Classical Binding for Quantum Commitments

Nir Bitansky* Zvika Brakerski†

Abstract

In classical commitments, statistical binding means that for almost any commitment transcript there is at most one possible opening. While quantum commitments (for classical messages) sometimes have benefits over their classical counterparts (e.g. in terms of assumptions), they provide a weaker notion of binding. Essentially that the sender cannot open a given commitment to a random value with probability noticeably greater than 1/2.

We introduce a notion of *classical binding for quantum commitments* which provides guarantees analogous to the classical case. In our notion, the receiver performs a (partial) measurement of the quantum commitment string, and the outcome of this measurement determines a single value that the sender may open. We expect that our notion can replace classical commitments in various settings, leaving the security proof essentially unchanged. As an example we show a soundness proof for the GMW zero-knowledge proof system.

We construct a non-interactive quantum commitment scheme which is classically statistically-binding and has a classical opening, based on the existence of *any* post-quantum one-way function. Prior candidates had inherently quantum openings and were not classically binding. In contrast, we show that it is *impossible* to achieve classical binding for statistically hiding commitments, regardless of assumption or round complexity.

Our scheme is simply Naor's commitment scheme (which classically requires a common random string, CRS), but executed in superposition over all possible values of the CRS, and repeated several times. We hope that this technique for using quantum communication to remove a CRS may find other uses.

1 Introduction

Commitment schemes [Blu81] are one of the most basic cryptographic primitives, and can be viewed as a digital analog of a locked box. They involve two parties: a sender (committer) and a receiver, that interact in two phases: commit and reveal. After the reveal phase, the receiver can either accept or reject, and if it accepted then it should also obtain some message string m. Intuitively, in the commit phase, the sender is sending the message m inside a locked box, and in the reveal phase, the key to unlock the box is sent to the receiver. Formally, we wish that after the commit phase, no information about m should be known to the receiver, a property known as *hiding* (this guarantee can be either information theoretic or computational). At the same time, after the commit phase the sender should not be able to change their mind, so there can be at most one m that the receiver can accept in the reveal phase, this property is called *binding*.

The notion of binding becomes more complicated when quantum communication between the parties is allowed. In such a case, achieving the aforementioned guarantee is generally considered to be impossible due to the well-known superposition attack. Let us consider the task of committing to a single bit. A sender can generate a superposition of the values 0 and 1, e.g. $|b\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and perform the commitment

*Tel Aviv University, Israel, nbitansky@gmail.com. Member of the checkpoint institute of information security. Supported by ISF grants 18/484 and 19/2137, by Len Blavatnik and the Blavatnik Family Foundation, by the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, and by the European Union Horizon 2020 Research and Innovation Program via ERC Project REACT (Grant 756482).

†Weizmann Institute of Science, Israel, zvika.brakerski@weizmann.ac.il. Supported by the Binational Science Foundation (Grant No. 2016726), and by the European Union Horizon 2020 Research and Innovation Program via ERC Project REACT (Grant 756482) and via Project PROMETHEUS (Grant 780701).

phase honestly, controlled by the value $|b\rangle$. That is, Let Q_0, Q_1 be the quantum algorithms that perform the $0, 1$ commitments respectively. Then the sender executes the operation $|b\rangle |x\rangle \to |b\rangle Q_b |x\rangle$. One can think of this as a purification of the process of committing to a random value. Then, only in the reveal phase, the value of b is measured, which leaves the sender with a valid opening for the measured value. Therefore, there is no sense in which the sender's value is "fixed" after the commit phase. In fact, even for statistically binding classical commitment one may wonder what happens if the communication channel is quantum and a quantum adversary sends a quantum value as the commitment string, again causing potential ambiguity. A straightforward solution is for the receiver to measure the information it receives over the channel in order to "force" the commitment to be classical. The reader may want to keep this in mind.

Using quantum commitments has an advantage: it is possible to construct non-interactive quantum commitments from any (post-quantum) one-way function (OWF) [KO09, KO11, YWLQ15]. This is not known for classical commitments and is, in fact, subject to a black box barrier [MP12]. Alas, in order to enjoy the non-interactive scheme, we must sacrifice the beloved classical binding property. We therefore pose the following question.

> *Can we get the best of both worlds? In particular, can we get quantum non-interactive commitments from one-way functions with the binding guarantee of classical commitments?*

In this work we answer the above as follows. We start by defining the notion of classical binding for quantum commitments. We proceed by showing that classically binding commitments can replace classical commitments in an example protocol, with analysis that is essentially identical to the classical analysis. We then present a non-interactive classically-statistically-binding quantum commitment scheme based on the existence of any post-quantum OWF, thus showing that we can get the benefits of quantum commitments together with those of classical binding. Our construction has additional benefits compared to the (only) previous candidate [YWLQ15] in that it has a classical opening whereas the opening in [YWLQ15] is inherently quantum. This is an improvement both in terms of simplicity and also since we do not require the sender and receiver to keep a joint coherent quantum state between the commit and reveal phase. Instead, once the commitment string is sent, only the receiver needs to hold quantum information locally (which can be protected by, e.g., a quantum error correcting code). Finally, we show that classical binding is impossible for statistically hiding quantum commitments, regardless of their round complexity.

1.1 Overview of Our Results and Techniques

We now present our results and techniques in slightly more detail. The reader is encouraged to refer to the technical sections for full details.

Classical Binding for Quantum Commitments. Our definition provides a meaningful interpretation to the claim that, even in the quantum setting, the value of the transcript determines a single message that can be opened by the sender. In a nutshell, our definition instructs the receiver to *measure* a part of the commitment string, with the guarantee that (with high probability) conditioned on the measured value r, the sender can successfully reveal (at most) a single message $\bar{m}(r)$, where $\bar{m}$ is a fixed function. This alludes to our previous discussion on using classical commitments in the quantum setting. Indeed, classical statistically binding commitments over a quantum channel also enjoy our notion of classical binding by simply instructing the receiver to measure the entire transcript of the communication. We show (as discussed below) that classical binding can be achieved also with minimal interaction under minimal assumptions, namely non-interactively under one-way functions.

We view the introduction of this notion as a conceptual contribution of this work, since we believe it allows to pinpoint our intuitive idea of a quantum commitment that behaves like a classical one in terms of binding. The fact that it naturally generalizes the properties of classical commitments over quantum channels could be seen as an indication of its usefulness.

We note that our security model relies on the receiver's ability to perform a measurement. This is justified whenever the receiver has access to a "macroscopic" medium that cannot be placed in superposition under

any conceivable circumstances (e.g. a piece of paper).[1] We furthermore note that our notion is useful in many cases even if the measurement is not actually performed, since the register to be measured is kept under the control of the receiver and therefore the sender cannot "misbehave" since from its viewpoint this register may have been actually measured. We may therefore use the measurement as a tool in the analysis even if the actual receiver in our protocol never actually performs it.

Application: Soundness for Zero-Knowledge. The premise of our notion is in its potential to replace the use of classical commitments in the quantum setting. To illustrate this potential, we show how to prove soundness for the GMW zero-knowledge protocol [GMW86] using classically-binding quantum commitments. This method generalizes straightforwardly to commit-and-open Σ-protocols. This allows to obtain a 3-message zero-knowledge protocol (with non-trivial soundness) from any one-way function, using quantum communication (rather than in four messages, or with a CRS, classically). We note that this final result was already shown before in [YWLQ15, FUW$^+$20]. However, using our notion, the soundness analysis becomes straightforward. Furthermore, instantiated with our particular OWF-based commitment scheme, the resulting Σ-protocol requires only the first message to be quantum, whereas in previous solutions the third message was also inherently quantum.

We recall that the GMW protocol for 3-coloring requires the prover to commit to a coloring of the input graph (randomly permuting the colors) and send the commitments to the verifier. The verifier then samples an edge of the graph and requests the opening of its endpoints. If the graph is not colorable, then a commitment to any coloring will have at least one monochromatic edge which will be detected with probability at least $1/|E|$ (where E is the set of edges). Prior analysis using quantum commitment had to take into account a setting where the prover commits to a superposition over colorings, and one had to deduce from the weaker soundness guarantee that a monochromatic opening must occur with reasonable probability. Classical binding solves this problem straightforwardly: assume (even just for the sake of the analysis) that the verifier performs the "binding" measurement on the commitment values. Then, with all but negligible probability over the outcome of the measurement, the prover is committed to a single coloring (in the sense that any opening that deviates from this coloring will be rejected with overwhelming probability). The probability that a random edge is monochromatic in this coloring is again at least $1/|E|$ and therefore the probability that the verifier rejects is at least $1/|E|$ (up to negligible terms). We note that classical binding does not help (nor hurts) in dealing with complications that arise from establishing the zero-knowledge property in the quantum domain. Indeed, our aim is to replace *classical* commitments in *post-quantum secure* protocols.

For more details about the notion of classical binding and its applicability, see Section 3.

Non-Interactive Classically Statistically-Binding Commitments from OWF. Our construction from OWF can be viewed as a "derandomization" of Naor's commitment scheme (which normally requires a CRS). In some sense, we "delegate" the choice of the CRS to the prover, and the quantum communication allows us to do this without compromising soundness (i.e. binding). In that sense our construction is inherently different from the prior construction of quantum non-interactive statistically-binding commitments, and indeed it leads to new properties such as classical opening and (of course) to achieving classical binding. We hope that this technique of removing the CRS will find other applications and allow to use quantum communication as a resource.

Concretely, we recall Naor's commitment [Nao91], which will be convenient to consider as a 2-message protocol (rather than single message with a CRS). The scheme uses a length-tripling pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^{3n}$ as follows. In the first message, the receiver samples $x \in \{0,1\}^{3n}$ and sends it to the sender. The sender, wishing to send a bit b, samples a seed s for the PRG and sends $G(s) \oplus x^b$ (i.e. either $G(s)$ or $G(s) \oplus x$ depending on b). The opening is simply (b, s). Binding for this classical protocol follows since if it is possible to classically open a commitment to both 0 and 1, then there exist s_0, s_1 s.t. $G(s_0) \oplus G(s_1) = x$. A counting argument shows that there are at most 2^{2n} such strings, and therefore for a random x this is impossible with all but 2^{-n} probability.

[1] Alternatively, it suffices to perform an operation that is equivalent to a measurement from the viewpoint of an adversary, such as copying (via CNOT operation) the "measured" value into a space that is inaccessible by the adversary.

The basic intuition is to allow the sender to sample x and send it to the receiver. If we only have classical communication then soundness is lost since the sender will always choose a "bad" x. However, in the quantum setting we can instruct the sender to generate a superposition over all possible x values. This quantum state (a uniform superposition $\sum_x |x\rangle$) can be efficiently verified (just like a deterministic classical state) and, upon measurement, produces the uniform distribution over x. The intuition, therefore, is that the sender sends a superposition over commitments, so that the verifier can perform the measurement and sample the first message from the correct distribution. We will see that there are a few more ideas required in order to push this intuition through.

Let us take a look at a superposition of commitments. For a value b, we have $\sum_x |x\rangle |G(s) \oplus x^b\rangle$, where s is a random seed sampled by the sender. Glancing at this expression, we can see that the hiding property is now lost, since if $b = 0$ then the second register is independent of the first which makes it easy to recover the committed value. Essentially, we want to have a "fresh uncorrelated copy" of the Naor commitment for any x value. One way to do this is to replace s with $f(x)$ where f is a random function. This random function can be replaced by a pseudorandom function, but we notice an even simpler solution which is to replace f with a pairwise independent function h. That is, a commitment to b is $\sum_x |x\rangle |G(h(x)) \oplus x^b\rangle$ where h is chosen at random from a pairwise independent family. It is known [Zha12b] that pairwise-independent functions are indistinguishable from random functions if a single quantum query is made. The hiding property of this construction follows using by-now-standard arguments from [Zha12b]. The opening of the commitment are the values (b, h), note that they are completely classical. For reasons we explain below, our final scheme is a parallel repetition of this building block (with slightly different parameters).

Toward analyzing binding, we establish the following properties of the aforementioned building-block. First, we notice that given an opening (b, h) it is possible to "uncompute" the commitment string and verify that it has been honestly computed (note that (b, h) completely determine the quantum commitment state). Second, if indeed the state is as prescribed (for some (b, h) regardless of what these values are), then measuring the entire commitment (in the computational basis) will result in a "standard" Naor commitment, and furthermore x will be "bad" only with negligible probability. This means that for the particular classical value obtained from the measurement there can exist only a single accepting opening. These properties are still insufficient for classical binding but we note that they already suffice in order to establish the notion of quantum statistical binding as defined in [YWLQ15].

Nevertheless, we require the stronger notion of *classical binding*, for which the above seems insufficient. Recall that we wish to measure the commitment string so as to establish a classical value that will uniquely determine at most one value for which opening is possible. Alas, in the building block above, if we perform the measurement prior to receiving the opening, we are no longer able to verify the correctness of the state after the opening is received. Our solution is to repeat the commitment k times. This will allow us to measure some of the copies (say each copy with probability $1/2$) and use the other copies for the sake of verification. We show that with all but negligible probability, the measured values will bind the sender to a single message.

To prove the classical binding property of the parallel repeated commitment, we consider an interactive game as follows. A sender first sends a commitment from the single-instance building block. The receiver flips a coin and based on the outcome it does one of the following. For one coin-flip outcome, it measures the commitment state, and asks the receiver to produce two equivocal openings for the measured commitment. For the other coin-flip outcome, the receiver does not measure, and instead asks the sender for an opening that will pass the quantum well-formedness test. We show that in the basic building block, no sender can succeed with probability $> 1/2 + \mathrm{negl}$ in this game. We then use the parallel repetition theorem for quantum protocols of Kitaev and Watrous [KW00] to argue that in a k-parallel-repetition, no sender can succeed with non-negligible probability. The k-repeated version of the game exactly corresponds to our k-repeated commitment, and thus we establish that it is impossible to produce an opening that will explain the measured values in the "wrong" way, and at the same time pass the quantum tests on the other copies. Note that the malicious sender is allowed to know which copies have been measured as well as the measured values and still breaking binding is impossible with noticeable probability.

In the body, we prove amplification for a class of commitments that generalizes the properties of the

above Naor-type commitment. For more details about our construction and proof, see Section 4.

Statistical Hiding with Classical (Computational) Binding. Lastly, we show that our classical binding approach can only be carried out in the setting of statistical binding. This is perhaps not surprising because statistical hiding implies that measurements performed by the receiver cannot noticeably effect the state that is held by the sender. In particular, the well-known superposition adversary can break classical binding. We prove this formally in Section 5.

1.2 Related Work

Commitment schemes in the quantum setting have been studied from various aspects. One line of research is concerned with providing post-quantum security guarantees for *classical* commitment schemes, e.g. [AC02, Unr12, Unr16a, Unr16b]. Most of these efforts are concerned with statistically hiding commitments where binding poses challenges even when using a completely classical scheme. Another line of work is concerned with using quantum communication in order to reduce the assumptions required to achieve commitment schemes with certain properties. This includes the negative result showing that statistical hiding and statistical binding cannot be simultaneously achieved even in the quantum setting [May97, LC97]. Other works showed how to achieve statistically hiding commitments with improved round complexity from minimal assumptions [DMS00, KO09, KO11]. There are also works that are concerned with constructing cryptographic applications, most notably oblivious transfer from one-way functions [CDMS04, BCKM20, GLSV20].

Most relevant to this work are the works of Yan et al. [YWLQ15] and of Fang et al. [FUW$^+$20] which focus on statistical binding in the quantum setting.

The former [YWLQ15] proposes a definition which is weaker than ours and only requires that the honest commitments to $b = 0$ and $b = 1$ are far apart in trace distance. This yields a canonical reveal phase as follows. Consider the sender's preparation of a commitment to some bit value b, and consider the purification (deferred measurement) version of this procedure, so that the sender can be assumed, without loss of generality, to generate a pure state $|\varphi_b\rangle$ and send some part of it to the receiver as the commitment string. In the canonical reveal phase, the sender sends the purification (in addition to b itself of course) so that the receiver can indeed verify that it is holding $|\varphi_b\rangle$. The statistical binding property is used by the authors in order to prove soundness for protocols such as the aforementioned GMW zero-knowledge protocol. However, as they explain, they are required to take a geometric approach and analyze the Hilbert space induced by the protocol in quite detail. Our stronger notion in comparison allows to carry out the classical argument almost verbatim. As explained above, our construction also enjoys the property of the opening being classical and in particular it does not require the sender and receiver to share an entangled state at any point in the protocol.

The latter work [FUW$^+$20] is focused on deriving more applications from the notion of statistical binding. They notice that if we had perfect binding, then it would have been possible to introduce a "virtual measurement" in the analysis that fixes the value of the commitment. They then show that statistical binding can be viewed as an approximation of the above. In some sense, one can view their measurement as playing a similar role to the binding measurement in our definition. However, in our case we are guaranteed by design that the measurement outcome, with high probability, fixes the sender's possible opening. This again makes our notion seemingly easier to work with.

Some notions of commitments where the sender is bound to a single value have been considered in the literature, but mostly as means towards an end and not as a target for investigation in its own right. Damgård et al. [DFR$^+$07] defined a notion of classical binding for quantum commitments in the *bounded storage model*. In this model, the sender is effectively forced to make a partial measurement on the quantum messages sent from the receiver. In contrast, our commitments are in the plain model (we do not make any assumptions on the sender), and binding is enforced by having the (honest) receiver perform certain measurements as prescribed by the protocol.

Recently (and concurrently to our work) Bartusek et al. [BCKM21] presented a definition of a similar spirit to ours. Their notion is slightly weaker as in their case the equivocator does not see the measurement values of the receiver, whereas we allow it. Their application is (fully-simulatable) oblivious transfer, but

for their purposes it suffices to use classical commitments (i.e. to rely on a complete measurement of the commitment string).

2 Preliminaries and Basic Tools

2.1 Quantum Formalism

We propose a formalism that associates "quantum variables" with wires of a quantum circuit. This circuit is sometimes explicit but in other cases it is implicit in the description of a quantum procedure. We denote quantum variables with boldface letters, e.g. $\mathbf{x}$ and classical values using plain letters, e.g. x. We can consider density matrices of quantum variables and also joint density matrices for variables that can jointly occur, namely there exists a cut in our (explicit or implicit) circuit that contains both variables. When a value is "classical" it can be copied, and we therefore formally assume that for any classical value there exist numerous (an unbounded number) of copies of that value.

We refer to all physically allowed manipulation of a quantum system as "quantum operations". This includes quantum gates, unitaries, and also non-unitary operations as tracing out, concatenation of ancilla variables and measurements. For measurement or tracing out, the lost information (i.e. the traced out register or the purification of the measurement) may not be accessible to the parties in our setting, but they can always be recalled for the sake of analysis. Note that all of the above can be formulated in the form of a quantum circuit, and therefore it complies with our aforementioned notion of quantum variables. We denote an application of a quantum operator F on a quantum variable $\mathbf{x}$ by $\mathbf{y} = F(\mathbf{x})$, in this case $\mathbf{y}$ is the quantum variable representing the output wires of F. A quantum operation can be given in oracle form, in which case a party with access to the oracle can perform $\mathbf{y} = F(\mathbf{x})$, but without receiving any information on the functionality of F.

For example, let us consider quantum teleportation where an EPR pair $(\mathbf{x}, \mathbf{y})$ is shared between two parties. Then the party holding $\mathbf{x}$ takes another (independent) single-qubit variable $\mathbf{z}$ and measures $\mathbf{zx}$ in the EPR basis to obtain two classical values z, x. We can then compute $\mathbf{w} = Z^z X^z(\mathbf{y})$.

In this case, we can consider the joint density matrix $\rho_{\mathbf{xyz}}$ which in this case will be equal to $\rho_{\mathbf{xy}} \otimes \rho_{\mathbf{z}}$. The reduced density matrix $\rho_{\mathbf{x}}$ will just be (scaled) identity. However, the density matrix $\rho_{\mathbf{yw}}$ does not exist since $\mathbf{w}$ is derived from $\mathbf{y}$. We can also consider density matrices of classical values, e.g. ρ_{zx} (for the post-measurement values) is a scaled identity matrix (maximally mixed state). However, $\rho_{zx\mathbf{y}}$ is not diagonal. The operation $\mathbf{w} = Z^z X^z(\mathbf{y})$ can be described as applying CNOT and CZ on the joint state $zx\mathbf{y}$.

We denote the class of quantum polynomial time algorithms by QPT. We say that two distribution ensembles $\mathcal{D}_0, \mathcal{D}_1$ are computationally indistinguishable (by quantum adversaries), which we denote $\mathcal{D}_0 \approx \mathcal{D}_1$, if no QPT algorithm (possibly with quantum auxiliary input) can distinguish them with noticeable probability.

2.2 Standard Tools

Definition 2.1 (PRG)**.** *A pseudorandom generator G with stretch $\ell(\lambda) > \lambda$ is a classical polynomial-time algorithm that satisfies pseudorandomness (against quantum distinguishers):*

$$\{ G(U_\lambda) \}_\lambda \approx \{ U_{\ell(\lambda)} \}_\lambda \ ,$$

where for any k, U_k is the uniform distribution on k bits.

Such PRGs are known based on one-way functions [HILL99].[2]

Definition 2.2 (PIH)**.** *A pairwise independent family of hash functions $H = \{ h : \{0,1\}^n \to \{0,1\}^m \}$ satisfies for any distinct $x, x' \in \{0,1\}^n$ and any $y, y' \in \{0,1\}^m$:*

$$\Pr[h(x) = y, h(x') = y' : h \leftarrow H] = 2^{-2m} \ .$$

[2]The proof there considers classical distinguishers (and inverters), but is known to extend to the quantum setting.

Such polynomial-time computable families of functions are known where each function is described by $|h| = O(m+n)$ bits.

3 Classically Binding Quantum Commitments

In this section we define classically binding quantum commitments. For simplicity we restrict attention to non-interactive commitments (which we later construct); the definition can be naturally extended also to interactive protocols.

Definition 3.1 (CBQC)**.** *A classically binding quantum commitment (CBQC) scheme consists of QPT algorithms (S, R, V) satisfying:*

- **Syntax:**
  - *$S(m)$ is a sender algorithm that given classical string $m \in \{0,1\}^\ell$, outputs quantum commitment $\mathbf{c}$ and decommitment $\mathbf{d}$.*
  - *$R(\mathbf{c})$ is a receiver algorithm that (w.l.o.g) has the following structure. Apply an efficiently computable unitary U_R on $(\mathbf{c}, \mathbf{0})$. Then parse the output as $(\mathbf{q}, \mathbf{r})$ and apply a computational-basis measurement on $\mathbf{r}$ to obtain a classical value r. Return $(\mathbf{q}, r)$.*
  - *$V(\mathbf{q}, r, m, \mathbf{d})$ is a verification algorithm that given quantum and classical receiver state $(\mathbf{q}, r)$, classical string m, and quantum decommitment state $\mathbf{d}$ outputs a bit (accept or reject).*

  All algorithms also take a security parameter 1^λ and string length parameter 1^ℓ, which we typically suppress.

- **Correctness:** *For any $m \in \{0,1\}^\ell$,*

$$\Pr\left[V(\mathbf{q}, r, m, \mathbf{d}) = \mathtt{acc} : \begin{array}{c}(\mathbf{c}, \mathbf{d}) \leftarrow S(m) \\ (\mathbf{q}, r) \leftarrow R(\mathbf{c})\end{array}\right] = 1 \ ,$$

  where the probability is over all measurements.

- **Computational Hiding:**

$$\{\, \mathbf{c} : (\mathbf{c}, \mathbf{d}) \leftarrow S(m_0) \,\}_{\lambda, m_0, m_1} \approx \{\, \mathbf{c} : (\mathbf{c}, \mathbf{d}) \leftarrow S(m_1) \,\}_{\lambda, m_0, m_1} \ .$$

- **Classical Binding:** *There exists a negligible function ν (called the* binding error*) and a (classical) function $\bar{m} : \{0,1\}^* \to \{0,1\}^\ell$ (called an extractor), such that for any quantum state $(\mathbf{c}, \mathbf{s})$ and for any quantum circuit $\bar{E}$,*

$$\Pr\left[(\mathbf{q}, r, \mathbf{s}) \text{ is } \bar{m}\text{-binding} : (\mathbf{q}, r) \leftarrow R(\mathbf{c})\right] \geq 1 - \nu(\lambda) \ ,$$

  where the probability is over the measurement done by R and $(\mathbf{q}, r, \mathbf{s})$ is $\bar{m}$-binding if

$$\Pr\left[V(\mathbf{q}, r, m, \mathbf{d}) = \mathtt{acc} : \begin{array}{c}(\mathbf{d}, m) \leftarrow \bar{E}(\mathbf{s}, r) \\ m \neq \bar{m}(r)\end{array}\right] \leq \nu(\lambda) \ ,$$

  where the probability is over all measurements.

The honest commitment experiment as well as the binding experiment are depicted in Figure 1.

In the above definition, the equivocation algorithm E is fixed before the receiver's measurement, but obtains the result of the measurement. We next note that this is equivalent to allowing the equivocation algorithm E to be fixed after the receiver measurement and may depend on the classical description (e.g., as a density matrix) of the state of the system after the measurement. This definition will be slightly cleaner to use in applications.

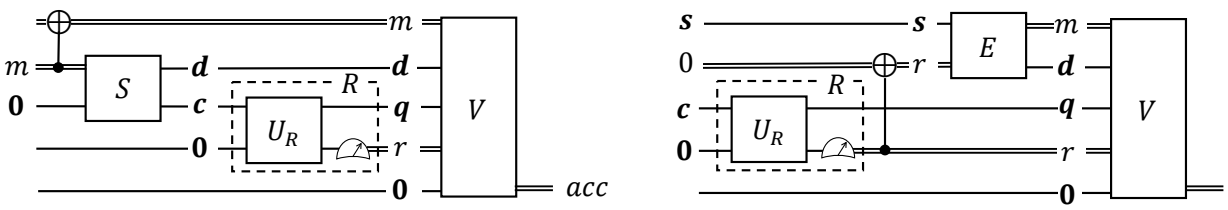

Figure 1: The figure on the left depicts the honest commitment experiment, where the decommitment $\mathbf{d}$ is generated together with the commitment $\mathbf{c}$. The figure on the right depicts the binding experiment, where the commitment $\mathbf{c}$ is entangled with an arbitrary state $\mathbf{s}$, and the equivocation circuit E may use it along with the measured r in order to generate the decommitment.

Definition 3.2 (Classical Binding with Post-Measurement Equivocation)**.** *There exists a negligible function ν (called the* binding error*) and a (classical) function $\bar{m} : \{0,1\}^* \to \{0,1\}^\ell$ (called an extractor), such that for any quantum state $(\mathbf{c}, \mathbf{s})$,*

$$\Pr\left[(\mathbf{q}, r, \mathbf{s}) \text{ is } \bar{m}\text{-binding} : (\mathbf{q}, r) \leftarrow R(\mathbf{c})\right] \geq 1 - \nu(\lambda) \ ,$$

where the probability is over the measurement done by R and $(\mathbf{q}, r, \mathbf{s})$ (where r is a fixed *post-measurement value) is $\bar{m}$-binding if for any quantum circuit $E = E_{\rho_{(\mathbf{q},r,\mathbf{s})}}$ it holds that*

$$\Pr[V(\mathbf{q}, r, m, \mathbf{d}) = \mathtt{acc} : \begin{array}{c} (\mathbf{d}, m) \leftarrow E(\mathbf{s}) \\ m \neq \bar{m}(r) \end{array}] \leq \nu(\lambda) \ ,$$

where the probability is over all measurements.

Proposition 3.1. *A set of algorithms (S, R, V) is CBQC according to Definition 3.2 if and only if it is CBQC according to Definition 3.1.*

Proof. We prove that binding according to one notion implies binding according to the other, with respect to the same extractor $\bar{m}$ and binding error ν, and vise versa.

Assume that binding holds with respect to definition 3.2. Consider a state $(\mathbf{c}, \mathbf{s})$, let $(\mathbf{q}, r)$ be defined using R as above. Consider any family of equivocators $E = \{ E_{\rho_{(\mathbf{q},r,\mathbf{s})}} \}$, which takes $\mathbf{s}$ as input and produces an arbitrary output. Then we show that there exists $\bar{E}$ such that $(\mathbf{q}, r, \bar{E}(\mathbf{s}, r))$ is distributed identically to $(\mathbf{q}, r, E_{\rho_{(\mathbf{s},\mathbf{q},r)}}(\mathbf{s}))$. This implies that binding holds with respect to definition 3.1. To see why the above is true, note that the state $(\mathbf{s}, \mathbf{q}, r)$ is exactly $((I \otimes |r\rangle\langle r|) \cdot (I \otimes U_R))(\mathbf{s}, \mathbf{c}, \mathbf{0})$, properly normalized. Therefore, given r and given the density matrix of $(\mathbf{c}, \mathbf{s})$, it is possible to compute exactly the density matrix of $(\mathbf{s}, \mathbf{q}, r)$.

Consider, therefore, the procedure $\bar{E}$ which contains a description of $\rho_{(\mathbf{c},\mathbf{s})}$, and takes r as one if its inputs. It can compute out of $\rho_{(\mathbf{c},\mathbf{s})}$ and r the density matrix $\rho_{(\mathbf{q},r,\mathbf{s})}$, and then recovers the corresponding equivocator $E_{\rho_{(\mathbf{q},r,\mathbf{s})}}$ (which as defined depends on $(\mathbf{q}, r, \mathbf{s})$ so is fully specified by their density matrix), and applies this $E_{\rho_{(\mathbf{q},r,\mathbf{s})}}$ on its input $\mathbf{s}$. By definition $(\mathbf{q}, r, \bar{E}(\mathbf{s}, r))$ is identical to $(\mathbf{q}, r, E(\mathbf{s}))$ and the claim follows.

In the converse direction, assume that binding holds with respect to definition 3.1. Consider again a state $(\mathbf{c}, \mathbf{s})$, and $(\mathbf{q}, r)$ be defined using R as above. Consider any (universal) equivocator $\bar{E}$, which takes $(\mathbf{s}, r)$ as input and produces an arbitrary output. Then consider $E = \{ E_{\rho_{(\mathbf{q},r,\mathbf{s})}} \}$ where $E_{\rho_{(\mathbf{q},r,\mathbf{s})}}(\mathbf{s})$ applies $\bar{E}(\mathbf{s}, r)$. Then $(\mathbf{q}, r, \bar{E}(\mathbf{s}, r))$ is distributed identically to $(\mathbf{q}, r, E_{\rho_{(\mathbf{q},r,\mathbf{s})}}(\mathbf{s}))$. This implies that binding holds with respect to definition 3.2. □

3.1 Composition and Application

In this section, we show that like classical commitments, classically-binding quantum commitments can be composed in parallel. In particular, it seems that they can generally replace classical commitments in

"commit and open" protocols such as zero knowledge protocols, essentially without changing the proof. As a simple example, we show how CBQCs can be used to prove the soundness of the GMW protocol. Throughout this section, it will be convenient to use the equivalent Definition 3.2 of classical binding with post-measurement equivocation.

Proposition 3.2 (Multi-Commitment Classical Binding)**.** *Let (S, R, V) be a CBQC with extractor $\bar{m} : \{0,1\}^* \to \{0,1\}^\ell$ and binding error ν. Then for any quantum state $(\mathbf{s}, \mathbf{c}_1, \ldots, \mathbf{c}_t)$,*

$$\Pr\left[(\mathbf{q}_1, r_1, \ldots, \mathbf{q}_t, r_t, \mathbf{s}) \text{ is } \bar{m}\text{-binding} : (\mathbf{q}_1, r_1) \leftarrow R(\mathbf{c}_1) \ldots (\mathbf{q}_t, r_t) \leftarrow R(\mathbf{c}_t)\right] \geq 1 - t \cdot \nu(\lambda) \ ,$$

where the probability is over the measurements done by R and $(\mathbf{q}_1, r_1, \ldots, \mathbf{q}_t, r_t, \mathbf{s})$ is $\bar{m}$-binding if for any quantum circuit E and $i \in [t]$,

$$\Pr\left[V(\mathbf{q}_i, r_i, m, \mathbf{d}) = \mathtt{acc} : \begin{array}{c}(\mathbf{d}, m) \leftarrow E(\mathbf{s}) \\ m \neq \bar{m}(r_i)\end{array}\right] \leq \nu(\lambda) \ ,$$

where the probability is over all measurements.

Remark 3.1 (String Commitments). Note that an immediate corollary of the above is that as in the classical case, classically binding bit commitments (i.e. where $\ell = 1$) imply classically binding string commitment (i.e. where $\ell = \text{poly}(\lambda)$ for an arbitrary polynomial).

Proof of Proposition 3.2. Fix $(\mathbf{s}, \mathbf{c}_1, \ldots, \mathbf{c}_t)$ and assume toward contradiction that

$$\Pr\left[(\mathbf{q}_1, r_1, \ldots, \mathbf{q}_t, r_t, \mathbf{s}) \text{ is not } \bar{m}\text{-binding} : (\mathbf{q}_1, r_1) \leftarrow R(\mathbf{c}_1) \ldots (\mathbf{q}_t, r_t) \leftarrow R(\mathbf{c}_t)\right] > t \cdot \nu(\lambda) \ .$$

Then there exists an $i \in [t]$ such that

$$\begin{aligned}&\Pr\left[(\mathbf{q}_i, r_i, \mathbf{s}) \text{ is not } \bar{m}\text{-binding} : (\mathbf{q}_i, r_i) \leftarrow R(\mathbf{c}_i)\right] = \\ &\Pr\left[(\mathbf{q}_i, r_i, \mathbf{s}) \text{ is not } \bar{m}\text{-binding} : (\mathbf{q}_1, r_1) \leftarrow R(\mathbf{c}_1) \ldots (\mathbf{q}_t, r_t) \leftarrow R(\mathbf{c}_t)\right] > \nu(\lambda) \ ,\end{aligned}$$

where the probability is over the measurements done by R, and $\bar{m}$-binding is according to Definition 3.2 (the single commitment case). This contradicts classical binding of (S, R, V) with respect to the commitment and sender state $(\mathbf{c}_i, \mathbf{s})$. □

Soundness of GMW. As a simple example we show how CBQCs can replace classical commitments in the GMW three-coloring protocol [GMW91], while the soundness proof remains the same as in the classical case.

We do not address zero knowledge here. The proof of Watrous [Wat09] that the protocol is zero knowledge relies only on the computational hiding of the commitments, and holds as is, in the case that the commitments are quantum rather than classical. This was already observed for instance in [YWLQ15].

We recall the description of the honest verifier in the GMW protocol, where we instantiate the commitment scheme using a CBQC (S, R, V) (we omit details about the honest prover algorithm, as they are irrelevant to the proof of soundness.

The GMW verifier V_{zk}, given a graph $G = ([n], E)$:

1. V_{zk} receives from the prover commitments $\mathbf{c}_1, \ldots, \mathbf{c}_n$, each to a color $\sigma_k \in [3]$.
2. V_{zk} applies the commitment receiver $(\mathbf{q}_k, r_k) \leftarrow R(\mathbf{c}_k)$ for all $k \in [n]$.
3. V_{zk} picks a random edge $(i, j) \in E$, and sends it to the prover.
4. V_{zk} receives openings $(\mathbf{d}_i, \sigma_i), (\mathbf{d}_j, \sigma_j)$ to the corresponding commitments i, j.
5. V_{zk} applies the commitment verifier $V(\mathbf{q}_i, r_i, \sigma_i, \mathbf{d}_i), V(\mathbf{q}_j, r_j, \sigma_j, \mathbf{d}_j)$, and accepts if both accept, and $\sigma_i \neq \sigma_j$.

Remark 3.2. In the above description, we could defer the application of R to the last step (and also apply it only on $\mathbf{c}_i, \mathbf{c}_j$). Indeed, these operations commute and do not change the probability of acceptance. However, the above order will make the soundness analysis conceptually simple.

Proposition 3.3. *Let G be a graph that is not three-colorable. Then no prover (unbounded quantum circuit) convinces the verifier of excepting with probability greater than $1 - 1/|E| + \mathrm{negl}(\lambda)$.*

Proof. Fix any graph $G = ([n], E)$ that is not three colorable, and any prover. We assume w.l.o.g that the prover has the following simple form:

- It sends quantum commitments $\mathbf{c}_1, \ldots, \mathbf{c}_n$ and keeps a corresponding state $\mathbf{s}$.
- Given the verifier choice i, j, it applies a quantum circuit $P_{i,j}(\mathbf{s})$ to generate its message $(\mathbf{d}_i, \sigma_i, \mathbf{d}_j, \sigma_j)$.

By (multi-commitment) classical binding, with probability $1 - \mathrm{negl}(\lambda)$ over the measurements of R in Step 2, $(\mathbf{s}, \mathbf{q}_1, r_1, \ldots, \mathbf{q}_n, r_n)$ is $\bar{m}$-binding. Let $\bar{\sigma}_k = \bar{m}(r_k)$, where $\bar{m}$ is the extractor function given by the CBQC. Then, because G is not three-colorable, there exists $(i^*, j^*) \in E$ such that $\bar{\sigma}_{i^*} = \bar{\sigma}_{j^*}$. Conditioned on the verifier choosing (i^*, j^*), it accepts only in the case that for some $k \in \{ i^*, j^* \}$, $V(\mathbf{q}_k, r_k, \sigma_k, \mathbf{d}_k) = \mathtt{acc}$ and $\sigma_k \neq \bar{\sigma}_k = \bar{m}(r_k)$. However, by $\bar{m}$-binding, this occurs with probability at most $\mathrm{negl}(\lambda)$. Overall, the prover fails to convince the verifier with probability $1/|E| - \mathrm{negl}(\lambda)$.

□

4 Construction

Toward the construction we define a stronger notion that we call *split classical binding* (SCB). The advantage of this notion is that it allows for *binding amplification*, which we will use in our constructions.

4.1 Split Classical Binding

In split classical binding quantum commitments (SCBQC), the decommitment d is classical. Furthermore, the verifier V is split to a classical part cV and a quantum part qV. The high-level guarantee is that with overwhelming probability over the measurements of the receiver, the measured value r is either:

- a (classical) commitment that is binding with respect to the classical verifier cV — i.e. cV would accept at most a single message as an opening of r.
- or, the quantum verifier qV will reject with overwhelming probability.

Definition 4.1 (Split Classical Binding)**.** *A quantum commitment (S, R, V) is split classically binding if:*

- **Classical Decommitment:** *The sender $(\mathbf{c}, d) \leftarrow S(m)$ produces a classical decommitment (equivalently, $V(\mathbf{q}, r, m, \mathbf{d})$ always measures the decommitment $\mathbf{d}$ in the computational basis).*
- **Split Verifier:** *There exists a classical PPT verifier cV and a QPT verifier qV such that*

$$V(\mathbf{q}, r, m, d) = \mathtt{acc} \text{ if and only if } qV(\mathbf{q}, m, d) = \mathtt{acc} \text{ and } qV(r, m, d) = \mathtt{acc}.$$

- **Split Binding:** *There exists a negligible function ν (called the* binding error*) such that for any quantum state $(\mathbf{c}, \mathbf{s})$ and any (unbounded) quantum circuit E,*

$$\Pr\left[qV(\mathbf{q}, b, d) = \mathtt{acc} \text{ and } r \text{ is not binding} : \begin{array}{l} (\mathbf{q}, r) \leftarrow R(\mathbf{c}) \\ (d, b) \leftarrow E(\mathbf{s}, r) \end{array} \right] \leq \nu(\lambda) \ ,$$

where the probability is over all measurements done by R, E, and qV, and r is not binding if

$$cV(r, m_0, d_0) = cV(r, m_1, d_1) = \mathtt{acc} \qquad \text{for some } d_0, d_1 \text{ and } m_0 \neq m_1.$$

The scheme is **δ-binding** *if ν is replaced by some (non-negligible) function δ.*

Proposition 4.1. *Any SCBQC is a CBQC.*

Proof. Let (S, R, V) be SCBQC. Then by split binding, there exists a negligible function ν such that for all $(\mathbf{s}, \mathbf{c})$ and E it holds that

$$\Pr\left[qV(\mathbf{q}, r, m, d) = \texttt{acc} \text{ and } r \text{ is not binding} : \begin{array}{c}(\mathbf{q}, r) \leftarrow R(\mathbf{c}) \\ (d, m) \leftarrow E(\mathbf{s}, r)\end{array}\right] \leq \nu(\lambda) \ .$$

Define the extractor function $\bar{m}(r)$ that returns m if there is a unique bit m such that $cV(r, m, d) = \texttt{acc}$ for some d; otherwise, $\bar{m}(r)$ returns $\perp$.

Therefore, with probability at least $1 - \sqrt{\nu(\lambda)}$ over the measurement $(\mathbf{q}, r) \leftarrow R(\mathbf{c})$, the state $(\mathbf{q}, r, \mathbf{s})$ satisfies either:

1. r is binding, in which case $cV(r, m, d) = \texttt{rej}$ for any $m \neq \bar{m}(r)$, or
2. $\Pr\left[qV(\mathbf{q}, b, d) = \texttt{acc} : (d, m) \leftarrow E(\mathbf{s}, r)\right] \leq \sqrt{\nu(\lambda)}$.

Recall that by definition, V accepts only if both qV and cV accept. It follows that

$$\Pr\left[V(\mathbf{q}, r, m, \mathbf{d}) = \texttt{acc} \wedge m \neq \bar{m}(r) : \begin{array}{c}(\mathbf{q}, r) \leftarrow R(\mathbf{c}) \\ (\mathbf{d}, m) \leftarrow E(\mathbf{s}, r)\end{array}\right] \leq \sqrt{\nu(\lambda)} \ .$$

This completes the proof, showing classical binding with binding error $\sqrt{\nu(\lambda)}$). □

4.2 Split Binding Amplification

In this section we prove that for SCBQC we can amplify δ-binding to negl-binding.

Definition 4.2 (n-Fold SCBQC)**.** *Let $(S, R, V = (qV, cV))$ be an SCBQC, the corresponding n-fold SCBQC denoted by $(S^{\otimes n}, R^{\otimes n}, V^{\otimes n} = (qV^{\otimes n}, cV^{\otimes n}))$ is defined as follows:*

- *$S^{\otimes n}(m)$ applies $S(m)$ n times independently resulting in $(\mathbf{c}_1, d_1), \ldots, (\mathbf{c}_n, d_n)$.*
- *$R^{\otimes n}(\mathbf{c}_1, \ldots, \mathbf{c}_n)$ applies $R(\mathbf{c}_i)$ for every i resulting in $(\mathbf{q}_1, r_1), \ldots, (\mathbf{q}_n, r_n)$.*
- *$qV^{\otimes n}((\mathbf{q}_1, \ldots, \mathbf{q}_n), m, (d_1, \ldots, d_n))$ applies $qV(\mathbf{q}_i, b, d_i)$ for every i and outputs* acc *if and only if all are* acc*.*
- *$cV^{\otimes n}((r_1, \ldots, r_n), m, (d_1, \ldots, d_n))$ applies $cV(r_i, b, d_i)$ for every i and outputs* acc *if and only if all are* acc*.*

Proposition 4.2 (Binding Amplification)**.** *If (S, R, qV, cV) is δ-binding for some constant $\delta < 1$, then the n-fold $(S^{\otimes n}, R^{\otimes n}, qV^{\otimes n}, cV^{\otimes n})$ is δ^n-binding.*

Proof. Consider the following 3-message quantum proof system $(\mathbb{P}, \mathbb{V})$ for the empty language:

1. $\mathbb{P}$ sends $\mathbb{V}$ a commitment $\mathbf{c}$.
2. $\mathbb{V}$ applies $(\mathbf{q}, r) \leftarrow R(\mathbf{c})$ and sends r to $\mathbb{P}$.
3. $\mathbb{P}$ provides d_0, d_1, m_0, m_1.
4. $\mathbb{V}$ accepts if $cV(r, m_0, d_0) = cV(r, m_1, d_1) = \texttt{acc}$. $m_0 \neq m_1$, and $qV(\mathbf{q}, m_0, d_0) = \texttt{acc}$.

Claim 4.1. *The soundness error ε of $(\mathbb{P}, \mathbb{V})$ is at most δ.*

Proof. Fix any prover $\mathbb{P}^\star$ with initial state $\mathbf{s}_0$ and let ε be the probability it convinces the verifier $\mathbb{V}$ to accept. Let $\mathbf{c}$ be the first message of $\mathbb{P}^\star$ and let $\mathbf{s}$ be its state after sending it. Let E be the quantum circuit that given $(\mathbf{s}, r)$ computes the prover's third message (d_0, d_1, m_0, m_1) corresponding to state $\mathbf{s}$ and verifier message r, and outputs (d_0, m_0).

By the definition of $\mathbb{V}$, we can bound the probability ε that $\mathbb{P}^\star$ convinces $\mathbb{V}$ as follows

$$\varepsilon \leq \Pr\left[qV(\mathbf{q}, m_0, d_0) = \texttt{acc} \text{ and } r \text{ is not binding} : \begin{array}{l}(\mathbf{q}, r) \leftarrow R(\mathbf{c}) \\ (d_0, m_0) \leftarrow E(\mathbf{s}, r)\end{array}\right] \leq \delta \ ,$$

where the last inequality follows by the δ-binding of the SCBQC $(S, R, V = (qV, cV))$. □

Invoking a parallel repetition theorem by Kitaev and Watrous for 3-message quantum interactive proofs, we deduce that in the n-fold version of the protocol the soundness error reduces at an exponential rate.

Claim 4.2 ([KW00])**.** *Let $(\mathbb{P}^{\otimes n}, \mathbb{V}^{\otimes n})$ be the n-fold parallel repetition of $(\mathbb{P}, \mathbb{V})$. The soundness error of $(\mathbb{P}^{\otimes n}, \mathbb{V}^{\otimes n})$ is $\varepsilon_n = \varepsilon^n$.*

Finally, to prove that the binding error of the n-fold SCBQC $(S^{\otimes n}, R^{\otimes n}, V^{\otimes n} = (qV^{\otimes n}, cV^{\otimes n}))$ also reduces at an exponential rate, we relate it to the soundness of the corresponding n-fold interactive proof.

Claim 4.3. *$(S^{\otimes n}, R^{\otimes n}, qV^{\otimes n}, cV^{\otimes n})$ is δ_n-binding for $\delta_n \leq \varepsilon_n$.*

Proof. Let $(\mathbf{c}, \mathbf{s})$ be a quantum state and E a quantum circuit which violate η-binding for some $\eta \in (0, 1]$. We describe a prover strategy $\mathbb{P}^\star$ that convinces $\mathbb{V}^{\otimes n}$ to accept with probability $\varepsilon' \geq \eta$:

1. $\mathbb{P}^\star$ sends $\mathbf{c}$ as its first message, and keeps the register $\mathbf{s}$.
2. Given r, $\mathbb{P}^\star$ applies $(d_0, m_0) \leftarrow E(\mathbf{s}, r)$.
3. $\mathbb{P}^\star$ searches for a decommitment d_1 and m_1 such that r can be opened to m_1, namely such that $cV^{\otimes n}(r, m_1, d_1) = \texttt{acc}$. If such d_1 exists, $\mathbb{P}^\star$ sends (d_0, d_1, m_0, m_1) to $\mathbb{V}$; otherwise, it aborts.

We can bound from below the probability ε' that $\mathbb{P}^\star$ convinces $\mathbb{V}^{\otimes n}$ as follows:

$$\varepsilon' \geq \Pr\left[qV(\mathbf{q}, m_0, d_0) = \texttt{acc} \text{ and } r \text{ is not binding} : \begin{array}{l}(\mathbf{q}, r) \leftarrow R(\mathbf{c}) \\ (d_0, m_0) \leftarrow E(\mathbf{s}, r)\end{array}\right] \geq \eta \ ,$$

where the last inequality follows by our assumption that $\mathbf{c}, \mathbf{s}, E$ violate η-binding. □

Overall, we deduce that $\delta_n \leq \delta^n$. Proposition 4.2 follows. □

4.3 SCBQC from any One-Way Function

In this section we show how to construct SCBQC from any post-quantum secure one-way function.

Theorem 4.1. *Assuming QOWFs there exist a $\Omega(1)$-binding split classically binding quantum bit commitment.*

In what follows, let $G : \{0,1\}^\lambda \to \{0,1\}^{4\lambda}$ be a length-tripling PRG and, let $H_{4\lambda,\lambda}$ be a pairwise independent hash family mapping $\{0,1\}^{4\lambda}$ to $\{0,1\}^\lambda$. As noted in Section 2, PRGs exist assuming one-way functions, and pairwise independent hashing families exist unconditionally.

The Scheme:

- $(\mathbf{c}, d) \leftarrow S(b)$: samples a random hash $h \leftarrow H$ and prepares the state:

$$|\mathbf{c}\rangle = |\mathbf{c}_{h,b}\rangle := 2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |G(h(x)) \oplus x^b\rangle \quad ,$$

  where $x^1 := x$ and $x^0 := 0^{|x|}$.
  The decommitment information d is the hash h.

- $(\mathbf{q}, r) \leftarrow R(\mathbf{c})$: tosses a random coin $t \leftarrow \{\, \texttt{measure}, \texttt{keep} \,\}$ and

  - If $t = \texttt{measure}$, measures $\mathbf{c}$ in the computational basis, stores the bit t and the result of measuring $\mathbf{c}$ in r and also stores t in $\mathbf{q}$.
  - If $t = \texttt{keep}$, stores the bit t and $\mathbf{c}$ in $\mathbf{q}$ and also stores t in r.

  We note that this functionality can be arranged to comply with the syntax in Definition 3.2 by defining the unitary U_R as follows.

  First consider a purification of the coin t by considering a variable $\mathbf{t}$ initialized to 0, and then applying a Hadamard gate so that $\mathbf{t}$ contains the $|+\rangle$ state (associating the value `measure` with 0 and `keep` with 1). It then CNOTs $\mathbf{t}$ into another quantum register $\mathbf{t}'$ (so that $\mathbf{t}, \mathbf{t}'$ are in fact an EPR pair).

  It then creates two registers $\mathbf{q}$ and $\mathbf{r}$, where the former contains $(\mathbf{t}, \mathbf{c})$, and the latter contains $(\mathbf{t}', \mathbf{0})$. Then controlled on the value of $\mathbf{t}$ (i.e. controlled on the value being equal to `keep`), swap the second parts of $\mathbf{q}$ and $\mathbf{r}$.

  One can verify that the outcome of this procedure is as described above. Note that $\mathbf{t}$ is always being measured since it is a part of $\mathbf{r}$ and the value of $\mathbf{t}'$ in $\mathbf{q}$ will always be equal to this classical measured value, so after the measurement we can refer to this value as one classical value t.

- $qV(\mathbf{q}, b, d)$: parse $\mathbf{q} = (\mathbf{t}', \mathbf{c}')$, recall that $\mathbf{t}'$ has been indirectly measured and therefore corresponds to the classical value t:

  - If $t = \texttt{measure}$, outputs `acc`.
  - If $t = \texttt{keep}$, parses $d = h$ as a hash, performs the measurement $\{ \; |\, \mathbf{c}_{h,b}\rangle\langle \mathbf{c}_{h,b} \,|\, , I - |\, \mathbf{c}_{h,b}\rangle\langle \mathbf{c}_{h,b} \,|\; \}$ on $\mathbf{c}'$, and accepts if it succeeded.

  $cV(r, b, d)$: reads t from r:

  - If $t = \texttt{keep}$, outputs `acc`.
  - If $t = \texttt{measure}$, parses $d = h$, reads the measurement (x, y) from r, and outputs `acc` if and only if

$$y = G(h(x)) \oplus x^b \quad .$$

The correctness of the scheme follows readily from the construction. We prove that the scheme is $\Omega(1)$-binding in Proposition 4.3, and prove that it is computationally hiding in Proposition 4.4.

Proposition 4.3. *The scheme is δ-binding for $\delta = 1/2 - 3 \cdot 2^{-\lambda/2}$.*

Proof. We consider a quantum system defined over input wires $\mathbf{c}, \mathbf{s}, \mathbf{t}, \mathbf{a}$, where $\mathbf{c}$ corresponds to a commitment, $\mathbf{s}$ is a sender state, $\mathbf{t}$ represents a choice in $\{\, \texttt{measure}, \texttt{keep} \,\}$, and $\mathbf{a}$ corresponds to any ancilla required by the system. Fix any state $(\mathbf{c}, \mathbf{s})$ and circuit E, and assume w.l.o.g. that the state $(\mathbf{c}, \mathbf{s})$ is pure and we accordingly denote it by $|\mathbf{c}, \mathbf{s}\rangle$ (if $(\mathbf{c}, \mathbf{s})$ is not pure, we consider a purification $(\mathbf{c}, \mathbf{s}')$ of $(\mathbf{c}, \mathbf{s})$). The initial (pure) state of the system is $|\zeta\rangle = |\mathbf{c}, \mathbf{s}\rangle \, |\mathbf{0}\rangle$.

Let U be a unitary circuit that is a purification of the quantum circuit corresponding to a coherent execution of the binding experiment. Namely, it applies $U_R(\mathbf{c}, \mathbf{0})$ followed by $E(\mathbf{s}, \mathbf{r})$ and finally by $qV(\mathbf{d}, \mathbf{b}, \mathbf{q})$. We consider the outputs $\mathbf{v}$ indicating whether qV accepts, as well as $\mathbf{o}$, which is a CNOT of $\mathbf{r}$ onto a zero ancilla. We disregard any additional output wires. The circuit is depicted in Figure 2.

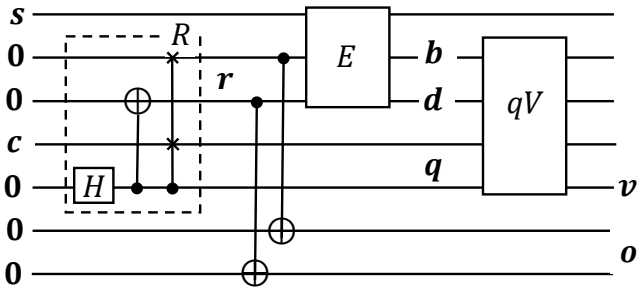

Figure 2: The unitary U capturing the binding experiment. The circuits R, E, qV are purified and replaced with their unitary versions. In the above figure, $\mathbf{r}, \mathbf{q}, \mathbf{o}$ each consist of two wires (above and below the corresponding letter).

We define a projection Π on the output wires of U that corresponds to breaking split binding; namely, where the quantum verifier accepts $\mathbf{v} = \mathtt{acc}$, and in addition $\mathbf{o} = r$ is not binding. We also define restrictions $\Pi_{\mathtt{m}}, \Pi_{\mathtt{k}}$ of Π to the subspace where $t = \mathtt{measure}$ and $t = \mathtt{keep}$, respectively.

Formally, we define the set of equivocable strings as

$$G_{\oplus} = \{\, x = G(s_1) \oplus G(s_2) \text{ for some } s_1, s_2 \,\} \ ,$$

and note that $r = (t, x, y)$ is not binding only if $t = \mathtt{keep}$ or $x \in G_{\oplus}$.

We define

$$\Pi_{\mathtt{m}} := U^{\dagger}\Big(I \otimes \sum_{\substack{r=(t,x,y) \\ x \in G_{\oplus}, t=\mathtt{measure}}} |r, \mathtt{acc}\rangle\langle \mathtt{acc}, r| \Big) U \ ,$$

$$\Pi_{\mathtt{k}} := U^{\dagger}\Big(I \otimes \sum_{\substack{r=(t,x,y) \\ t=\mathtt{keep}}} |r, \mathtt{acc}\rangle\langle \mathtt{acc}, r| \Big) U \ ,$$

$$\Pi = \Pi_{\mathtt{m}} + \Pi_{\mathtt{k}} \ ,$$

where $\sum |r, \mathtt{acc}\rangle\langle \mathtt{acc}, r|$ acts on wires $(\mathbf{o}, \mathbf{v})$, and I acts on all other output wires.

Then the probability of breaking split binding is

$$\delta := \|\Pi\,|\zeta\rangle\,\|^2 = \|\Pi_{\mathtt{m}}\,|\zeta\rangle\,\|^2 + \|\Pi_{\mathtt{k}}\,|\zeta\rangle\,\|^2 \ ,$$

where above we use the fact that $\Pi = \Pi_{\mathtt{m}} + \Pi_{\mathtt{k}}$ and the fact that $\Pi_{\mathtt{m}}$ and $\Pi_{\mathtt{k}}$ are projections on two orthogonal subspaces.

To bound δ we consider a partition of the input commitment wires $\mathbf{c}$ into wires $(\mathbf{x}, \mathbf{y})$ and define another projection $\Pi_{\oplus}$ on $\mathbf{x}$ that corresponds to the subspace of equivocable strings. Formally,

$$\Pi_{\oplus} := \sum_{x \in G_{\oplus}} |x\rangle\langle x| \otimes I \ ,$$

where $\sum |x\rangle\langle x|$ acts on $\mathbf{x}$ and I acts on all other input wires. We denote $\bar{\Pi}_{\oplus} := I - \Pi_{\oplus}$ (where here I acts on the entire space).

We now define $|\zeta_{\oplus}\rangle = \Pi_{\oplus}\,|\zeta\rangle\,/\alpha$ and $|\bar{\zeta}_{\oplus}\rangle = \bar{\Pi}_{\oplus}\,|\zeta\rangle\,/\bar{\alpha}$, for $\alpha = \|\Pi_{\oplus}\,|\zeta\rangle\,\|$ and $\bar{\alpha} = \|\bar{\Pi}_{\oplus}\,|\zeta\rangle\,\| = \sqrt{1-\alpha^2}$, where the last equality follows from the fact that $\Pi_{\oplus}$ and $\bar{\Pi}_{\oplus}$ project to orthogonal subspaces. (In the degenerate case $\alpha = 0$, set $|\zeta_{\oplus}\rangle = 0$, similarly if $\bar{\alpha} = 0$, set $|\bar{\zeta}_{\oplus}\rangle = 0$.)

Then

$$\delta = \|\alpha\Pi_{\mathtt{m}}\,|\zeta_\oplus\rangle + \bar{\alpha}\Pi_{\mathtt{m}}\,|\bar{\zeta}_\oplus\rangle\,\|^2 + \|\alpha\Pi_{\mathtt{k}}\,|\zeta_\oplus\rangle + \bar{\alpha}\Pi_{\mathtt{k}}\,|\bar{\zeta}_\oplus\rangle\,\|^2 \quad .$$

To conclude the proof we show:

Claim 4.4.

1. $\Pi_{\mathtt{m}}\,|\bar{\zeta}_\oplus\rangle = 0$,
2. $\|\Pi_{\mathtt{m}}\,|\zeta_\oplus\rangle\,\|^2 \leq 1/2$,
3. $\|\Pi_{\mathtt{k}}\,|\bar{\zeta}_\oplus\rangle\,\|^2 \leq 1/2$,
4. $\|\Pi_{\mathtt{k}}\,|\zeta_\oplus\rangle\,\|^2 \leq 2^{-\lambda+1}$.

Before we prove the claim, we show that it indeed gives the desired bound on δ:

$$\begin{aligned}\delta &\leq \alpha^2\|\Pi_{\mathtt{m}}\,|\zeta_\oplus\rangle\,\|^2 + \alpha^2\|\Pi_{\mathtt{k}}\,|\zeta_\oplus\rangle\,\|^2 + \bar{\alpha}^2\|\Pi_{\mathtt{k}}\,|\bar{\zeta}_\oplus\rangle\,\|^2 + 2\alpha\bar{\alpha}\|\Pi_{\mathtt{k}}\,|\zeta_\oplus\rangle\,\| \cdot \|\Pi_{\mathtt{k}}\,|\bar{\zeta}_\oplus\rangle\,\| \\ &\leq \alpha^2/2 + \alpha^2 2^{-\lambda+1} + \bar{\alpha}^2/2 + 2\alpha\bar{\alpha}\cdot 2^{\frac{-\lambda+1}{2}}/\sqrt{2} \\ &\leq 1/2 + 3\cdot 2^{\frac{-\lambda}{2}} \quad ,\end{aligned}$$

where the inequalities follows from Claim 4.4 and the fact that $\alpha^2 + \bar{\alpha}^2 = 1$ (and in particular both are smaller than 1).

Proof of Claim 4.4.

1. When the initial state is $|\bar{\zeta}_\oplus\rangle$, the commitment $\mathbf{c} = (\mathbf{x}, \mathbf{y})$ is such that $\mathbf{x}$ is in the subspace of binding strings spanned by $\{\ |\,x\rangle : x \notin G_\oplus\ \}$; in particular, the output wire $\mathbf{o} = (\mathbf{t}', \mathbf{x}', \mathbf{y}')$ is such that $\mathbf{x}'$ (which represents the measurement of $\mathbf{x}$) is in the subspace spanned by $\{\ |\,x\rangle : x \notin G_\oplus\ \}$, accordingly the projection $\Pi_{\mathtt{m}}\,|\bar{\zeta}_\oplus\rangle$ is zero.

2,3. Note that for any state $|\xi\rangle$, $\|\Pi_{\mathtt{m}}\,|\xi\rangle\,\|^2$ (respectively, $\|\Pi_{\mathtt{k}}\,|\xi\rangle\,\|^2$) is the probability that split binding is broken and $t = \mathtt{measure}$ (respectively, $t = \mathtt{keep}$). This probability is in particular at most the probability that $t = \mathtt{measure}$ (respectively, $t = \mathtt{keep}$), which is 1/2. In particular, both $\|\Pi_{\mathtt{m}}\,|\zeta_\oplus\rangle\,\|^2$ and $\|\Pi_{\mathtt{k}}\,|\bar{\zeta}_\oplus\rangle\,\|^2$ are at most 1/2.

4. To bound the probability $\|\Pi_{\mathtt{k}}\,|\zeta_\oplus\rangle\,\|^2$ that $t = \mathtt{keep}$ and split binding is broken, consider the state $\xi_\oplus$ on all wires, after E is applied and before qV is applied on wires $(\mathbf{q}, \mathbf{b}, \mathbf{d})$. Then $\mathbf{q} = (\mathbf{t}, \mathbf{x}, \mathbf{y})$ is such that $\mathbf{x}$ is in the subspace spanned by $\{\ |\,x\rangle : x \in G_\oplus\ \}$. Recall that qV will then accept only if the measurement $\{\ |\,\mathbf{c}_{h,b}\rangle\langle\mathbf{c}_{h,b}\,|\,, I - |\,\mathbf{c}_{h,b}\rangle\langle\mathbf{c}_{h,b}\,|\ \}$ on $(\mathbf{x}, \mathbf{y})$ succeeds, where (h, b) are given by the decommitment $\mathbf{d}$ of E. Then we can bound the probability that the measurement succeeds by

$$\langle\xi_\oplus|\left(\sum_{h,b}|\mathbf{c}_{h,b}\rangle\langle\mathbf{c}_{h,b}|\otimes|h,b\rangle\langle b,h|\otimes I\right)|\xi_\oplus\rangle \quad ,$$

where $\sum_{h,b}|\mathbf{c}_{h,b}\rangle\langle\mathbf{c}_{h,b}|$ acts on $(\mathbf{x}, \mathbf{y})$, $|h, b\rangle\langle b, h|$ acts on $\mathbf{d}$, and I acts on all other wires. To simplify notation, we denote from hereon $\Pi_{h,b} := |h, b\rangle\langle b, h| \otimes I$.

Recall that

$$|\mathbf{c}_{h,b}\rangle = 2^{-2\lambda}\sum_{x\in\{0,1\}^{4\lambda}}|x\rangle\,|g_{x,h(x),b}\rangle \quad \text{where } g_{x,h(x),b} := G(h(x)) \oplus x^b.$$

We consider a decomposition of $|\xi_\oplus\rangle$, according to wires $\mathbf{x}, \mathbf{y}$:

$$|\xi_\oplus\rangle = \sum_{x\in G_\oplus, y}\alpha_{x,y}\,|x\rangle\,|y\rangle\,|\tau_{x,y}\rangle \quad ,$$

where $\sum_{x\in G_\oplus,y}|\alpha_{x,y}|^2=1$, $|x\rangle\,|y\rangle$ correspond to $(\mathbf{x},\mathbf{y})$, and $|\tau_{x,y}\rangle$ is a unit vector that corresponds to all other wires.

Then

$$\langle\xi_\oplus|\left(\sum_{h,b}|\mathbf{c}_{h,b}\rangle\langle\mathbf{c}_{h,b}|\otimes\Pi_{h,b}\right)|\xi_\oplus\rangle = 2^{-4\lambda}\sum_{h,b}\left\|\sum_{x\in G_\oplus,y}\alpha_{x,y}\,\langle g_{x,h(x),b}|y\rangle\,\Pi_{h,b}\,|\tau_{x,y}\rangle\right\|^2 \tag{1}$$

$$= 2^{-4\lambda}\sum_{h,b}\left\|\sum_{x\in G_\oplus}\alpha_{x,g_{x,h(x),b}}\Pi_{h,b}\,|\tau_{x,g_{x,h(x),b}}\rangle\right\|^2 \tag{2}$$

$$\text{(Cauchy-Schwartz)}\qquad \le 2^{-4\lambda}\sum_{h,b}\left(\sum_{x\in G_\oplus}|\alpha_{x,g_{x,h(x),b}}|^2\right)\left(\sum_{x\in G_\oplus}\|\Pi_{h,b}\,|\tau_{x,g_{x,h(x),b}}\rangle\,\|^2\right) \tag{3}$$

$$\Big(\sum_{x\in G_\oplus,y}|\alpha_{x,y}|^2=1\Big)\qquad \le 2^{-4\lambda}\left(\sum_{x\in G_\oplus,h,b}\|\Pi_{h,b}\,|\tau_{x,g_{x,h(x),b}}\rangle\,\|^2\right) \tag{4}$$

$$= 2^{-4\lambda}\left(\sum_{x\in G_\oplus,b}\sum_{s\in\{0,1\}^\lambda}\sum_{h:h(x)=s}\|\Pi_{h,b}\,|\tau_{x,g_{x,s,b}}\rangle\,\|^2\right) \tag{5}$$

$$\text{(all }\Pi_{h,b}\text{ are orthogonal)}\qquad = 2^{-4\lambda}\left(\sum_{x\in G_\oplus,b}\sum_{s\in\{0,1\}^\lambda}\|\sum_{h:h(x)=s}\Pi_{h,b}\,|\tau_{x,g_{x,s,b}}\rangle\,\|^2\right) \tag{6}$$

$$\Big(\sum_{h:h(x)=s}\Pi_{h,b}\le I\Big)\qquad \le 2^{-4\lambda}\left(\sum_{x\in G_\oplus,b}\sum_{s\in\{0,1\}^\lambda}\|\,|\tau_{x,g_{x,s,b}}\rangle\,\|^2\right) \tag{7}$$

$$(\|\,|\tau_{x,g_{x,s,b}}\rangle\,\|=1)\qquad \le 2^{-4\lambda}\cdot|G_\oplus|\cdot 2\cdot 2^\lambda \tag{8}$$

$$(\,|G_\oplus|\le 2^{2\lambda})\qquad \le 2^{-\lambda+1}\ . \tag{9}$$

□

This completes the proof of Proposition 4.3. □

Proposition 4.4. *The scheme is computationally hiding.*

Our proof relies on the following two theorems by Zhandry. (The actual theorems are more general, here we state specific, simpler, versions that suffice for our needs.)

Theorem 4.2 ([Zha12b])**.** *Let A be an oracle-aided quantum circuit making one quantum query to an oracle $f:X\to Y$, then for any distribution D on functions f, and pure state $\mathbf{z}$ the quantity $\Pr_{f\leftarrow D}[A^f(\mathbf{z})=1]$ is a linear combination of the quantities $\Pr_{f\leftarrow F}[f(x_1)=y_1,f(x_2)=y_2]$ for all possible settings of x_1,y_1,x_2,y_2.*

Theorem 4.3 ([Zha12a])**.** *Let $G:\{0,1\}^\lambda\to\{0,1\}^{4\lambda}$ be a pseudorandom generator. Then the function ensembles $\{\,G(R)\,\}_\lambda$ and $\{\,R'\,\}_\lambda$, where $R:\{0,1\}^{4\lambda}\to\{0,1\}^\lambda$ and $R':\{0,1\}^{4\lambda}\to\{0,1\}^{4\lambda}$ are random functions, are computationally indistinguishable quantumly.*

Proof of Proposition 4.4. Our goal is to prove that

$$2^{-2\lambda}\sum_{x\in\{0,1\}^{4\lambda}}|x\rangle\,|G(h(x))\rangle \approx 2^{-2\lambda}\sum_{x\in\{0,1\}^{4\lambda}}|x\rangle\,|G(h(x))\oplus x\rangle\ ,$$

where $h \leftarrow H_{4\lambda,\lambda}$ is a random pairwise independent function.

Since H is pairwise independent, for any $x_1, y_1, x_2, y_2 \in \{0,1\}^{4\lambda}$ and $b \in \{0,1\}$,

$$\Pr_{h \leftarrow H_{4\lambda,\lambda}}[G(h(x_1)) \oplus x_1^b = y_1, G(h(x_2)) \oplus x_2^b = y_2] = \Pr_{R \leftarrow \mathcal{F}_{4\lambda,\lambda}}[G(R(x_1)) \oplus x_1^b = y_1, G(R(x_2)) \oplus x_2^b = y_2] \ ,$$

where $\mathcal{F}_{3n,n}$ is the set of all functions $\{0,1\}^{4\lambda} \to \{0,1\}^{\lambda}$. It then follows from Theorem 4.2 that for any $b \in \{0,1\}$,

$$2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |G(h(x)) \oplus x^b\rangle \equiv 2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |G(R(x)) \oplus x^b\rangle \ ,$$

where $h \leftarrow H_{4\lambda,\lambda}$ and $R \leftarrow \mathcal{F}_{4\lambda,\lambda}$. Indeed, note that each of the above states can be constructed with one quantum query to the oracles $x \mapsto G(h(x)) \oplus x^b$ and $x \mapsto G(R(x)) \oplus x^b$, respectively.

By Theorem 4.3,

$$2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |G(R(x))\rangle \approx 2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |R'(x)\rangle \ , \tag{10}$$

where $R' \leftarrow \mathcal{F}_{4\lambda,4\lambda}$.

Applying bit-wise CNOT (which is efficient and reversible) over the registers in Eq. (10), we have

$$2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |G(R(x)) \oplus x\rangle \approx 2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |R'(x) \oplus x\rangle \ .$$

It is left to note that $R'(x)$ and $R'(x) \oplus x$ are identically distributed for all x if R' is a random function, and hence

$$2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |R'(x)\rangle \equiv 2^{-2\lambda} \sum_{x \in \{0,1\}^{4\lambda}} |x\rangle \, |R'(x) \oplus x\rangle \ .$$

This concludes the proof. □

5 Classical Binding is Impossible with Statistical Hiding

In this section we show that classical binding, even in a computational sense, is not possible for statistically hiding commitments. Intuitively, since the view of the receiver is independent of the bit committed to by the sender, performing measurements on the side of the receiver cannot "force" the sender to collapse to a commitment of either 0 or 1. We believe that a formal argument is still required and it is thus provided below. Our techniques are somewhat similar to those used to show the impossibility of quantum commitments that are both statistically hiding and statistically binding [May97, LC97].

The attack we have in mind is simply of a malicious sender that generates a superposition over the committed bit b, i.e. $(|0\rangle + |1\rangle)/\sqrt{2}$, and executes the honest commitment protocol controlled by the bit b as the committed bit. Finally during the opening phase, the sender measures the bit b to collapse its state and opens accordingly. We show that even conditioned on any specific outcome of any possible measurement of the client's state, the sender's measurement of b still yields both values 0 and 1 with probability close to $1/2$ each, and therefore classical binding does not hold. (Note that this attack is efficiently implementable.)

Theorem 5.1. *Consider an ϵ-statistically hiding commitment scheme. Then there exists a sender that can produce an opening that is accepted by the receiver with the same probability as an honest opening, and which has the following property. Even conditioning on the output of any measurement performed by the receiver in the commitment phase, the distribution of the opening $(b, \mathbf{d}_b)$ is such that the marginal of b is statistically close to uniform. Formally it holds that*

$$\mathbb{E}_x\left[\left|\mathbb{E}_b[(-1)^b]\right|\right] \leq \epsilon \ , \tag{11}$$

where the first expectation is over the value x measured by the receiver and the second is over the measurement of the register b.

Note that via a Markov argument, Eq. (11) implies that with all but $\sqrt{\epsilon}$ probability over the receiver's measurement, the marginal of b is within $\sqrt{\epsilon}$ statistical distance from uniform.

Proof. Assume w.l.o.g that in the commitment phase, the receiver defers all measurements until the end of the experiment, and that the sender performs no measurements at all. Note that if the theorem holds in this case, it also holds in general since we consider classical binding with respect to the receiver's state at the end of the commitment phase, and we require that it holds against arbitrary senders (including ones that are purified).

Let $\mathcal{S}_b$ be an honest sender for the commitment scheme that commits to a bit b, as explained above, we assume that $\mathcal{S}_b$ is purified. We now consider a sender $\mathcal{S}^*$ defined as follows. It starts by generating a register $\mathbf{b} = |+\rangle$, and then executes $\mathcal{S}_b$ controlled by the value $\mathbf{b}$, namely it runs commitments to 0 and 1 in superposition. After the end of the commitment phase and some arbitrary set of measurements performed by the receiver, the value $(b, \mathbf{d}_b)$ is produced by measuring the variable $\mathbf{b}$ together with the register containing the decommitment of $\mathcal{S}_b$. By the correctness of the scheme, the opening $(b, \mathbf{d}_b)$ will be accepted by the receiver.

It remains to analyze the marginal distribution of the value b produced by the attacker, conditioned on the outcome of an arbitrary measurement by the receiver. We let $((\mathbf{b}, \mathbf{s}), \mathbf{t})$ denote the joint state of the sender and receiver after the end of the commitment phase but before the receiver performs any measurements.

We now consider the following experiment: trace out the $\mathbf{s}$ register, apply an arbitrary (possibly partial) measurement $\mathcal{M}$ on the $\mathbf{t}$ register to obtain a bit value v, and measure the $\mathbf{b}$ register in the computational basis to obtain a bit b. Return the value $(-1)^{b+v}$. We note that the measurement on $\mathbf{t}$ which produces v commutes with the measurement on b. The expected value of this experiment is therefore $\mathbb{E}_v[(-1)^v \mathbb{E}_b[(-1)^b]]$ or alternatively $\mathbb{E}_b[(-1)^b \mathbb{E}_v[(-1)^v]]$.

We show that: (i) there exists $\mathcal{M}$ such that the value of the experiment is $\mathbb{E}_x[|\mathbb{E}_b[(-1)^b]|]$ as in the theorem statement. (ii) The maximum value of the experiment over all $\mathcal{M}$ is ϵ, even in absolute value. Combining the two, the theorem will follow.

Starting with property (i), consider a measurement $\mathcal{M}$ on $\mathbf{t}$ that produces v as follows. First, perform the same measurement that the classical binding receiver performs, let x be the classical output of this measurement. Based on the value of x, consider the marginal distribution of b (conditioned on knowing x) and let v be the best predictor for the value of b (i.e. v is the most likely value that b takes). Note that the computation of v is not necessarily efficient, however we are now describing a thought experiment. Using this definition of the measurement and the value v, the expected value of the experiment is exactly $\mathbb{E}_x[|\mathbb{E}_b[(-1)^b]|]$, since by definition of v as the best predictor, $(-1)^v$ has the same sign as $\mathbb{E}_b[(-1)^b]$ (all conditioned on x).

As for property (ii), for every measurement $\mathcal{M}$, consider the following distinguisher between the reduced states of $\mathbf{t}$ conditioned on $b = 0$ and $\mathbf{t}$ conditioned on $b = 1$ as follows. Perform the measurement $\mathcal{M}$ on $\mathbf{t}$ to obtain v and output v as the distinguisher output. The distinguishing gap of this distinguisher is $\left|\mathbb{E}_b[(-1)^b \mathbb{E}_v[(-1)^v]]\right|$. It follows that for any $\mathcal{M}$, the value of the experiment (even in absolute value) cannot exceed the trace distance between the aforementioned reduced states, which is ϵ since the commitment scheme is ϵ-statistically hiding. □

Acknowledgements

We thank the reviewers of TCC 2021 for their comments

References

[AC02] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In Helmut Alt and Afonso Ferreira, editors, *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings*, volume 2285 of *Lecture Notes in Computer Science*, pages 323–334. Springer, 2002.

[BCKM20] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. *CoRR*, abs/2011.13486, 2020.

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, pages 467–496, 2021.

[Blu81] Manuel Blum. Coin flipping by telephone. In Allen Gersho, editor, *Advances in Cryptology: A Report on CRYPTO 81, CRYPTO 81, IEEE Workshop on Communications Security, Santa Barbara, California, USA, August 24-26, 1981*, pages 11–15. U. C. Santa Barbara, Dept. of Elec. and Computer Eng., ECE Report No 82-04, 1981.

[CDMS04] 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.

[DFR+07] Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, pages 360–378, 2007.

[DMS00] 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.

[FUW+20] Junbin Fang, Dominique Unruh, Jian Weng, Jun Yan, and Dehua Zhou. How to base security on the perfect/statistical binding property of quantum bit commitment? *IACR Cryptol. ePrint Arch.*, 2020:621, 2020.

[GLSV20] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. *CoRR*, abs/2011.14980, 2020.

[GMW86] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design (extended abstract). In *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986*, pages 174–187. IEEE Computer Society, 1986.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[KO09] Takeshi Koshiba and Takanori Odaira. Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In Andrew M. Childs and Michele Mosca, editors, *Theory of Quantum Computation, Communication, and Cryptography, 4th Workshop, TQC 2009, Waterloo, Canada, May 11-13, 2009, Revised Selected Papers*, volume 5906 of *Lecture Notes in Computer Science*, pages 33–46. Springer, 2009.

[KO11] Takeshi Koshiba and Takanori Odaira. Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function, 2011.

[KW00] Alexei Y. Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 608–617, 2000.

[LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410–3413, Apr 1997.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, Apr 1997.

[MP12] Mohammad Mahmoody and Rafael Pass. The curious case of non-interactive commitments - on the power of black-box vs. non-black-box use of primitives. In *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, pages 701–718, 2012.

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *J. Cryptology*, 4(2):151–158, 1991.

[Unr12] 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.

[Unr16a] 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.

[Unr16b] 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.

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.

[YWLQ15] 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.

[Zha12a] Mark Zhandry. How to construct quantum random functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 679–687. IEEE Computer Society, 2012.

[Zha12b] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 758–775. Springer, 2012.