assume otherwise; then

$$\frac{1}{2} + \varepsilon \leq \frac{1 + \varepsilon}{2\ell} + \Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1 \wedge j \neq i\right] \quad ,$$

and so $\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1 \wedge j \neq i\right] \geq \frac{1}{2}(1 - \frac{1}{\ell}) + \varepsilon \cdot (1 - \frac{1}{2\ell})$.

Substituting into (1) yields

$$\Pr[k = j] \geq \frac{1}{2\ell} + \frac{1 - \frac{1}{\ell}}{2(\ell - 1)} + \varepsilon \cdot \left(\frac{1 - \frac{1}{2\ell}}{\ell - 1} - \frac{1}{\ell}\right) = \frac{1}{\ell} + \frac{\varepsilon}{2\ell(\ell - 1)} \ ,$$

which completes the proof. □

4 Equivocality

[AGKZ20] define a notion they call *equivocal collision-resistant hash functions*, and show how these can be used to construct a variety of interesting quantum cryptographic schemes. Here we consider a slight variant, which we call a *one-time equivocal commitment scheme* (with "one-time" to distinguish this from classical notions of equivocal commitment). We note that an equivocal CRH is a one-time equivocal commitment to the bit $p(x)$ where p is the adversary's chosen predicate and x is the hash preimage, and that one-time equivocal commitments imply one-shot chameleon hash functions.

Definition 4.1. A commitment scheme is *one-time equivocal* if there exists a stateful QPT algorithm Eq such that for all messages $m \in \mathcal{M}$,

$$\Pr\left[\mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{com} \;\middle|\; \begin{array}{r} \mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda) \\ \mathsf{com} \leftarrow \mathsf{Eq}(\mathsf{ck}) \\ \omega \leftarrow \mathsf{Eq}(m) \end{array}\right] = 1 - \mathsf{negl}(\lambda) \ .$$

[AGKZ20] also informally define a "converse" notion to the above, which they call "unequivocality". A formal definition follows.

Definition 4.2. A commitment scheme is *unequivocal* if for any adversary Adv,

$$\Pr\left[\mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{com} \;\middle|\; \begin{array}{r} m \leftarrow \mathcal{M} \\ \mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda) \\ \mathsf{com} \leftarrow \mathsf{Adv}(\mathsf{ck}) \\ \omega \leftarrow \mathsf{Adv}(m) \end{array}\right] \leq \frac{1}{|\mathcal{M}|} + \mathsf{negl}(\lambda) \ .$$

While Definitions 4.1 and 4.2 are with respect to arbitrary message spaces, hereafter we focus on the case that $\mathcal{M} = \{0, 1\}$. One can immediately observe that in this case, unequivocality is identical to sum-binding (and hence, in turn, chosen-bit binding). Equivocal string commitments can be obtained from equivocal bit commitments by the usual composition.

Remark 4.3 (Equivocality vs. unequivocality)**.** Despite what the terminology suggests, we stress that equivocality and unequivocality are *not* the logical negation of one another: aside from the usual technical issues of infinitely-often vs. almost-everywhere, equivocality is syntactically much stronger than "non-unequivocality", as it requires a correct opening with all but negligible probability.

[AGKZ20] claim that an adversary breaking unequivocality yields an equivocal commitment scheme as follows (we adapt their argument to our definitions). The new commitment is a parallel repetition of the original, where the committed bit is taken to be the *majority* of the underlying commitments. To equivocate, we ask the adversary to open each underlying commitment to the same bit b. The idea is that taking the majority amplifies the small bias that adversary achieves. However, this argument has a significant flaw: what do we do when the adversary fails to equivocate on a particular commitment? In this case it may either produce an invalid opening, preventing us from opening the commitment altogether, or even consistently provide openings for $1 - b$, leading to a valid opening to the wrong bit!

We will show that, via the technique of quantum rewinding, breaking unequivocality in fact implies one-time equivocality – albeit with an *expected* polynomial-time equivocator Eq. To this end, first note that the key ck and commitment string com sent by Adv in the one-time equivocation experiment defines a *single-player quantum game* (as in [CMSZ22]): we denote by $\mathcal{G} = \mathcal{G}_{\mathsf{ck},\mathsf{com}}$ the game where Adv receives a random question $b \leftarrow \{0,1\}$, replies with ω and wins if the predicate $f(b,\omega) = \mathsf{Commit}(\mathsf{ck}, b, \omega) = \mathsf{com}$ is satisfied. We call $\omega_{\mathcal{G}}(\mathsf{Adv}, \rho)$ the winning probability of Adv when its internal state is ρ at the start of the game (i.e., after it sends com in the experiment).

We will make use of the following two lemmas, which are simplified versions of [CMSZ22, Lemmas 4.9 and 4.10].

Lemma 4.4. *Given a* $\mathrm{poly}(\lambda)$*-time adversary* Adv *for the game* $\mathcal{G}$ *and two real parameters* $\gamma, \delta > 0$*, there exists a real-valued* $\mathrm{poly}(\lambda, \varepsilon, \log 1/\delta)$*-time measurement* $\mathsf{ValEst} = \mathsf{ValEst}_{\mathcal{G}}$ *satisfying the following.*

(i) $\mathbb{E}_{p \leftarrow \mathsf{ValEst}(\rho)}[p] = \omega_{\mathcal{G}}(\mathsf{Adv}, \rho)$*;*

(ii) ValEst *is* (γ, δ)*-almost projective, that is, applying* ValEst *twice in a row to* ρ *yields* p, p' *such that* $\Pr[|p - p'| \leq \gamma] \geq 1 - \delta$*;*

(iii) If ρ' *is the post-measurement state of an application of* ValEst *on* ρ*, then* $\omega_{\mathcal{G}}(\mathsf{Adv}, \rho') \geq \omega_{\mathcal{G}}(\mathsf{Adv}, \rho) - \delta$*.*

Lemma 4.5. *Let* M *and* $\Pi = (\Pi_0, \Pi_1)$ *be* (γ, δ)*-almost projective and projective measurements, respectively. For any positive integer* t*, there exists a procedure* $\mathsf{Repair}_t^{\mathsf{M},\Pi}(p, b)$*, that applies* M *and* Π *a total of* $O(1 + t\sqrt{\delta})$ *times in expectation, such that the following is a* $\big(2\gamma, O(1/t + \sqrt{\delta})\big)$*-projective measurement: apply* M *followed by* Π*, obtaining outcomes* p *and* b*; run* $\mathsf{Repair}_t^{\mathsf{M},\Pi}(p, b)$ *on the post-measurement state; and output* p*.*

We are now ready to show that (almost-everywhere) non-unequivocality implies one-time equivocality (with an expected polynomial time equivocator). Our one-time equivocal commitment scheme is constructed as follows.

Construction 4.6. Let $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ be a commitment scheme. For $r \in \mathbb{N}$, we construct COM^r as follows:

- $\mathsf{Gen}^r(1^\lambda)$ runs, for each $i \in [r]$, $\mathsf{ck}_i \leftarrow \mathsf{Gen}(1^\lambda)$, and outputs $\mathsf{ck} \coloneqq (\mathsf{ck}_1, \ldots, \mathsf{ck}_r)$.
- $\mathsf{Commit}^r((\mathsf{ck}_1, \ldots, \mathsf{ck}_r), m, (i, \omega)) \coloneqq (i, \mathsf{Commit}(\mathsf{ck}_i, m, \omega))$.

Given an adversary Adv for the unequivocality experiment (Definition 4.2) with quantum auxiliary input ρ, we construct an equivocator as follows. Eq has as auxiliary input r copies of ρ on registers $\mathcal{A}_1, \ldots, \mathcal{A}_r$.

- $\mathsf{Eq}_\varepsilon^{\mathsf{Adv}}(\mathsf{ck}_1, \ldots, \mathsf{ck}_r; \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_r)$:
  1. For each $i \in [r]$:
     (a) Run $\mathsf{com}_i \leftarrow \mathsf{Adv}(\mathsf{ck}_i; \mathcal{A}_i)$.
     (b) Apply $\mathsf{ValEst}_{\mathcal{G}}$ (where $\mathcal{G} = \mathcal{G}_{\mathsf{ck}_i,\mathsf{com}_i}$) to $\mathcal{A}_i$ with parameters $\gamma = \varepsilon^2/(8\lambda)$ and $\delta = 2^{-\lambda}$, obtaining outcome p_i.
     (c) If $p_i \geq 1/2 + 3\varepsilon/4$, set $i^* \coloneqq i$ and stop.
  2. If i^* is not set, output $\perp$.
  3. Otherwise, output $(i^*, \mathsf{com}_{i^*})$ as the commitment and set $p \coloneqq p_{i^*}$. At this point we can discard $\mathcal{A}_i$ for $i \neq i^*$.
- $\mathsf{Eq}_\varepsilon^{\mathsf{Adv}}(b; \mathcal{A}_{i^*})$:
  Repeat the following at most λ/ε times:
  1. Apply the measurement $\mathsf{B} = (\Pi_b, I - \Pi_b)$ to $\mathcal{A}_{i^*}$. If the outcome is 1, measure the adversary's response ω, output (i^*, ω), and stop.

2. Otherwise, run $\mathsf{Repair}_{\delta^{-1/2}}^{\mathsf{ValEst}_{\mathcal{G}},\mathsf{B}}(p,b)$ and update $p \leftarrow \mathsf{ValEst}_{\mathcal{G}}$ (with the same parameters as above).

Theorem 4.7. *Let* COM *be a commitment scheme admitting a* $\mathrm{poly}(\lambda)$*-time adversary* Adv *that produces a valid opening in the experiment of Definition 4.2 with probability* $1/2+\varepsilon$ *where* $\varepsilon = \mathrm{poly}(1/\lambda)$ *(i.e., that violates unequivocality infinitely often). Then, with* $r = \lambda/\varepsilon$*, Construction 4.6 yields a one-time equivocal commitment scheme* COM^r *with an expected* $\mathrm{poly}(\lambda)$*-time equivocator.*

Proof. By assumption, $\mathbb{E}[p_i] = \mathbb{E}[\omega_{\mathcal{G}_{\mathsf{ck}_i,\mathsf{com}_i}}(\rho_i)] \geq 1/2+\varepsilon$, where ρ_i is the post-measurement state after Step 1a. Hence by Proposition 2.1, $\Pr[p \geq 1/2+3\varepsilon/4] \geq \varepsilon/4$. Since each iteration of the loop is independent, the probability that $p_i < 1/2+3\varepsilon/4$ for all $i \in [r]$ is at most $(1-\varepsilon/4)^r \leq e^{-\lambda/4} = \mathsf{negl}(\lambda)$.

This shows that $\mathsf{Eq}(\mathsf{ck}_1,\ldots,\mathsf{ck}_r)$, with $\mathsf{Eq} = \mathsf{Eq}_{\varepsilon}^{\mathsf{Adv}}$, outputs (i^*,com_{i^*}) for some $i^* \in [r]$ except with probability $\mathsf{negl}(\lambda)$. (Note that this step of Eq runs in strict $\mathrm{poly}(\lambda)$ time.) We now move on to the analysis of $\mathsf{Eq}(b)$. Set $\mathsf{ck} = \mathsf{ck}_{i^*}$, $\mathsf{com} = \mathsf{com}_{i^*}$, $\mathcal{A} = \mathcal{A}_{i^*}$ and recall that $(\Pi_b, I-\Pi_b)$ is the projective measurement corresponding to the whether Adv wins the unequivocality experiment when the challenge is b (that is, Π_b projects onto the subspace spanned by $|b,\omega\rangle$ such that $\mathsf{Commit}(\mathsf{ck},b,\omega) = \mathsf{com}$).

Let ρ_j be the state in $\mathcal{A}$ in the beginning of iteration $j \in [\lambda/\varepsilon]$ of $\mathsf{Eq}(b)$ and b_j be the output of Π in the same iteration. We now argue that $\Pr[b_j = 1]$ is lower bounded for all j: since $p \geq 1/2+3\varepsilon/4$, by item (iii) of Lemma 4.4, we have $\frac{1}{2}\operatorname{Tr}\left((\Pi_0+\Pi_1)\rho_1\right) \geq p-\delta$, and thus $\operatorname{Tr}(\Pi_b\rho_1) \geq \varepsilon/2$. Since $\gamma = \varepsilon^2/8$, the estimate-repair procedure of Lemma 4.5 is $(\varepsilon^2/4, O(\sqrt{\delta}))$-almost projective. Then $\Pr[b_j = 1] = \operatorname{Tr}(\Pi_b\rho_j) \geq \frac{\varepsilon}{2} - \frac{\lambda}{\varepsilon}\cdot\frac{\varepsilon^2}{4\lambda} = \varepsilon/4$ for all j, except with probability $O(\sqrt{\delta}/\varepsilon) = \mathsf{negl}(\lambda)$. Note, moreover, that as each iteration runs in expected $O(1)$ time, the total (expected) runtime is $O(\lambda/\varepsilon) = \mathrm{poly}(\lambda)$.

The random variables b_j are not independent; however, we can conclude by showing that they stochastically dominate a sequence of independent random variables.

Claim 4.8 (Stochastic dominance)**.** *Let* $b_1,\ldots,b_n$ *be a sequence of binary random variables such that for all* $j \in [n]$*,* $\Pr[b_j = 1 \mid b_1,\ldots,b_{j-1}] \geq p$*. Then*

$$\Pr\left[b_j = 0 \ \forall j \in [n]\right] \leq (1-p)^n$$

Using the foregoing claim for the *conditional probability space* (with measure $1-\mathsf{negl}(\lambda)$) where the first step of Eq does not return $\perp$ and $\Pr[b_j = 1] \geq \varepsilon/4$ for all j (where it holds, in particular, that $\Pr[b_j = 1 \mid b_i, i \neq j]$ is lower bounded by the same value), we conclude that either $\mathsf{Eq}(\mathsf{ck}_1,\ldots,\mathsf{ck}_r)$ aborts or $\mathsf{Eq}(b)$ does not return a valid opening with probability at most

$$(1-\varepsilon/4)^{\lambda/\varepsilon} + \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda). \qquad \square$$

References

[ACP21] Prabhanjan Ananth, Kai-Min Chung, and Rolando L. La Placa. On the concurrent composition of quantum zero-knowledge. In *CRYPTO (1)*, volume 12825 of *Lecture Notes in Computer Science*, pages 346–374. Springer, 2021.

[AGKZ20] Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In *Proceedings of the 52nd Annual ACM Symposium on Theory of Computing*, STOC '20, pages 255–268, 2020.

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '14, pages 474–483, 2014.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security*, ASIACRYPT '11, pages 41–69, 2011.

[BZ13a] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 592–608. Springer, 2013.

[BZ13b] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *CRYPTO (2)*, volume 8043 of *Lecture Notes in Computer Science*, pages 361–379. Springer, 2013.

[CCY21] Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa. A black-box approach to post-quantum zero-knowledge in constant rounds. In *CRYPTO (1)*, volume 12825 of *Lecture Notes in Computer Science*, pages 315–345. Springer, 2021.

[CDMS04] Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail. Computational collapse of quantum state with application to oblivious transfer. In *TCC*, volume 2951 of *Lecture Notes in Computer Science*, pages 374–393. Springer, 2004.

[CMSZ22] Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry. Post-quantum succinct arguments: breaking the quantum rewinding barrier. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 49–58. IEEE, 2022.

[CX22] Shujiao Cao and Rui Xue. The gap is sensitive to size of preimages: Collapsing property doesn't go beyond quantum collision-resistance for preimages bounded hash functions. Cryptology ePrint Archive, Paper 2022/671, 2022. `https://eprint.iacr.org/2022/671`.

[FLPS21] Prastudy Fauzi, Helger Lipmaa, Zaira Pindado, and Janno Siim. Somewhere statistically binding commitment schemes with applications. In *Financial Cryptography (1)*, volume 12674 of *Lecture Notes in Computer Science*, pages 436–456. Springer, 2021.

[GYZ17] Sumegha Garg, Henry Yuen, and Mark Zhandry. New security notions and feasibility results for authentication of quantum data. In *CRYPTO (2)*, volume 10402 of *Lecture Notes in Computer Science*, pages 342–371. Springer, 2017.

[HW15] Pavel Hubácek and Daniel Wichs. On the communication complexity of secure function evaluation with long output. In *ITCS*, pages 163–172. ACM, 2015.

[LMS21] Alex Lombardi, Fermi Ma, and Nicholas Spooner. Post-quantum zero knowledge, revisited (or: How to do quantum rewinding undetectably). *CoRR*, abs/2111.12257, 2021.

[LZ19] Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat–Shamir. In *Proceedings of the 39th Annual International Cryptology Conference*, CRYPTO '19, pages 326–355, 2019.

[Unr16a] Dominique Unruh. Collapse-binding quantum commitments without random oracles. In *Proceedings of the 22nd International Conference on the Theory and Applications of Cryptology and Information Security*, ASIACRYPT '16, pages 166–195, 2016.

[Unr16b] Dominique Unruh. Computationally binding quantum commitments. In *Proceedings of the 35th Annual International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT '16, pages 497–527, 2016.

[Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In *Proceedings of the 38th Annual International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT '19, pages 408–438, 2019.

[Zha22] Mark Zhandry. New constructions of collapsing hashes. Cryptology ePrint Archive, Paper 2022/678, 2022. `https://eprint.iacr.org/2022/678`.