On the Necessity of Collapsing for Post-Quantum and Quantum Commitments

Marcel Dall'Agnol ✉ 🏠
University of Warwick, Coventry, UK

Nicholas Spooner ✉ 🏠
University of Warwick, Coventry, UK

Abstract

Collapse binding and collapsing were proposed by Unruh (Eurocrypt '16) as post-quantum strengthenings of computational binding and collision resistance, respectively. These notions have been very successful in facilitating the "lifting" of classical security proofs to the quantum setting. A basic and natural question remains unanswered, however: are they the *weakest* notions that suffice 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). We also generalise the definition of collapse binding to *quantum commitment schemes*, and prove that the equivalence carries over when the sender in this commit-and-open protocol communicates quantum information.

As a consequence, we establish that a variety of "weak" binding notions (sum binding, CDMS binding and unequivocality) are in fact *equivalent* to collapse binding, both for post-quantum and quantum commitments.

Finally, we prove a "win-win" result, showing that a post-quantum computationally binding commitment scheme that is not collapse binding can be used to build an equivocal commitment scheme (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.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography; Theory of computation → Quantum computation theory

Keywords and phrases Quantum cryptography, Commitment schemes, Hash functions, Quantum rewinding

Digital Object Identifier 10.4230/LIPIcs.TQC.2023.2

Related Version *Full Version*: https://eprint.iacr.org/2022/786

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 simply 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 [6], message authentication codes [7, 17], as well as signatures and CCA-secure encryption [8].

18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023).
Editors: Omar Fawzi and Michael Walter; Article No. 2; pp. 2:1–2:23
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

This work studies the notion of *computational binding* (and the related notion of *collision resistance*) against quantum adversaries. While a natural quantum analogue of computational binding asserts that it is infeasible for a quantum computer to furnish valid openings of a commitment to more than one message, [1] demonstrated that this definition is not sufficient for many applications of commitment schemes. The key issue is that while binding rules out finding openings to distinct messages *simultaneously*, it does not rule out being able to "choose" the message that is opened. Note that this is an exclusively quantum problem: a classical algorithm able to make such a choice can break computational binding via rewinding.

Unruh [24] proposed post-quantum strengthenings of computational binding and collision resistance (for classical protocols) called *collapse binding* and *collapsing*, respectively. These have since become central in post-quantum cryptography: a sequence of works [24, 20, 3, 10, 11, 21] has demonstrated that this strengthening is sufficient to prove post-quantum security for various important schemes. Roughly speaking, these properties state that an adversary that has committed to a superposition of messages cannot tell whether or not that superposition has been measured.

Collapsing hash functions can be built from LWE [23]; additionally, any CRH that satisfies a certain regularity property is collapsing, which includes constructions from LPN and isogenies, and plausibly functions like SHA [30, 9]. Nonetheless, in general there remains a gap between collapsing and collision resistance. Zhandry [28, 29] showed 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.

Quantum commitments

So far we have restricted our attention to the security of classical schemes against quantum adversaries (*post-quantum* security). Complicating matters further, however, quantum *communication* enables the construction of "intrinsically quantum" cryptographic constructions for which classical notions of security may not even apply. In *quantum commitment schemes*, where commitments and openings are (possibly entangled) quantum states, the basic notion of computational binding does not have a clear analogue; indeed, finding an appropriate definition of binding for quantum commitments has proved difficult [14, 27, 15, 4, 5], even in the statistical case, owing to an adversary's ability to commit to a superposition of messages.

2 Results

In this work we investigate collapse binding and related properties. We first propose a definition of collapse binding for quantum commitments (formalised in Definition 20). Then, using chosen-bit binding as a bridge, we show that collapse binding is equivalent to CBB (Theorems 2 and 4) and sum binding (Corollary 5), among others, both for post-quantum and quantum commitments.

Lastly, we use quantum rewinding techniques to show that, if computational and collapse binding are distinct, then a commitment scheme in this gap can be used to construct a *one-shot equivocal* scheme and, consequently, a variety of useful quantum cryptographic primitives (see Section 6).

▶ Remark 1 (Quantum vs. post-quantum results). For clarity, in this section we discuss the post-quantum versions of our experiments and results. We stress, however, that our proofs hold with respect to both quantum and classical (i.e., post-quantum) versions of the experiments.

(Note that, as the standard definition of quantum commitment schemes does not include post-quantum as a special case, this is not trivial; see Section 2.2 for a discussion.) ⌟

2.1 Chosen-bit binding commitments

We introduce a new notion of binding we call *chosen-bit binding*, which is defined in terms of an interactive game against a (potentially quantum) adversary Adv.

Let $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ be a commitment scheme for the set of messages $M = \{0,1\}^{\ell(\lambda)}$. The chosen-bit binding experiment is as follows. (See Experiment 25 for the general version.)

1. Sample a commitment key $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. Obtain an index-commitment pair $(i, \mathsf{com}) \leftarrow \mathsf{Adv}(\mathsf{ck})$.
3. Sample $b \leftarrow \{0,1\}$ uniformly at random.
4. Obtain a message-opening pair $(m, \omega) \leftarrow \mathsf{Adv}(b)$.
5. Output 1 if $m_i = b$ and $\mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{com}$.

We say that COM is chosen-bit binding (CBB) if, for every efficient adversary Adv, the above experiment outputs 1 with probability at most $1/2 + \mathsf{negl}(\lambda)$. Note that the definition of CBB is agnostic to the actual form of the commitment, which is used only as an abstract functionality. It therefore readily applies to both classical and quantum commitments, as well as to schemes where the commit or reveal phases are interactive[1] (or even to "physical" commitments like a locked safe).

Note, also, that CBB is equivalent to requiring that COM be a *sum-binding bit commitment at every coordinate* $i \in [\ell]$ (which is distinct from Definition 18, the natural generalisation of sum binding to message spaces with size larger than 2); the CBB experiment concisely captures all ℓ sum binding experiments into one.

It is straightforward to show, via rewinding, that classical CBB is equivalent to computational binding. Our first result is an equivalence between CBB against quantum adversaries and collapsing.

▶ **Theorem 2.** *A classical commitment scheme is collapse binding if and only if it is post-quantum chosen-bit binding.*

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 (3-message protocols where the prover initiates, consisting of (1) commitments to s strings; (2) a challenge $C \subseteq [s]$; and (3) for each $i \in C$, an opening of the i^{th} string). Indeed, it was shown in [21] that any classically secure commit-and-open protocol is post-quantum secure when instantiated with a collapse binding commitment. Our result yields a converse:

▶ **Corollary 3.** *There exists a classical commit-and-open protocol which is insecure when instantiated with a commitment that is not collapse binding.*

We note, however, that Theorem 2 follows from a more general result: since Definition 20 captures collapse binding of commitments with either classical or quantum messages, we prove the equivalence between collapse and chosen-bit binding for a generalisation that captures both quantum and post-quantum schemes (Definition 14; see also Remark 16).

[1] In this work we restrict our attention to noninteractive commitments. All of our results easily generalise to the setting where the commit phase is interactive. However, the definition of collapse binding seems to crucially rely on the *reveal* phase being noninteractive.

▶ **Theorem 4.** *A quantum commitment scheme is collapse binding if and only if it is chosen-bit binding.*

Several works [15, 25, 5] aim to surmount the difficulties of basing cryptographic protocols on the binding guarantees of quantum commitments, especially for computational security. We hope that introducing a notion of collapse binding for quantum commitments will allow for some of the successes in the post-quantum case to be carried over to the quantum setting.

2.2 Connections to existing notions

▶ **Corollary 5.** *Sum binding is equivalent to collapse binding for quantum and post-quantum bit commitments.*

This corollary improves upon and generalises results from prior work. In the classical (post-quantum) setting, Unruh [23] proves that collapse binding implies sum binding; one of the main contributions of this paper is proving the converse.[2]

In the quantum setting, Yan [26, Appendix F] shows that for parallel repetitions of "canonical" quantum bit commitments (which capture the one-bit case of the schemes in Experiments 17 and 25), sum binding implies collapse binding – though that work does not give a definition of the latter.[3] Definition 20 is the natural extension of collapse binding to quantum commitments (which does not appear in prior work), and enables us to generalise Yan's result to arbitrary string commitments; note that these include *compressing* commitments, which implies an analogous equivalence for hash functions (see Section 2.2.2).

For general ℓ, (classical) chosen-bit binding is a special case of so-called "CDMS binding" [12, 24]. 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 com is a fixed commitment previously output by Adv and y is chosen uniformly at random from Y. Unruh [23] showed that collapsing implies CDMS binding for all function classes where $|Y|$ is polynomial. CBB is easily seen to be equivalent to CDMS binding when F is the class of one-bit projection functions; we hence obtain the following corollary.

▶ **Corollary 6.** *CDMS binding against quantum adversaries 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.

[2] We note that the following seemingly simpler strategy towards Theorem 2 does not suffice: (i) prove sum binding implies collapse binding for bit commitments; then (ii) use Unruh's parallel repetition theorem [23] to "lift" the equivalence to string commitments. This strategy only works for parallel repetitions of bit commitments, whereas Theorem 2 holds for any string commitment (and extends to hash functions).

[3] In fact, [26] shows that for canonical quantum commitments, (i) *honest* binding (a seemingly weaker notion) is equivalent to sum binding; and (ii) honest binding implies a "computational collapse" property that is equivalent to collapse binding. This result relies on the particular structure of canonical quantum bit commitments.

2.2.1 Somewhere statistical binding and parallel repetition

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 enables "fully classical" proofs that previously required quantum machinery, as we demonstrate next.

We use the chosen-bit binding definition to reprove two known results: the (folklore) fact that somewhere statistically binding (SSB) commitment schemes are collapse binding; and the preservation of the collapse-binding property under parallel repetitions [24].

▶ **Lemma 7.** *Any somewhere-statistically binding commitment scheme is chosen-bit binding; in particular, post-quantum SSB commitment schemes are collapsing.*

▶ **Lemma 8.** *If a commitment scheme* COM *is chosen-bit binding, then is* k*-fold parallel repetition* COM^k *is also chosen-bit binding.*

2.2.2 Hash functions

While we shall only discuss commitment schemes in the body of the paper, for our purposes collision-resistant hash functions are binding (but not hiding) *classical* commitment schemes where the length of the randomness is zero; therefore, many of our results extend to CRHs *mutatis mutandis.*

More precisely, consider the analogous (classical) chosen-bit binding experiment for a family $\mathcal{H}_\lambda \subseteq \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}$ of hash functions defined next.

1. Sample $h \leftarrow \mathcal{H}_\lambda$.
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 $x \leftarrow \mathsf{Adv}(b)$.
5. Output 1 if $h(x) = y$ and $x_i = b$.

We say that $\mathcal{H}$ is classically (resp. post-quantum) chosen-bit binding (CBB) if for every efficient classical (resp. quantum) adversary Adv, the above experiment outputs 1 with probability at most $1/2 + \mathsf{negl}(\lambda)$.

Classical chosen-bit binding for hash functions is easily seen to be equivalent to collision resistance, and, by an essentially identical argument to Theorem 2, we can show that post-quantum CBB is equivalent to collapsing.

▶ **Corollary 9.** *A hash family* $\mathcal{H}$ *is collapsing if and only if it is post-quantum chosen-bit binding.*

Note that CBB also implies a method by which a quantum falsifier can convince a classical party that a hash function is *not* collapsing.

2.3 Equivocality

A (classical) commitment scheme is *one-shot equivocal* [2] if it has an additional functionality Eq, the equivocator, which produces a commitment string com and then, given a message m, outputs a valid opening ω to it (with probability close to 1).[4] In other words, Eq generates a commitment com it can *equivocate* to any message of its choice (but only once, if the scheme is computationally binding).

[4] While [2] defines equivocality for hash functions, it easily extends to commitment schemes. Indeed, the functionality they require is that of a commitment, which suffices to ensure security of the cryptographic objects constructed in that work.

We observe first that what [2] call "unequivocality" – roughly, that achieving the above with any nontrivial advantage is computationally infeasible – implies chosen-bit binding, and hence collapsing. This resolves an open question of [2].

However, we are able to show something much stronger, in the spirit of the "win-win" results of [28, 29]. In particular, we show that if a commitment scheme is (almost everywhere) *not* collapse binding, then it is one-shot equivocal. Note that the latter is a much stronger property than the negation of unequivocality, since Eq must succeed with probability close to 1. More formally, we obtain the following.[5]

▶ **Theorem 10** (Theorem 41, informally stated). *If* COM *is a post-quantum computationally but not sum-binding commitment scheme, it can be transformed into a one-shot equivocal scheme.*

Our proof uses recent quantum rewinding techniques [11] to amplify success probability. We remark that while [21, 11] build upon "Unruh's lemma" [22] – which shows that if a pair of projective measurements succeed with sufficiently high probability, then so does their sequential application – it is insufficient for our purposes.

We instead use an early quantum rewinding lemma [13], which ensures one-shot equivocality for any inverse-polynomial advantage against COM in the collapse binding experiment (Unruh's lemma would only apply assuming constant advantage).

3 Preliminaries

We denote by $\lambda \in \mathbb{N}$ the security parameter, and when we refer to probabilistic/quantum polynomial-time (PPT/QPT) algorithms, the time complexity is a polynomial in λ. We denote by $\mathsf{negl}(\lambda)$ any function asymptotically smaller than every inverse polynomial, i.e, that is $o(\lambda^{-c})$ for every $c \in \mathbb{N}$.

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 sampled uniformly from S. When D is a distribution, its support is denoted $\mathrm{supp}(D)$ and $i \leftarrow D$ denotes that i is chosen according to D.

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

▶ **Proposition 11.** *Let X be a random variable supported on $[0, 1]$. Then for all $\alpha \geq 0$, $\Pr[X \geq \alpha] \geq E[X] - \alpha$.*

▶ **Proposition 12** (Chernoff bound). *Let $X_1, \ldots, X_k$ be independent Bernoulli random variables distributed as X. Then, for every $\delta \in [0, 1]$,*

$$\Pr\left[\frac{1}{k}\sum_{i=1}^{k} X_i \geq (1+\delta)\mathbb{E}[X]\right] \leq e^{-\frac{\delta^2 k \mathbb{E}[X]}{3}} \quad \textit{and}$$

$$\Pr\left[\frac{1}{k}\sum_{i=1}^{k} X_i \leq (1-\delta)\mathbb{E}[X]\right] \leq e^{-\frac{\delta^2 k \mathbb{E}[X]}{2}}.$$

We also make use of the Cauchy-Schwarz inequality with respect to the Hilbert-Schmidt inner product.

[5] It is claimed in [2] that if COM is not unequivocal, its parallel repetition COM^k is equivocal for large enough k. This is in fact true, but their argument is flawed; see Remark 34 for a discussion.

▶ **Lemma 13** (Cauchy-Schwarz). *For any complex matrices A, B such that $A^\dagger B$ is defined,*

$$\left|\mathrm{Tr}\left(A^\dagger B\right)\right|^2 \leq \mathrm{Tr}\left(A^\dagger A\right) \cdot \mathrm{Tr}\left(B^\dagger B\right) \ .$$

We say a commitment scheme is *classical* when all of its communication is classical (but an adversary may be quantum); that is, we use classical commitments as a shorthand for classical-*message* commitments.

By the *k-fold parallel repetition* of an experiment/interactive protocol, we denote that which results from repeating it independently k times *with the same first message* (in our case, a commitment key ck); the output of the experiment is the conjunction of the outputs of each execution.

3.1 Quantum information

We recall the basics of quantum information. (Most of the following is taken almost verbatim from [11].) 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, and we use $|\mathbf{0}\rangle$ to refer to a fixed ("zero") state in $\mathcal{H}$. 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. $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, and we sometimes write $\mathcal{H} \setminus \mathcal{H}_2$ to denote $\mathcal{H}_1$; we also write $\rho^{\mathcal{H}_1}$ 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 $\Pi^2 = \Pi$. If a (unitary U or) projector Π in a Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ acts trivially (as the identity $\mathbf{I}$) in $\mathcal{H}_2$, we may write Π or $\Pi^{\mathcal{H}_1}$ to denote $\Pi \otimes \mathbf{I}^{\mathcal{H}_2}$. A collection of projectors $\mathsf{M} = (\Pi_i)_{i \in S}$ is a *projective measurement* when $\sum_{i \in S} \Pi_i = \mathbf{I}$, and a *submeasurement* when there exists a projector Π such that $\sum_{i \in S} \Pi_i = \mathbf{I} - \Pi$.

The application of M to a pure state $|\psi\rangle$ yields outcome $i \in S$ with probability $p_i = \|\Pi_i |\psi\rangle\|^2$; we denote sampling from this distribution by $i \leftarrow \mathsf{M}(\rho)$, and in this case the post-measurement state is $|\psi_i\rangle = \Pi_i |\psi\rangle / \sqrt{p_i}$. We also use $\sigma \leftarrow \mathsf{M}(\rho)$ to denote the mixture of post-measurement states $\Pi_i |\psi\rangle / \sqrt{p_i}$ with probability p_i. A two-outcome projective measurement is called a *binary projective measurement*, and is written as $\mathsf{M} = (\Pi, \mathbf{I} - \Pi)$, 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 (i.e., $\mathrm{Tr}(T(\rho)) = \mathrm{Tr}(\rho)$ for every $\rho \in \mathbf{S}(\mathcal{H})$) 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, with $\mathrm{Tr}_{\mathcal{K}}$ the partial trace operator that traces out $\mathcal{K}$, we have $T(\rho) = \mathrm{Tr}_{\mathcal{K}}(U(\rho \otimes |0\rangle\!\langle 0|^{\mathcal{K}})U^\dagger)$. 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 $O(|T|)$.

4 Commitment schemes

In this section, we define commitment schemes and the different notions of binding that we shall use (except for CBB, whose definition we defer to Section 5). While most of what follows is not novel, to the best of our knowledge the notion of collapse binding has as yet only been defined and studied for *classical* commitments. Our definition generalises that put forth by [24] (and coincides with it in the classical case).

▶ **Definition 14.** *A* quantum commitment scheme COM *consists of a PPT algorithm* Gen*, a unitary QPT algorithm* Commit *acting on a 4-tuple of registers $\mathcal{K} \otimes \mathcal{M} \otimes \mathcal{C} \otimes \mathcal{O}$, and a "check" subregister $\mathcal{S} \subseteq \mathcal{C} \otimes \mathcal{O}$.*

Commit *uses the key register $\mathcal{K}$ and message register $\mathcal{M}$ as classical controls. The dimension of $\mathcal{K}$ is $\left|\mathrm{supp}\left(\mathsf{Gen}(1^\lambda)\right)\right|$ and $\mathcal{M}$ has $\ell(\lambda)$ qubits; its computational basis is labeled by elements of the* message spaces $\{M_\lambda\}_{\lambda\in\mathbb{N}}$*, where $M = \{0,1\}^{\ell(\lambda)}$.*

In addition, $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit}, \mathcal{S})$ *is a* bit commitment *if $\ell = 1$, i.e., if $M_\lambda = \{0,1\}$ for all $\lambda \in \mathbb{N}$.*

As the register $\mathcal{S}$ will be clear from context, we use $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ as shorthand for $(\mathsf{Gen}, \mathsf{Commit}, \mathcal{S})$. Moreover, we denote by $\mathsf{Commit}_{\mathsf{ck},m}$ the unitary acting on $\mathcal{C} \otimes \mathcal{O}$ as $\mathsf{Commit}_{\mathsf{ck},m} |\psi\rangle = \mathsf{Commit} |\mathsf{ck}\rangle |m\rangle |\psi\rangle$.

▶ **Definition 15.** *A* classical commitment scheme $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ *is a quantum commitment scheme where* Commit *is a PPT algorithm and $\mathcal{S} = \mathcal{C}$.*

We use function notation for classical commitments, i.e., $\mathsf{Commit}(\mathsf{ck}, m, \omega)$ is the function computed and inserted (by a bitwise XOR) into the commitment register $\mathcal{C}$.

▶ Remark 16. Our definition of quantum commitment schemes deviates slightly from those in the literature in order to generalise classical commitments. In prior work it is typically assumed that quantum commitments are generated *deterministically*, which is without loss of generality since any randomness can be "purified out". Then the challenger may measure both $\mathcal{C}$ and $\mathcal{O}$ in the last step to check that $\mathsf{Commit}^\dagger_{\mathsf{ck},m}$ indeed inverts the adversary's computation (i.e., the challenger checks the register $\mathcal{S} = \mathcal{C} \otimes \mathcal{O}$).

However, in classical commitments randomness is inherent and *only the $\mathcal{C}$ register* is "uncomputed": the challenger reads ω from $\mathcal{O}$ and checks that the contents of $\mathcal{C}$ coincide with $\mathsf{Commit}(\mathsf{ck}, m, \omega)$. This corresponds to applying $\mathsf{Commit}^\dagger_{\mathsf{ck},m}(\mathcal{C}, \mathcal{O})$ and only measuring $\mathcal{S} = \mathcal{C}$.

(Given this discussion, it is natural to ask whether, for quantum commitments, it suffices to measure only $\mathcal{C}$. We leave this question to future work.) ⌟

We now define two notions of binding (sum and collapse) that apply to both quantum and classical commitments. Recall that, in order to be non-trivial, commitment schemes typically also satisfy a notion of hiding, which we omit since it is not relevant to the current work.

▶ **Experiment 17** (Sum binding)**.** *Given an adversary* Adv*, define the experiment* $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{sum}}(\lambda)$*, parametrised by $\lambda \in \mathbb{N}$, as follows.*

1. *Generate* $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. *Obtain the commitment register* $\mathcal{C} \leftarrow \mathsf{Adv}(\mathsf{ck})$.
3. *Sample a (classical) message* $m \leftarrow M$.
4. *Obtain the opening register* $\mathcal{O} \leftarrow \mathsf{Adv}(m)$*, apply* $\mathsf{Commit}^\dagger_{\mathsf{ck},m}(\mathcal{C}, \mathcal{O})$ *and measure $\mathcal{S}$ in the computational basis.*
5. *Output 1 if the measurement yields $|\mathbf{0}\rangle$.*

▶ **Definition 18.** *A quantum commitment scheme* COM *is sum binding if, for all non-uniform QPT adversaries* Adv *in Experiment 17,*

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

When COM *is classical and* Adv *is PPT (resp. QPT), we say it is classically (resp. post-quantum) sum binding.*

Note that the definition of sum binding given by [24] refers only to bit commitments; the above is a natural generalisation to quantum commitments and larger message spaces (which seems, however, to be of limited use when M is of superpolynomial size).

We proceed to the definition of collapse binding for quantum commitments.

▶ **Experiment 19** (Collapse binding). *For an adversary* Adv, *define the experiment* $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{coll}}(\lambda)$ *as follows.*

1. *Generate* $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. *Obtain the registers* $\mathcal{C} \otimes \mathcal{M} \otimes \mathcal{O} \leftarrow \mathsf{Adv}(\mathsf{ck})$.
3. *Sample* $b \leftarrow \{0,1\}$. *If* $b = 1$, *measure* $\mathcal{M}$ *in the computational basis.*
4. *Obtain* $b' \leftarrow \mathsf{Adv}(\mathcal{M} \otimes \mathcal{O})$.
5. *Output* 1 *if* $b = b'$.

We say that Adv is valid if, for all $\mathsf{ck} \in \operatorname{supp}\big(\mathsf{Gen}(1^\lambda)\big)$, the state ρ in $\mathcal{C}\otimes\mathcal{M}\otimes\mathcal{O} \leftarrow \mathsf{Adv}(\mathsf{ck})$ is a mixture of superpositions of valid commitments; that is, $\rho = \sum_i p_i \left|\psi_i\middle\rangle\middle\langle\psi_i\right|$ where $|\psi_i\rangle$ has nonzero amplitude only on computational basis states $|\mathsf{com}, m, \omega\rangle$ in the image of the projector $\mathsf{Commit}_{\mathsf{ck},m} \left|\mathbf{0}\middle\rangle\middle\langle\mathbf{0}\right|^{\mathcal{S}} \mathsf{Commit}^\dagger_{\mathsf{ck},m}$. (In the post-quantum case, this simplifies to $|m, \omega\rangle$ satisfying $\mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{com}$.)

▶ **Definition 20.** *A quantum commitment scheme* COM *is collapse binding if, for all* valid *non-uniform QPT adversaries* Adv *in Experiment 19,*[6]

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

Note that the challenger does not return the register $\mathcal{C}$ to the adversary in Step 4 for the purpose of distinguishing; this is crucially used in the proof of Theorem 4, and would otherwise lead to an unsatisfiable generalisation of classical commitments: an adversary that sends $\sum_{m\in M} |\mathsf{Commit}(\mathsf{ck}, m, \omega)\rangle\, |m\rangle\, |\omega\rangle$ (normalised) and receives all three registers can detect a measurement with high probability by uncomputing Commit and using the binary measurement with projector $\left|\psi\middle\rangle\middle\langle\psi\right|^{\mathcal{M}}$ where $|\psi\rangle = \sum_{m\in M} |m\rangle$.

4.1 Classical binding

We conclude this section with a discussion of notions of binding that we only apply to *classical* commitments (with possibly quantum adversaries).

▶ **Experiment 21** (Computational binding). *Given an adversary* Adv, *define* $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{bind}}(\lambda)$ *as follows.*

1. *Generate* $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. *Obtain* $(m_0, \omega_0, m_1, \omega_1) \leftarrow \mathsf{Adv}(\mathsf{ck})$.
3. *Output* 1 *if* $m_0 \neq m_1$ *and* $\mathsf{Commit}(\mathsf{ck}, m_0, \omega_0) = \mathsf{Commit}(\mathsf{ck}, m_1, \omega_1)$.

▶ **Definition 22.** *A commitment scheme* COM *is classically (resp. post-quantum) computationally binding if for all PPT (resp. QPT) adversaries* Adv *in Experiment 21,*

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

[6] Equivalently, we could drop the validity constraint by measuring the state obtained in Step 2 with the appropriate binary projective measurement and aborting unless the outcome is 1.

Somewhere statistical binding (SSB)

Finally, we recall the notion of somewhere statistical binding, introduced by [19] in the context of hash functions. Here we present the equivalent notion for commitments; note that this is different to the more sophisticated notion of SSB commitments given by [16].

▶ **Definition 23** (Somewhere statistical binding)**.** *Let ℓ be a polynomial in λ. 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* $\mathsf{ck} \in \operatorname{supp}\left(\mathsf{Gen}(1^\lambda, i)\right)$, *if* $\mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{Commit}(\mathsf{ck}, m', \omega')$ *for some (m, ω, m', ω'), then $m_i = m'_i$.*

More precisely, computational indistinguishability of $\mathsf{Gen}(\cdot, i)$ and $\mathsf{Gen}(\cdot, j)$ is defined by the experiment defined next.

▶ **Experiment 24.** *Given a commitment scheme* COM*, define* $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{ssb}}(\lambda)$ *as follows.*

1. *Sample $j \leftarrow [\ell(\lambda)]$ and generate* $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda, j)$.
2. *Obtain* $i \leftarrow \mathsf{Adv}(\mathsf{ck})$.
3. *Output 1 if $i = j$.*

Therefore, $(\mathsf{Gen}, \mathsf{Commit})$ is classically (resp. post-quantum) somewhere-statistically binding if for all non-uniform PPT (resp. QPT) adversaries Adv,

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

(And, in addition, commitment keys ck determine the i^{th} coordinate of messages that map to the same commitment string.)

5 Chosen-bit binding

We begin this section with the definition of our main conceptual tool: the notion of chosen-bit binding. We define this notion in generality, for quantum schemes (and, owing to Definition 15, for classical schemes as a special case). Recall that $\mathcal{S} \subseteq \mathcal{C} \otimes \mathcal{O}$ is the subregister checked in a quantum (de)commitment.

▶ **Experiment 25** (Chosen-bit binding)**.** *Given a commitment scheme* COM*, define* $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda)$ *as follows.*

1. *Sample* $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$.
2. *Obtain the index and commitment register pair $(i, \mathcal{C}) \leftarrow$* $\mathsf{Adv}(\mathsf{ck})$.[7]
3. *Sample $b \leftarrow \{0, 1\}$.*
4. *Obtain the message and opening register pair $(m, \mathcal{O}) \leftarrow$* $\mathsf{Adv}(b)$.
5. *Apply* $\mathsf{Commit}^\dagger_{\mathsf{ck},m}$ *to $\mathcal{C} \otimes \mathcal{O}$ and measure $\mathcal{S}$ in the computational basis.*
6. *Output 1 if $m_i = b$ and the measurement outcome is $|\mathbf{0}\rangle$.*

▶ **Definition 26.** *A quantum commitment scheme is chosen-bit binding if, for all non-uniform QPT adversaries* Adv *in Experiment 25,*

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

[7] Alternatively, $\mathsf{Adv}(\mathsf{ck})$ may output two quantum registers $(\mathcal{I}, \mathcal{C})$; then i is obtained by a computational basis measurement of $\mathcal{I}$. (An analogous observation holds for Step 4, with $(\mathcal{M}, \mathcal{O}) \leftarrow \mathsf{Adv}(b)$ and a measurement of $\mathcal{M}$.)

Note that, in the case of bit commitments (i.e., when $M = \{0,1\}$), this notion coincides with sum binding. Recall that, in the case of classical adversaries, we have:

▶ **Lemma 27.** *A (classical) commitment scheme is chosen-bit binding against classical adversaries if and only if it is computationally binding.*

(The proof of this lemma is straightforward and hence omitted.)

We now prove the first of our main results: an equivalence between chosen-bit binding and collapse binding. We will make extensive use of the following binary projective measurements associated with a quantum commitment scheme COM. With $\big(|m\rangle\big)_{m\in M}$ and $\big(|\omega\rangle\big)_{\omega}$ as bases for the registers $\mathcal{M}$ and $\mathcal{O}$, respectively, we define:
$\mathsf{M}_{\mathsf{ck},m} := (\Pi_{\mathsf{ck},m}, \mathbf{I} - \Pi_{\mathsf{ck},m})$ by

$$\Pi_{\mathsf{ck},m} := \mathsf{Commit}_{\mathsf{ck},m}\left(|\mathbf{0}\rangle\!\langle\mathbf{0}|^{\mathcal{S}} \otimes \mathbf{I}^{(\mathcal{C}\otimes\mathcal{O})\setminus\mathcal{S}}\right)\mathsf{Commit}^{\dagger}_{\mathsf{ck},m} \;\; ; \qquad (1)$$

$\mathsf{M}_{\mathsf{ck}} := (\Pi_{\mathsf{ck}}, \mathbf{I} - \Pi_{\mathsf{ck}})$ by

$$\Pi_{\mathsf{ck}} := \sum_{m\in M} |m\rangle\!\langle m|^{\mathcal{M}} \otimes \Pi_{\mathsf{ck},m} \;\; ; \qquad (2)$$

$\mathsf{M}_{i,b} := (\Pi_{i,b}, \mathbf{I} - \Pi_{i,b})$ by

$$\Pi_{i,b} := \sum_{m, m_i = b} |m\rangle\!\langle m|^{\mathcal{M}} \otimes \Pi_{\mathsf{ck},m} \;\; ; \text{ and} \qquad (3)$$

$\mathsf{M}_{i} := (\Pi_{i}, \mathbf{I} - \Pi_{i})$ by

$$\Pi_{i} := \sum_{b\in\{0,1\}} |b\rangle\!\langle b|^{\mathcal{B}} \otimes \Pi_{i,b} \;\; . \qquad (4)$$

Note that $\Pi_{\mathsf{ck},m}$ (Equation 2) projects onto the subspace of valid commitment-opening register pairs, and the other measurements do so with additional restrictions: $\Pi_{\mathsf{ck},m}$ (Equation 1) projects onto valid messages; $\Pi_{i,b}$ (Equation 3) projects onto (valid) messages with $m_i = b$; and Π_i (Equation 4) onto messages whose i^{th} coordinate overlaps with the contents of $\mathcal{B}$.

▶ **Theorem 28** (Theorem 4, restated)**.** *A quantum commitment scheme* COM *is collapse binding if and only if it is chosen-bit binding.*

We first prove (via the contrapositive) that collapse binding implies chosen-bit binding, which extends [23, Theorem 32] to quantum commitments.

Proof (collapsing ⇒ CBB). Let Adv be an adversary that achieves advantage ε in Experiment 25 (the chosen-bit binding experiment). We may assume, without loss of generality, that the adversary's action in Step 4 consists of the application of a unitary U on $\mathcal{B}\otimes\mathcal{M}\otimes\mathcal{O}\otimes\mathcal{H}$ (where $\mathcal{B}$ contains the bit received from the challenger and $\mathcal{H}$ is an additional workspace register) followed by a computational basis measurement of $\mathcal{M}$. We construct an adversary Adv' for the collapse binding experiment as follows.

- Upon receipt of ck:
  1. Run $\mathsf{Adv}(\mathsf{ck})$ to obtain $i \in [\ell]$ and state ρ on $\mathcal{C}\otimes\mathcal{M}\otimes\mathcal{O}\otimes\mathcal{H}$.
  2. Apply $U \otimes \mathbf{I}^{\mathcal{C}}$ to $\sigma = |+\rangle\!\langle+|^{\mathcal{B}} \otimes \rho$ followed by the binary projective measurement M_i.
  3. If the measurement outcome is 0, overwrite $\mathcal{C}\otimes\mathcal{M}\otimes\mathcal{O}$ with a valid commitment (to, say, the all-zero string). Output $i \in [\ell]$ along with the registers $\mathcal{C}$, $\mathcal{M}$ and $\mathcal{O}$.

- Upon receipt of $\mathcal{M}$, $\mathcal{O}$:
  1. If the measurement outcome in the previous step was 0, stop and output a random bit.
  2. Apply $U^\dagger$ to $\mathcal{B} \otimes \mathcal{M} \otimes \mathcal{O} \otimes \mathcal{H}$ and measure $\mathcal{B}$ in the $\{|+\rangle, |-\rangle\}$ basis.
  3. If the outcome is $|+\rangle$, output 0; otherwise output 1.

Note that Adv' is valid, as $\Pi_{\mathsf{ck}} = \Pi_{i,0} + \Pi_{i,1}$ (by Equations 2 and 3) and Equation 4 implies $\mathrm{Tr}_{\mathcal{B},\mathcal{H}}(\Pi_i \sigma \Pi_i) \in \mathrm{Im}(\Pi_{i,0} + \Pi_{i,1})$. Moreover, if either (i) the challenger measures or (ii) the outcome of the first measurement by Adv' is 0, the experiment outputs a uniformly random bit.

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

▶ **Proposition 29.** *Let P, Q be projectors and ρ a density matrix such that $\rho Q = \rho$. Then*

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

Proof. $\mathrm{Tr}(P\rho) = \mathrm{Tr}(P\rho Q) \leq \sqrt{\mathrm{Tr}(QP\rho PQ)}$, by Cauchy-Schwarz (Lemma 13). ◀

Assume that $b = 0$ in Step 3 of Experiment 19, so $\mathcal{M}$ is not measured (we deal with the case $b = 1$ next). We lower bound the probability that the measurement outcomes of $\mathsf{Adv}'(\mathsf{ck})$ and $\mathsf{Adv}'(\mathcal{M}, \mathcal{O})$ are 1 and $|+\rangle$, respectively, whereupon the experiment outputs 1: since $\sigma \cdot |+\rangle\langle+| = \sigma$, by Proposition 29,

$$\begin{aligned}\mathrm{Tr}\left(|+\rangle\langle+|\, \Pi_i \sigma \Pi_i\right) &\geq \mathrm{Tr}(\Pi_i \sigma)^2 \\ &= \left(\frac{1}{2}\mathrm{Tr}\left(\Pi_{i,0}\rho\right) + \frac{1}{2}\mathrm{Tr}\left(\Pi_{i,1}\rho\right)\right)^2 \\ &= \left(\frac{1}{2} + \varepsilon\right)^2 .\end{aligned}$$

Now note that, if $b = 1$ in Step 3, the $\mathcal{M}$ register is measured and $\mathcal{B}$ collapses to a computational basis state, namely, $|m_i\rangle$ when the outcome is m; since the adversary measures $\mathcal{B}$ in the Hadamard basis, the experiment outputs 1 with (conditional) probability 1/2 in this event. Moreover, if the adversary's first measurement outcome is 0 (an event with $1 - \mathrm{Tr}(\Pi_i\sigma)$ probability) it outputs a uniformly random bit; in this case, Experiment 19 also outputs 1 with probability 1/2.

Overall, the probability that the experiment outputs 1 is thus

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

Before proving the reverse implication, we show a basic fact about non-commuting projective measurements. Let M be a projective measurement and $\mathsf{B} = (D, \mathbf{I} - D)$ 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 following 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 [30, 9].

▷ Claim 30. Let D be a projector, $\mathsf{M} = (\Pi_i)_{i\in[N]}$ be a projective submeasurement and ρ be a Hermitian matrix such that $\sum_i \mathrm{Tr}(\Pi_i\rho) = \mathrm{Tr}(\rho)$. Then

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

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

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

where $\Pi_{\neq j} := \sum_{i\neq j} \Pi_i$. Applying Cauchy-Schwarz (Lemma 13, with $A = \sqrt{\rho}\cdot\Pi_j D\Pi_{\neq j}$ and $B = \sqrt{\rho}$) yields $|\mathrm{Tr}(\Pi_{\neq j} D\Pi_j\rho)| \leq \sqrt{\mathrm{Tr}(\Pi_{\neq j} D\Pi_j\rho\Pi_j D)}\sqrt{\mathrm{Tr}(\rho)}$. Substituting into the above equation and squaring we have

$$\frac{\mathrm{Tr}\left(D(\rho - \mathsf{M}(\rho))\right)^2}{\mathrm{Tr}(\rho)} \leq \left(\sum_j \sqrt{\mathrm{Tr}(\Pi_{\neq j} D\Pi_j\rho\Pi_j D)}\right)^2 \ ,$$

and applying Cauchy-Schwarz again (with respect to Euclidean norm and the N-dimensional pair of vectors with 1 and $\sqrt{\mathrm{Tr}(\Pi_{\neq j} D\Pi_j\rho\Pi_j D)}$ in the j^{th} coordinate, respectively) 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 experiment as follows.

- Upon receipt of ck:
  1. Run $\mathsf{Adv}(\mathsf{ck})$ obtain a quantum state ρ in $\mathcal{C}\otimes\mathcal{M}\otimes\mathcal{O}\otimes\mathcal{H}$.
  2. Output a random index $i \leftarrow [\ell]$ and $\mathcal{C}$.
- Upon receipt of b:
  1. Measure the first i bits of $\mathcal{M}$, obtaining outcomes $b_1,\dots,b_i$.
  2. If $b_i \neq b$, apply Adv's (projective) distinguishing measurement $(D, \mathbf{I}-D)$ to $\mathcal{M}\otimes\mathcal{O}\otimes\mathcal{H}$.[8]
  3. Measure $\mathcal{M}$ in the computational basis. Output the outcome m and the opening register $\mathcal{O}$.[9]

Let $\mathsf{M}_j(\rho)$ be the map corresponding to measuring the j^{th} qubit of $\mathcal{M}$, i.e.,

$$\mathsf{M}_j(\rho) = \Pi_i\rho\Pi_i + (\mathbf{I} - \Pi_i)\rho(\mathbf{I} - \Pi_i).$$

[8] Here we use that D acts trivially on $\mathcal{C}$.

[9] Note that in the case of classical commitments, $\mathcal{O}$ is a classical register containing an opening string ω; equivalently, we may assume $\mathcal{O}$ is implicitly measured.

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

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

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

The adversary's success probability γ in Experiment 25 can be written as

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

Note that the validity of Adv ensures ρ_{i-1} is in the span of Π_{ck}, which simplifies the first term of the sum: $\sum_{i\in[\ell]}\sum_{b\in\{0,1\}} \operatorname{Tr}(\Pi_{i,b}\rho_{i-1}) = \sum_{i\in[\ell]} \operatorname{Tr}(\rho_{i-1}) = \ell$. It also enables us to apply Claim 30 with respect to the submeasurement $(\Pi_{i,0}, \Pi_{i,1})$; using the claim and Cauchy-Schwarz (Lemma 13), we obtain that

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

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

5.1 Somewhere statistical binding and parallel repetitions

Using chosen-bit binding, we give "fully classical" proofs that somewhere-statistical binding commitments are collapse binding, and that the parallel repetition of collapse binding commitments are collapse binding.

▶ **Lemma 31.** *Post-quantum somewhere statistically binding commitment schemes are chosen-bit binding against quantum adversaries, and therefore collapse binding.*

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 $\mathsf{Adv}'(\mathsf{ck})$ for Experiment 24 (SSB) as follows: simulate Experiment 25 (CBB) with the key ck, obtaining $(\mathsf{com}, i, b, m, \omega)$. (Recall that Experiment 24 is classical, so Adv outputs strings com and ω.) 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 (which determines $\mathsf{Gen}(1^\lambda, j)$ as the generator in the experiment).

The success probability of this adversary is

$$\Pr[k = j] = \frac{1}{\ell} \cdot \Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 0\right] + \frac{1}{\ell - 1} \cdot \Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1 \wedge j \neq i\right] \quad . \tag{5}$$

Observe that the experiment outputs 1 with probability at most 1/2 when conditioned on $j = i$ (since, by Definition 23, one of the choices for $b \in \{0, 1\}$ is such that no message-opening pair

(m, ω) with $\mathsf{Commit}(\mathsf{ck}, m, \omega) = \mathsf{com}$ and $m_i = b$ exists); that is, $\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1 \,\middle|\, j = i\right] \le 1/2$. Hence

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

Note that, if $\Pr[j = i] \ge (1 + \varepsilon)/\ell$ (infinitely often), the adversary that always outputs i has inverse polynomial advantage. We therefore assume otherwise; then

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

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

Substituting into (5) and using $\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 0\right] = 1/2 - \varepsilon$ (by hypothesis) yields

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

which completes the proof. ◀

Observe that Theorem 28 implies that parallel repetitions preserve collapse binding if and only if they preserve chosen-bit binding. Then,

▶ **Proposition 32.** *If a quantum commitment scheme* $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ *is chosen-bit binding, then its k-fold parallel repetition is also chosen-bit binding.*

Proof. Let Adv be an adversary satisfying $\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{cbb}}(\lambda) = 1\right] = 1/2 + \varepsilon$ in the k-wise parallel repetition of Experiment 25. (Recall that the same key ck is used in each repetition; we index message bits by pairs $(i, j) \in [k] \times [\ell]$, so that m_{ij} is the j^{th} bit of the i^{th} message.)

Then an adversary $\mathsf{Adv}'(\mathsf{ck})$ for the original commitment scheme, with the same advantage, simply executes $\mathsf{Adv}(\mathsf{ck})$ to obtain an index (i, j) along with commit registers $\mathcal{C}_1 \otimes \ldots \otimes \mathcal{C}_k$, and outputs $(j, \mathcal{C}_i)$; upon receipt of b, it obtains $(m_1, \ldots, m_k, \mathcal{O}_1 \otimes \cdots \otimes \mathcal{O}_k) \leftarrow \mathsf{Adv}(b)$ and returns $(m_i, \mathcal{O}_i)$ in the last step.

Since $m_{ij} = (m_i)_j = b$ and applying $\mathsf{Commit}^{\dagger}_{\mathsf{ck}, m_i}(\mathcal{C}_i, \mathcal{O}_i)$ followed by a measurement of $\mathcal{S}_i$ yields $|\mathbf{0}\rangle$ with probability at least $1/2 + \varepsilon$ (because applying $\mathsf{Commit}^{\dagger}_{\mathsf{ck}, m_1} \otimes \cdots \otimes \mathsf{Commit}^{\dagger}_{\mathsf{ck}, m_k}$ to $(\mathcal{C}_1 \otimes \mathcal{O}_1) \otimes \cdots \otimes (\mathcal{C}_k \otimes \mathcal{O}_k)$ and measuring $\mathcal{S}_1 \otimes \cdots \otimes \mathcal{S}_k$ yields $|\mathbf{0}\rangle$ with probability $1/2 + \varepsilon$), the result follows. ◀

6 Equivocality

Amos, Georgiou, Kiayias and Zhandry [2] define two closely related notions they call *equivocal* and *one-shot chameleon* collision-resistant hash functions, and show how they can be used to obtain a variety of interesting quantum cryptographic constructions. Here we consider a slight variant, which we call a *one-shot equivocal commitment scheme.* We note that an equivocal CRHF associated to a predicate p is a one-shot equivocal commitment to the bit $p(x)$ where x is the hash preimage.[10]

[10] While [2] distinguish between the notions of equivocal and one-shot chameleon hash functions (roughly speaking, equivocal hashes allow equivocation to *some* string under a predicate constraint, while one-shot chameleon hashes equivocate to *any* string), they also prove how to construct one from the other. We choose to only define the (syntactically) stronger property, which we call *one-shot equivocality* – both to distinguish it from classical notions of equivocality and to evince the connection to one-shot chameleon hashes.

▶ **Definition 33.** *A commitment scheme* $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ *is* one-shot equivocal *if there exists a stateful QPT algorithm* Eq *such that for all messages* $m \in M$*,*

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

While this definition allows arbitrary message spaces, hereafter we focus on the case $M = \{0,1\}$. We also note that Definition 18 (sum binding) is identical to a "converse" notion to the above, which [2] define informally and call *unequivocality.*

▶ Remark 34. Despite what the terminology may suggest, we stress that (one-shot) equivocality and unequivocality (i.e., sum binding) 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.

It is claimed in [2] that an adversary breaking unequivocality yields a one-shot 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 an 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!

Regardless, we show in Theorem 41 that the implication still holds: sum binding can be "boosted" to one-shot equivocality via quantum rewinding. ⌟

One-shot equivocal commitments only differ from equivocal hashes in their mildly weaker "collision-resistance", which does not prevent an adversary from efficiently finding distinct valid openings for the same message. However, we remark that the construction of one-shot signatures of [2] can be based on one-shot equivocal commitments rather than hashes without harm to their security: while an adversary may find distinct signatures for the same message, the resulting scheme still ensures it *cannot sign distinct messages.* (As a result, subsequent constructions that rely on one-shot signatures – quantum money and proofs of quantumness, among others – also satisfy this weakened but sufficient security guarantee.)

Nontrivial (i.e., computationally binding) one-shot equivocal string commitments can be obtained from one-shot equivocal bit commitments by the usual composition, which we prove next for completeness.

▶ **Proposition 35.** *If a bit commitment scheme* $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ *is computationally binding and one-shot equivocal, then its k-fold parallel repetition is also computationally binding and one-shot equivocal when* $k = \mathrm{poly}(\lambda)$*.*

Proof. Computational binding follows from the fact that an adversary Adv in the parallel repetition of Experiment 21 achieving $\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{bind}}(\lambda)\right] = \varepsilon$ with message space $M = \{0,1\}^k$ immediately yields Adv' with advantage ε/k when $M = \{0,1\}$: Adv' samples $i \leftarrow [k]$, runs the (bit) experiment with the challenger on this coordinate and simulates the interaction for coordinates $j \neq i$. When $\varepsilon = \mathrm{poly}\left(\lambda^{-1}\right)$, the resulting advantage ε/k is also inverse polynomial.

If Eq with quantum auxiliary input ρ is the equivocator for COM, we define Eq' as the natural equivocator for the parallel repetition: $\mathsf{Eq}'(\mathsf{ck})$, with auxiliary input $\rho^{\otimes k}$, obtains from each copy of ρ a commitment string $\mathsf{com}_i \leftarrow \mathsf{Eq}(\mathsf{ck})$ and a post-measurement state ρ_i, then returns $(\mathsf{com}_1, \ldots, \mathsf{com}_k)$. Upon receipt of a message, $\mathsf{Eq}'(m)$ runs each $\mathsf{Eq}(m_i)$ on the state ρ_i, obtains ω_i and returns $(\omega_1, \ldots, \omega_k)$. Since $\mathsf{Commit}(\mathsf{ck}, m_i, \omega_i) = \mathsf{com}_i$ with probability $1 - \mathsf{negl}(\lambda)$ for each i, all k openings succeed except with probability $k \cdot \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda)$. ◀

We will show via quantum rewinding techniques that a commitment scheme that is computationally but not sum binding is indeed one-shot equivocal. To this end, we first recall an early "basic quantum rewinding" lemma, first used in [13], which shows that when two different computations (on the same state) yield prescribed outcomes with sufficiently high probability, performing the computations sequentially obtains both outcomes with non-negligible probability. We state a slightly more general statement than [13] and prove it for completeness.

▶ **Lemma 36.** *For any projectors P, Q and quantum state ρ it holds that*

$$\operatorname{Tr}(PQP\rho) \geq \frac{1}{4}\big(\operatorname{Tr}(P\rho) + \operatorname{Tr}(Q\rho) - 1\big)^2 \ .$$

Proof. Let $\varepsilon := \operatorname{Tr}(P\rho) + \operatorname{Tr}(Q\rho) - 1$. Then $\operatorname{Tr}((P+Q)\rho) = 1 + \varepsilon$ by assumption and linearity, and, by Cauchy-Schwarz,

$$\begin{aligned}(1+\varepsilon)^2 = \operatorname{Tr}\big((P+Q)\rho\big)^2 &\leq \operatorname{Tr}\big((P+Q)\rho(P+Q)\big) \\ &= \operatorname{Tr}(P\rho) + \operatorname{Tr}(Q\rho) + 2\operatorname{Re}\operatorname{Tr}(QP\rho) \ .\end{aligned}$$

It follows that $\operatorname{Re}\operatorname{Tr}(QP\rho) \geq \varepsilon/2$. Then, again by Cauchy-Schwarz (Lemma 13),

$$\varepsilon/2 \leq \operatorname{Re}\operatorname{Tr}(QP\rho) \leq |\operatorname{Tr}(QP\rho)| \leq \sqrt{\operatorname{Tr}(QP\rho PQ)} \ ,$$

which completes the proof. ◀

Next, we recall Jordan decompositions and two singular vector algorithms that we shall use in our construction.

▶ **Lemma 37** (Jordan decomposition). *Any pair of projectors Π_A and Π_B induces a decomposition of the Hilbert space they act upon into $\oplus_i \mathcal{S}_i$ where each $\mathcal{S}_i$ has dimension 1 or 2.*

The projectors can be written as $\Pi_A = \sum_i |v_i\rangle\langle v_i|$ and $\Pi_B = \sum_i |w_i\rangle\langle w_i|$ for $\mathcal{S}_i$-bases $\{|v_i\rangle, |v_i^\perp\rangle\}$ and $\{|v_i\rangle, |v_i^\perp\rangle\}$; the sums range over all $\mathcal{S}_i$ except the one-dimensional ones where the projector acts trivially (as the zero projector).

We call the $\mathcal{S}_i$ *Jordan subspaces*, and define $p_i := |\langle v_i|w_i\rangle|^2 = |\langle v_i^\perp|w_i^\perp\rangle|^2$. We also define the *Jordan measurement* $\mathsf{M}^{\mathsf{Jor}} = (\Pi_i^{\mathsf{Jor}})$ by

$$\Pi_i^{\mathsf{Jor}} := |v_i\rangle\langle v_i| + |v_i^\perp\rangle\langle v_i^\perp| = |w_i\rangle\langle w_i| + |w_i^\perp\rangle\langle w_i^\perp|;$$

that is, $\mathsf{M}^{\mathsf{Jor}}$ projects onto a subspace $\mathcal{S}_i$ and outputs its index i.

The singular vector algorithms, due to [21, 18], allow us to effectively "filter out" components of a quantum state below a threshold of our choice and then "flip" the image of a projector to its complement if needed.

▶ **Lemma 38.** *Let Π_A, Π_B be projectors described by uniform $\operatorname{poly}(\lambda)$-size quantum circuits. Then there exists a (uniform) family $\{\mathsf{Threshold}_\theta\}_{\theta \in (0,1]}$ of algorithms described by $\operatorname{poly}(\lambda)$-size circuits that satisfy the following:*

- *if $p_i \geq \theta$, $\mathsf{Threshold}_\theta(|v_i\rangle)$ outputs 1 with probability $1 - \mathsf{negl}(\lambda)$.*
- *if $p_i \leq \theta/2$, $\mathsf{Threshold}_\theta(|v_i\rangle)$ outputs 1 with probability $\mathsf{negl}(\lambda)$.*

Moreover, $\mathcal{S}_i$ is invariant under $\mathsf{Threshold}_\theta$ for all i and θ, and the post-measurement state is $|v_i\rangle$ when the measurement outputs 1.

▶ **Lemma 39.** *Let Π_A, Π_B be projectors described by uniform $\operatorname{poly}(\lambda)$-size quantum circuits. Then there exists a (uniform) family of circuits $\{\mathsf{Transform}_\gamma\}_{\gamma \in (0,1]}$ of size $\operatorname{poly}(\lambda)/\sqrt{\gamma}$ such that, when $p_i \geq \gamma$, the output (i.e., post-measurement state) of $\mathsf{Transform}(|v_i\rangle)$ is $|w_i\rangle$ with probability $1 - \mathsf{negl}(\lambda)$.*

Moreover, $\mathcal{S}_i$ is invariant under $\mathsf{Transform}_\gamma$ for all i and γ.

We are now ready to show that (almost-everywhere) non-unequivocality implies one-shot equivocality. Our one-shot equivocal commitment scheme is constructed as follows.

▶ **Construction 40.** *Let $\mathsf{COM} = (\mathsf{Gen}, \mathsf{Commit})$ be a bit commitment scheme. For $k \in \mathbb{N}$, we construct COM^k by:*

- *$\mathsf{Gen}^k(1^\lambda)$ runs $\mathsf{ck}_i \leftarrow \mathsf{Gen}(1^\lambda)$ for each $i \in [k]$ and outputs $\mathsf{ck} := (\mathsf{ck}_1, \ldots, \mathsf{ck}_k)$.*
- *$\mathsf{Commit}^k\big((\mathsf{ck}_1, \ldots, \mathsf{ck}_k), m, (i, \omega)\big) := \big(i, \mathsf{Commit}(\mathsf{ck}_i, m, \omega)\big)$.*

Let Adv be an adversary for $\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{sum}}$ with quantum auxiliary input ρ, which applies the projector Π_b and measures the opening register $\mathcal{O}$ when asked to open to bit b. We construct an equivocator Eq, whose auxiliary input consists of k copies of ρ on registers $\mathcal{A}_1, \ldots, \mathcal{A}_k$, as follows.

```
- $\mathsf{Eq}^{\mathsf{Adv}}_\varepsilon(\mathsf{ck}_1, \ldots, \mathsf{ck}_k; \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_k)$:
  1. For each $j \in [k]$:
     a. Run $\mathsf{com}_j \leftarrow \mathsf{Adv}(\mathsf{ck}_j; \mathcal{A}_j)$.
     b. Apply the measurement $(\Pi_0, \mathbf{I} - \Pi_0)$ followed by $\mathsf{Threshold}_{\varepsilon^2/2}$ to $\mathcal{A}_j$.
        If both outcomes are 1, set $j^* := j$ and skip to Step 3.
  2. If $j^*$ is unset, output $\perp$.
  3. Output $(j^*, \mathsf{com}_{j^*})$ as the commitment. (At this point we can discard $\mathcal{A}_j$ for $j \neq j^*$.)
- $\mathsf{Eq}^{\mathsf{Adv}}_\varepsilon(b; \mathcal{A}_{j^*})$:
  1. If $b = 1$, apply $\mathsf{Transform}_{\varepsilon^2/4}$ followed by the measurement $(\Pi_1, \mathbf{I} - \Pi_1)$ to $\mathcal{A}_{j^*}$.
  2. Measure the opening register $\mathcal{O} \subset \mathcal{A}_{j^*}$, obtaining outcome $\omega$, and output $(j^*, \omega)$.
```

Note that $\mathsf{COM}^k = (\mathsf{Gen}^k, \mathsf{Commit}^k)$ is not the k-wise parallel repetition of COM (as decommitting a single coordinate suffices).

▶ **Theorem 41.** *Let $\varepsilon = \varepsilon(\lambda)$ be an inverse polynomial, and let COM be a bit commitment scheme such that $\Pr\left[\mathsf{Exp}^{\mathsf{Adv}}_{\mathsf{sum}}(\lambda) = 1\right] = 1/2 + \varepsilon$ for some QPT adversary Adv and all sufficiently large λ (i.e., that violates sum binding almost everywhere). Then, with $k = \lambda/\varepsilon^2$, the commitment scheme COM^k of Construction 40 is one-shot equivocal.*

Proof. First, note that the running time of Eq is $\operatorname{poly}(\lambda)$, as it executes the QPT algorithm Adv (at most) $k = \operatorname{poly}(\lambda)$ times; $\mathsf{Threshold}$ (which is QPT regardless of the parameter) once; and $\mathsf{Transform}$ (with a $\operatorname{poly}(\lambda^{-1})$ parameter, in which case it is QPT) at most once.

For each j, denote by ρ_j the post-measurement state after Step 1a (where the mixture ρ_j includes the distribution over ck_j as well as the measurement that outputs com_j). By assumption, we have

$$\operatorname{Tr}\big((\Pi_0 + \Pi_1)\rho_j\big) \geq 1 + 2\varepsilon.$$

Hence, by Lemma 36,

$$\mathrm{Tr}\left(\Pi_0\Pi_1\Pi_0\rho_j\right) \geq \varepsilon^2 \ .$$

Now, consider the distribution obtained by applying $(\Pi_0, \mathbf{I} - \Pi_0)$ followed by the Jordan measurement $\mathsf{M}^{\mathsf{Jor}}$ (with respect to the pair of projectors Π_0, Π_1), obtaining outcomes (b, i) and outputting $b \cdot p_i$. Then

$$\begin{aligned}
\mathbb{E}\left[b \cdot p_i\right] &= \sum_i p_i \cdot \mathrm{Tr}\left(\Pi_i^{\mathsf{Jor}}\Pi_0\rho_j\Pi_0\right) \\
&= \mathrm{Tr}\left(\left(\sum_i p_i\Pi_0\Pi_i^{\mathsf{Jor}}\Pi_0\right)\rho_j\right) \\
&= \mathrm{Tr}\left(\left(\sum_i p_i\left|v_i\middle\rangle\middle\langle v_i\right|\right)\rho_j\right) \\
&= \mathrm{Tr}\left(\left(\sum_i \left|v_i\middle\rangle\middle\langle v_i\right|\right)\left(\sum_i \left|w_i\middle\rangle\middle\langle w_i\right|\right)\left(\sum_i \left|v_i\middle\rangle\middle\langle v_i\right|\right)\rho_j\right) \\
&= \mathrm{Tr}\left(\Pi_0\Pi_1\Pi_0\rho_j\right) \\
&\geq \varepsilon^2
\end{aligned}$$

where the second-to-last equality uses $p_i = \left|\langle v_i|w_i\rangle\right|^2$.

Therefore, the probability that Step 1b of $\mathsf{Eq}_\varepsilon^{\mathsf{Adv}}(\mathsf{ck}_1, \ldots, \mathsf{ck}_k)$ sets j^* to j (which is unchanged by the Jordan measurement, since $\mathsf{M}^{\mathsf{Jor}}$ commutes with $\mathsf{Threshold}$ and Π_0) is

$$\begin{aligned}
\Pr\left[b \cdot p_i \geq \frac{\varepsilon^2}{2} \text{ and } \mathsf{Threshold}_{\varepsilon^2/2}(|v_i\rangle) \text{ outputs } 1\right] &\geq \left(1 - 2^{-\lambda}\right) \cdot \Pr\left[b \cdot p_i \geq \frac{\varepsilon^2}{2}\right] \\
&\geq \left(1 - 2^{-\lambda}\right) \cdot \frac{\varepsilon^2}{2},
\end{aligned}$$

by Lemma 38 and Proposition 11.

By the Chernoff bound (Proposition 12), the probability j^* is left unset in all $j \in [k]$ (causing $\mathsf{Eq} = \mathsf{Eq}_\varepsilon^{\mathsf{Adv}}$ on input $(\mathsf{ck}_1, \ldots, \mathsf{ck}_k)$ to abort in Step 2) is at most $e^{-\Omega(\lambda)} = \mathsf{negl}(\lambda)$.

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 $(\Pi_b, \mathbf{I} - \Pi_b)$ is the projective measurement corresponding to the whether Adv wins the sum binding experiment when the challenge is b (that is, Π_b projects onto the subspace spanned by $|\mathsf{ck}, b, \omega\rangle$ such that $\mathsf{Commit}(\mathsf{ck}, b, \omega) = \mathsf{com}$). Then, if $b = 0$, the output of Step 2 of $\mathsf{Eq}(0)$ is a correct opening (with probability 1), since the post-measurement state of Step 3 of $\mathsf{Eq}(\mathsf{ck}_1, \ldots, \mathsf{ck}_k)$ is contained in $\mathrm{Im}(\Pi_0)$; we thus only need to argue that the measurement $(\Pi_1, \mathbf{I} - \Pi_1)$ in Step 1 of $\mathsf{Eq}(1)$ outputs 1 except with probability $\mathsf{negl}(\lambda)$.

For a fixed $j \in [k]$, consider the distribution of (binary) outcomes that arises from applying the measurements $\mathsf{Threshold}_{\varepsilon^2/2}$, $\mathsf{Transform}_{\varepsilon^2/4}$ and $(\Pi_1, \mathbf{I} - \Pi_1)$ in this order to an arbitrary quantum state in $\mathrm{Im}(\Pi_0)$. Note that it suffices to show that the first output is 1 and the last is 0 with probability $\mathsf{negl}(\lambda)$, as this ensures (by a union bound over j) that the probability $\mathsf{Eq}(1)$ fails to return a valid opening remains negligible.

By commutativity of the Jordan measurement with $\mathsf{Threshold}$ and $\mathsf{Transform}$ (and Π_1; recall that every $\mathcal{S}_i$ is invariant under all three), the distribution is identical to that which arises by applying $\mathsf{M}^{\mathsf{Jor}}$ before $\mathsf{Threshold}_{\varepsilon^2/2}$. We now analyse two cases: (i) when $\mathsf{M}^{\mathsf{Jor}}$ outputs i such that $p_i \leq \varepsilon^2/4$, and (ii) when $p_i > \varepsilon^2/4$. (Note that the post-measurement outcome is $|v_i\rangle$ in both cases, as the sequence of measurements is applied to a state in $\mathrm{Im}(\Pi_0)$.)

In case (i), Lemma 38 immediately implies that the outcome of $\mathsf{Threshold}_{\varepsilon^2/2}$ is 1 with probability $\mathsf{negl}(\lambda)$. In case (ii), while Lemma 38 does not allow us to analyse the distribution of $\mathsf{Threshold}_{\varepsilon^2/2}$ (when $\varepsilon^2/4 < p_i < \varepsilon^2/2$), it ensures that *conditioned on outcome* 1 the post-measurement state remains unchanged; then Lemma 39 implies the output of $\mathsf{Transform}_{\varepsilon^2/4}(|v_i\rangle)$ is $|w_i\rangle$ with probability $1 - \mathsf{negl}(\lambda)$, in which case the $(\Pi_1, \mathbf{I} - \Pi_1)$ measurement always outputs 1.

The probability $\mathsf{Threshold}_{\varepsilon^2/2}$ outputs 1 *and* $(\Pi_1, \mathbf{I} - \Pi_1)$ outputs 0 is thus $\mathsf{negl}(\lambda)$ in either case, which concludes the proof. ◀

References

1 Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 474–483. IEEE Computer Society, 2014. doi:10.1109/FOCS.2014.57. 2

2 Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 255–268. ACM, 2020. doi:10.1145/3357713.3384304. 5, 6, 15, 16

3 Prabhanjan Ananth, Kai-Min Chung, and Rolando L. La Placa. On the concurrent composition of quantum zero-knowledge. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 346–374. Springer, 2021. doi:10.1007/978-3-030-84242-0_13. 2

4 Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 208–236. Springer, 2022. doi:10.1007/978-3-031-15802-5_8. 2

5 Nir Bitansky and Zvika Brakerski. Classical binding for quantum commitments. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I*, volume 13042 of *Lecture Notes in Computer Science*, pages 273–298. Springer, 2021. doi:10.1007/978-3-030-90459-3_10. 2, 4

6 Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011. doi:10.1007/978-3-642-25385-0_3. 1

7 Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 592–608. Springer, 2013. doi:10.1007/978-3-642-38348-9_35. 1

8 Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 361–379. Springer, 2013. doi:10.1007/978-3-642-40084-1_21. 1

9 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. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, volume 13509 of *Lecture Notes in Computer Science*, pages 564–595. Springer, 2022. doi:10.1007/978-3-031-15982-4_19. 2, 13

10 Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa. A black-box approach to post-quantum zero-knowledge in constant rounds. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 315–345. Springer, 2021. doi:10.1007/978-3-030-84242-0_12. 2

11 Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry. Post-quantum succinct arguments: Breaking the quantum rewinding barrier. In *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*, pages 49–58. IEEE, 2021. doi:10.1109/FOCS52979.2021.00014. 2, 6, 7

12 Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail. Computational collapse of quantum state with application to oblivious transfer. In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 374–393. Springer, 2004. doi:10.1007/978-3-540-24638-1_21. 4

13 Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two provers in isolation. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 407–430. Springer, 2011. doi:10.1007/978-3-642-25385-0_22. 6, 17

14 Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 300–315. Springer, 2000. doi:10.1007/3-540-45539-6_21. 2

15 Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou. How to base security on the perfect/statistical binding property of quantum bit commitment? In Sang Won Bae and Heejin Park, editors, *33rd International Symposium on Algorithms and Computation, ISAAC 2022, December 19-21, 2022, Seoul, Korea*, volume 248 of *LIPIcs*, pages 26:1–26:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPIcs.ISAAC.2022.26. 2, 4

16 Prastudy Fauzi, Helger Lipmaa, Zaira Pindado, and Janno Siim. Somewhere statistically binding commitment schemes with applications. In Nikita Borisov and Claudia Díaz, editors, *Financial Cryptography and Data Security - 25th International Conference, FC 2021, Virtual Event, March 1-5, 2021, Revised Selected Papers, Part I*, volume 12674 of *Lecture Notes in Computer Science*, pages 436–456. Springer, 2021. doi:10.1007/978-3-662-64322-8_21. 10

17 Sumegha Garg, Henry Yuen, and Mark Zhandry. New security notions and feasibility results for authentication of quantum data. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 342–371. Springer, 2017. doi:10.1007/978-3-319-63715-0_12. 1

18 András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In Moses Charikar and Edith Cohen, editors, *Proceedings of the 51st Annual ACM SIGACT*

Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019, pages 193–204. ACM, 2019. doi:10.1145/3313276.3316366. 17

19 Pavel Hubácek and Daniel Wichs. On the communication complexity of secure function evaluation with long output. In Tim Roughgarden, editor, *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ITCS 2015, Rehovot, Israel, January 11-13, 2015*, pages 163–172. ACM, 2015. doi:10.1145/2688073.2688105. 10

20 Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat-Shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 326–355. Springer, 2019. doi:10.1007/978-3-030-26951-7_12. 2

21 Alex Lombardi, Fermi Ma, and Nicholas Spooner. Post-quantum zero knowledge, revisited or: How to do quantum rewinding undetectably. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 851–859. IEEE, 2022. doi:10.1109/FOCS54457.2022.00086. 2, 3, 6, 17

22 Dominique Unruh. Quantum proofs of knowledge. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 135–152. Springer, 2012. doi:10.1007/978-3-642-29011-4_10. 6

23 Dominique Unruh. Collapse-binding quantum commitments without random oracles. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 166–195, 2016. doi:10.1007/978-3-662-53890-6_6. 2, 4, 11

24 Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 497–527. Springer, 2016. doi:10.1007/978-3-662-49896-5_18. 2, 4, 5, 7, 9

25 Jun Yan. Quantum computationally predicate-binding commitments with application in quantum zero-knowledge arguments for NP. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I*, volume 13090 of *Lecture Notes in Computer Science*, pages 575–605. Springer, 2021. doi:10.1007/978-3-030-92062-3_20. 4

26 Jun Yan. General properties of quantum bit commitments (extended abstract). In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV*, volume 13794 of *Lecture Notes in Computer Science*, pages 628–657. Springer, 2022. doi:10.1007/978-3-031-22972-5_22. 4

27 Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In Khaled M. Elbassioni and Kazuhisa Makino, editors, *Algorithms and Computation - 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings*, volume 9472 of *Lecture Notes in Computer Science*, pages 555–565. Springer, 2015. doi:10.1007/978-3-662-48971-0_47. 2

28 Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany,*

May 19-23, 2019, Proceedings, Part III, volume 11478 of *Lecture Notes in Computer Science*, pages 408–438. Springer, 2019. doi:10.1007/978-3-030-17659-4_14. 2, 6

29 Mark Zhandry. Quantum lightning never strikes the same state twice. Or: Quantum money from cryptographic assumptions. *J. Cryptol.*, 34(1):6, 2021. doi:10.1007/s00145-020-09372-x. 2, 6

30 Mark Zhandry. New constructions of collapsing hashes. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, volume 13509 of *Lecture Notes in Computer Science*, pages 596–624. Springer, 2022. doi:10.1007/978-3-031-15982-4_20. 2, 13