Quantum Advantage in Proof Systems Without Entanglement

Krishna Agaram
University of Illinois Urbana-Champaign, Urbana, IL, USA

Nicholas Spooner
Cornell University, Ithaca, NY, USA

Yuxi Zheng
EPFL, Lausanne, Switzerland

Abstract

The study of interactive proofs in the quantum setting has yielded profound insights in complexity theory and quantum information. A curious feature of these results is that the advantage, in terms of computational power, of quantum models over their classical counterparts is usually due to entanglement phenomena rather than quantum communication with the verifier. For example, it is known that QIP = IP = PSPACE, and QMIP with unentangled provers is equal to NEXP = MIP; on the other hand, MIP* = RE.

In this work we initiate the general study of (quantum) *positional* multi-prover interactive proofs ((Q)PMIP), in which provers and verifiers positioned in space communicate freely save for the constraints imposed by the speed of light. We investigate how the class of languages decidable by (Q)PMIPs depends on the arrangement of the verifiers and (honest) provers. In the case of classical PMIPs, we show a dichotomy: if the arrangement satisfies what we call the "min-ball" condition, then the class is NEXP, otherwise it is PSPACE. We then exhibit an arrangement that *does not* satisfy the min-ball condition for which there is a *quantum* PMIP for EXP in the no pre-shared entanglement model.

Our construction is based on positional cryptography and MIPs with no-signaling soundness. We introduce a new positional primitive, the positional hardcore bit, which allows a pair of spatially separated players to transmit a random bit to a particular location while guaranteeing that it remains strongly unguessable elsewhere.

2012 ACM Subject Classification Theory of computation → Interactive proof systems; Theory of computation → Cryptographic protocols; Theory of computation → Quantum complexity theory

Keywords and phrases Quantum interactive proofs, positional cryptography, multi-prover interactive proofs, no-signaling soundness

Digital Object Identifier 10.4230/LIPIcs.ICALP.2026.6

Category Track A: Algorithms, Complexity and Games

1 Introduction

In this work we initiate the general study of *positional proof systems*. A proof system for a language L is a protocol between one or more provers and verifiers in which, on input x, the provers aim to convince the verifiers that $x \in L$. A positional proof system is a proof system in which the provers and verifiers are situated in some metric space and interact subject to speed-of-light, or *relativistic*, constraints: that is, the time taken for a message to travel from party A to party B is proportional to the distance between A and B.

To the best of our knowledge, positional proof systems were initially proposed by Kilian [8] for the purpose of physically implementing *multi-prover interactive proofs* (MIPs) [3]. In an MIP, a polynomial-time verifier aims to determine membership in a language L with the help of two or more unbounded but untrusted provers, who are not permitted to communicate

53rd International Colloquium on Automata, Languages, and Programming (ICALP 2026).
Editors: Sayan Bhattacharya, Danupon Nanongkai, Michael Benedikt, and Gabriele Puppis;
Article No. 6; pp. 6:1–6:21


Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

with each other. MIPs are very powerful: such proof systems exist for all $L \in \mathbf{NEXP}$ [2]. If the provers are allowed to share quantum entanglement, then this model becomes *incredibly* powerful: one can construct proof systems for **RE**, the class of languages reducible to the halting problem [6].

The most commonly proposed approach for realising an MIP as a positional proof system is to "split" the verifier into two parts V_1 and V_2, which are placed a distance d light-seconds from one another, and place one prover near each verifier. Then, provided each verifier transmits simultaneously and receives a response within d seconds, the response received by V_1 cannot depend on the question sent by V_2, and vice versa. This structure was used in an experimental demonstration of "relativistic" zero-knowledge proof systems with unconditional security [5, 1]. It is important to note that while we specify the positions of the verifiers and *honest* provers, which is important for completeness, for soundness we do not constrain the positions (or number) of malicious provers.

Since the described arrangement of two (honest) provers and two verifiers can securely realise any one-round MIP, we can say that the complexity-theoretic power of this arrangement is **NEXP** (or **RE**, if the provers may share prior entanglement). On the other hand, consider a similar arrangement to the above but with the honest provers placed at distance $d/2$ from their corresponding verifiers. In any proof system with this arrangement, a single malicious prover placed at the midpoint of the two verifiers can simulate the action of the honest provers, and cause the verifiers to accept with the same probability;[1] it follows that the value of the optimal strategy can be computed in **PSPACE**.

Thus, the maximal complexity-theoretic power of a positional proof system depends crucially on the geometry of the arrangement of provers and verifiers. Our primary goal in this work is to characterise this dependency, in both the classical and quantum settings.

1.1 Our results

We formalise positional proof systems via a new notion of (quantum) positional multi-prover interactive proof ((Q)PMIP). We specify an arrangement of provers and verifiers via a *position map* p into a metric space; for the purposes of this introduction we take the latter to be (a discretisation of) the ℓ_2 metric on $\mathbb{R}^3$. We denote by $\mathbf{QPMIP}^{\mathsf{s}}[\mathsf{p}]$ the class of languages decidable by quantum honest provers and verifiers located at the positions in p in the no prior entanglement (no-PE) model, where neither honest nor malicious provers possess pre-shared entanglement, as originally introduced in [9] and [4]. We denote by $\mathbf{PMIP}[\mathsf{p}]$ the corresponding classical class. Our main theorem is the following.

▶ **Theorem 1** (informal). *There exists a position map* p *such that* $\mathbf{PMIP}[\mathsf{p}] = \mathbf{PSPACE}$, *and* $\mathbf{EXP} \subseteq \mathbf{QPMIP}^{\mathsf{s}}[\mathsf{p}]$.

That is, there exists an arrangement of honest provers and verifiers which admits a proof system for **EXP** with quantum communication in the no-PE model, but for which no classical communication proof system exists unless $\mathbf{EXP} = \mathbf{PSPACE}$. Our quantum proof system for **EXP** does not make use of entanglement: in fact, the only quantum capability required is to prepare and measure BB84 states. Our protocol moreover relies on the no-PE assumption for soundness; if malicious provers are allowed to share unbounded prior entanglement, known techniques for instantaneous non-local computation are likely to enable them to "collapse" $\mathbf{QPMIP}^{\mathsf{s}}[\mathsf{p}]$ to **PSPACE** as in the classical setting (though we leave it as an open question to show this).

[1] We assume throughout that local computation is instantaneous.

Our result demonstrates how *no-cloning* can be leveraged as a concrete source of quantum advantage in positional proof systems. In contrast to the classical setting, where information can be freely copied and distributed, quantum information must be split among spatially separated provers in order to satisfy the timing constraints. This idea has been used to obtain position verification and other positional cryptography in the no-PE model [4, 9]. To prove our main result, we introduce a new positional primitive, the *positional hardcore bit*, which we believe may be of independent interest.

▶ **Theorem 2** (Positional hardcore bit, informal)**.** *There exists a positional protocol in the no-PE model where two verifiers can jointly generate a* **positional hardcore bit** *with the following properties:*

- **Completeness:** *the honest prover* P *at the honest position can always make the verifiers accept and compute the hardcore bit at time* t^**.*
- **Positional soundness:** *for any coalition of provers at any positions, if the verifiers accept, then any subset* $\mathcal{S}$ *of these provers cannot guess the hardcore bit before time* $t_{\mathcal{S}} \equiv t^* + \min_{\widetilde{\mathsf{P}} \in \mathcal{S}} \mathsf{d}(\mathsf{P}, \widetilde{\mathsf{P}})$*, i.e. before the time it takes for a prover at the honest position to compute the hardcore bit and then send it to the closest malicious prover in set* $\mathcal{S}$*.*

The proof of security relies on monogamy of entanglement arguments similar to [9], along with the use of strong seeded extractors to reduce the guessing advantage. We describe our construction in more detail in Section 2.3.

We contrast this primitive to quantum position verification, where the goal is to certify the physical location of a prover. In contrast, the PHB allows verifiers to *hide information* from all locations distant from the honest prover for a period of time. The hardcore bit remains unguessable until the time at which a prover located at the honest position would be able to compute the hardcore bit and transmit it to the adversary, which corresponds to the strongest timing guarantee one can hope to achieve in this setting.

2 Technical Overview

We overview the main ideas underlying our results.

2.1 Model and classical dichotomy

Formalizing "arrangements"

In order to formalize the notion of "arrangement" of provers and verifiers, we introduce a position mapping, which maps provers and verifiers to points in a metric space:

▶ **Definition 3** (informal)**.** *Given a metric space* $(\mathcal{X}, \mathsf{d})$*, a set of* $\mathcal{V}$ *of verifiers and a set* $\mathcal{P}$ *of provers, a* **position mapping** *is a function* $\mathsf{p} : \mathcal{V} \cup \mathcal{P} \to \mathcal{X}$*, so that* $\mathsf{p}(\mathsf{V}) \in \mathcal{X}$ *is the "position" assigned to the verifier* $\mathsf{V} \in \mathcal{V}$*, and similarly,* $\mathsf{p}(\mathsf{P}) \in \mathcal{X}$ *is the "position" assigned to the prover* $\mathsf{P} \in \mathcal{P}$*.*

We work in a relativistic setting in which all communication is subject to the speed-of-light constraint. Concretely, a message sent at time t from a party located at $x \in \mathcal{X}$ to a party at $y \in \mathcal{X}$ must be received no earlier than time $t + \mathsf{d}(x, y)$. We formalize this constraint via a *transmission function*, which specifies the recipient of a message and the time at which it is delivered.

In the honest setting, message delivery is straightforward: if the verifier V sends a message towards the honest prover P at time t, then the message is delivered to the prover at time $t + \mathsf{d}(\mathsf{V}, \mathsf{P})$. However, in the malicious setting, messages sent by the verifier may be arbitrarily

intercepted and redirected by malicious provers. To model this behaviour, we introduce a more powerful *malicious transmission function* (see Definition 13), which always delivers verifier messages first to the nearest prover. This modelling choice is without loss of generality: a malicious strategy can always place a prover at every verifier location, ensuring that verifier messages are received in the next time step and can then be forwarded to any other party of the adversary's choosing. We analyse and justify this modelling choice in greater detail in Section 3.2 and Remark 14.

Positional proof systems

We introduce new *positional proof systems*, called (quantum) positional multi-prover interactive proofs ((Q)PMIPs). A (Q)PMIP for a relation $\mathcal{R}$ consists of a set of honest provers and verifiers, a metric space $(\mathcal{X}, \mathsf{d})$, an honest position mapping p, a timeout value T and an output predicate (or measurement in the quantum case) P_{output}.

The protocol proceeds in discrete timesteps. At each timestep $t \in [T]$, provers and verifiers can send messages to each other. These messages are transmitted via the transmission function. At the end of the protocol, the verifiers jointly decide to accept or reject by applying P_{output} to their transcripts.

Completeness says that for any $\mathbb{x} \in \mathcal{L}(\mathcal{R})$, the honest provers at the positions specified by the honest position mapping p will always convince the verifiers, while soundness requires that for any $\mathbb{x} \notin \mathcal{L}(\mathcal{R})$, any number of malicious provers at any positions cannot convince the verifier except with small probability. We give the formal definition in Section 3.3.

We define the "positional" complexity classes $\mathbf{PMIP}[\mathsf{p}]$ (resp. $\mathbf{QPMIP}^{\mathsf{s}}[\mathsf{p}]$) as the set of languages decidable by a PMIP (resp. QPMIP) defined on the metric space $(\mathcal{X}, \mathsf{d})$ with the honest position mapping p. The formal QPMIP definition appears in Definition 18; the PMIP definition is the analogous classical restriction. The term "positional" is reflected in the sense that the size of these complexity classes are dependent on the position mapping p.

Note that in the classical case, all messages are classical so can be copied and broadcasted. In particular, a malicious prover strategy can place a prover at each verifier position and relay the verifier messages to all other parties. In the quantum case however, messages may be quantum states and this is not possible due to no-cloning. This difference leads to a significant separation in the classical and quantum model as we will elaborate on below.

The min-ball condition: dichotomy in the classical case

Fix a verifier V, suppose the distance between V and the nearest honest prover to it is r, then any party that is able to interact with V as quickly as the closest honest prover must be within a ball that is centred at V with radius r. We call this region the *min-ball* of V. The min-ball captures the tightest response window that V can impose: any response that takes time more than $2 \cdot r$ can come from malicious provers outside of the ball, while any faster response is physically impossible for any honest provers.

▶ **Definition 4** (informal)**.** *We say that a position mapping* p *satisfies the* min-ball condition *if there exist two verifiers* $\mathsf{V} \neq \mathsf{V}'$ *such that their min-balls are disjoint.*

With this definition, we can restate the part about PMIP in Theorem 1. What we prove is a stronger result that says the min-ball condition exactly characterizes the dichotomy for classical PMIP:

▶ **Theorem 5** (informal)**.** *For any* p *that satisfies the* min-ball condition*,* $\mathbf{PMIP}[\mathsf{p}] = \mathbf{MIP} = \mathbf{NEXP}$*. Otherwise,* $\mathbf{PMIP}[\mathsf{p}] = \mathbf{IP} = \mathbf{PSPACE}$*.*

Intuitively, the min-ball condition characterizes whether relativistic timing constraints enforce informational independence between verifiers. Each verifier can require responses within a time window determined by the distance to its closest honest prover. If, for every pair of verifiers, information generated near one verifier can reach the other within this window, then timing constraints do not prevent malicious provers from globally sharing all verifier messages. In this case, the PMIP protocol effectively collapses to an IP. Conversely, if there exists a pair of verifiers whose response windows are too short to permit such communication, then the arrangement enforces separation, and the complexity class is as big as **MIP**. In the classical setting, the min-ball condition is precisely the geometric criterion that separates these two regimes.

To formalize this intuition and prove that violation of the min-ball condition implies $\mathbf{PMIP}[\mathsf{p}] = \mathbf{IP}$, we introduce a *canonical interactive proof* (IP). Given a PMIP protocol with T timesteps, we define a T-round IP in which, in each round $t \in [T]$, the IP verifier internally simulates all PMIP verifier at timestep t, while the IP prover internally simulates all PMIP provers at timestep t.

The canonical IP is trivially complete. We then show that it is also sound whenever the min-ball condition is violated. The key observation is that any cheating prover strategy for the canonical IP can be simulated by a coalition of malicious PMIP provers. Even if each PMIP verifier enforces the tightest possible timing constraint by communicating only with its nearest honest prover, violation of the min-ball condition guarantees that there is still sufficient time for information originating at one verifier to reach any other verifier. As a result, a malicious strategy can place a prover at each verifier location; these provers collectively obtain all verifier messages in time (up to known time shifts) and can locally simulate the behavior of a cheating canonical IP prover.

2.2 Quantum advantage

The proof breaks down in the quantum case

The above argument relies on the fact that classical information can be freely copied: a single canonical IP prover can be perfectly simulated by multiple provers placed at the verifier positions. This argument, however, does not carry over to the quantum setting. Even when the min-ball condition is violated, it is in general impossible to simulate multiple spatially separated copies of a single coherent quantum prover, due to the no-cloning principle.

Nevertheless, if all min-balls under position mapping p have a nonempty mutual intersection, then we can show that $\mathbf{QPMIP}^{\mathsf{s}}[\mathsf{p}] = \mathbf{IP}$. Indeed, in this case a single quantum prover located at the intersection point can faithfully simulate a single quantum prover and communicate with all QPMIP verifiers within the required time bounds.

This leaves an intermediate regime of particular interest: the quantum setting in which the min-ball condition is violated, but the min-balls do not admit a common intersection. Understanding the power of QPMIP protocols in this regime is one of the central motivations for our analysis.

A two prover toy example

To provide some intuition on how to obtain a lower bound on $\mathbf{QPMIP}^{\mathsf{s}}[\mathsf{p}]$, we consider a minimal two-prover, one-round setting in the regime of interest, where verifier min-balls pairwise intersect but admit no common intersection, as illustrated in Figure 1. In this configuration, P_1 and P_2 correspond to the two honest provers, and they are exactly at the

intersection of the min-balls for V_1 and V_3, and for V_2 and V_3 respectively. Our goal is to argue that the soundness of some QPMIP construction with parties positioned as in this configuration is upper bounded by the soundness of the underlying MIP.

Recall that in an MIP, soundness relies on the fact that each prover's response is independent of the other prover's query. In the positional setting, however, if V_1 and V_2 were to send the MIP queries in the clear, then a malicious prover placed at the intersection of the min-balls of V_1 and V_2 could receive both queries in time and respond to each verifier with answers that depend on both queries, thereby violating the MIP soundness condition. The two red paths in Figure 1 illustrate a similar attack strategy by malicious provers orchestrating the path so that the response to V_2 depends on the query sent by V_1, made possible because the min-balls of V_1 and V_2 intersect.

This observation shows that MIP queries cannot be transmitted in the clear. Instead, the verifiers must jointly encode each query using an encryption mechanism reminiscent of secret sharing. Crucially, the shares must be distributed so that only a prover located at the honest position can receive all of them early enough to decrypt the query and respond in time.

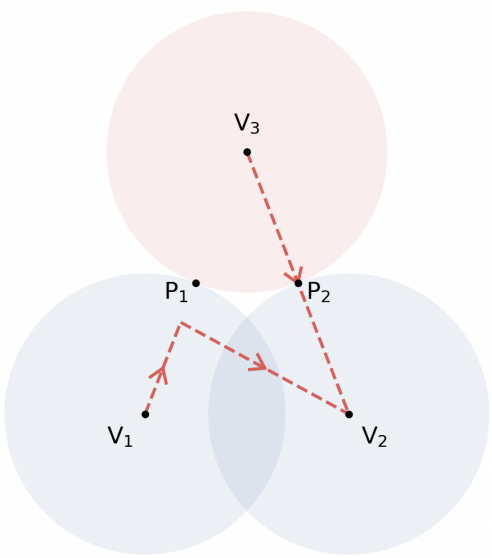

Figure 1 Toy example: a three-verifier two-prover configuration in which the min-ball condition is violated. The red paths illustrate how this violation can be exploited by malicious provers communicating with V_2 in time to make its response depend on the query sent by V_1, which is not allowed in a typical MIP.

An instructive attempt: use position verification

At first glance, the scheme we seek resembles a standard *position verification* (PV) protocol. Recall that in a position verification protocol, the verifiers always accept an honest prover located at the honest position, while no coalition of malicious provers – none of which are at the honest position – can fool the verifier except with small probability. It is known that position verification is impossible in both the classical and quantum settings if malicious provers are allowed to share an unbounded amount of entanglement. However, Buhrman *et al.* [4] showed that secure position verification is achievable in the quantum setting under the no prior entanglement (no-PE) model. Motivated by this result, we likewise restrict our attention to the no-PE model throughout this work.

Position verification protocol from [4].

- The verifiers jointly sample a random challenge string x and a random measurement basis θ, and send the state $H^\theta |x\rangle$ to the honest prover P in a way that they *arrive* at P at the same time t^*.
- P measures the state in basis θ to get an outcome x, and sends x back to both verifiers. Verifiers accept iff. they both receive the correct x.

In Figure 1, suppose that verifiers V_1 and V_3 execute the position verification protocol described above, with P_1 designated as the honest prover. (Symmetrically, V_2 and V_3 may run the same protocol with P_2 as the honest prover; since the two cases are symmetric, we focus on the former.) In this setting, position verification guarantees that only the honest prover P_1 can compute the challenge x at time t^*.

If we were to use such a bit x independently to mask each bit of the MIP query q_1, and have the verifier send the masked query to P_1, then only the honest prover would be able to recover q_1 at time t^*. Moreover, any coalition of provers located elsewhere – in particular, provers positioned so that they can communicate with V_2 starting from time t^* – would be unable to learn anything about q_1 except with small probability, since they cannot compute x in time.

However, this guarantee is insufficient for our purposes. What we require is the substantially stronger condition that no such coalition can learn q_1 at *any* time prior to V_2 receiving its response, that is, before time $t^* + \mathsf{d}(\mathsf{P}_2, \mathsf{V}_2)$. Without additional restrictions, this stronger guarantee does not hold. For example, since the min-ball condition is violated, malicious provers can redirect all messages from V_1 and V_3 directly to V_2 within the required time bounds. In this case, a prover positioned at V_2 can learn the query q_1 in time and produce a response that depends on both queries.

2.3 Constructing Positional Hardcore Bit (PHB) schemes

Defining the positional hardcore bit property

A violation of the min-ball condition allows for communication between malicious provers within the response windows of the verifiers. To circumvent this, we design a cryptographic primitive that can be used to encrypt the MIP queries in a way that no coalition of provers can learn the query value until it is "too late" to coordinate a cheating response to another verifier. We call this primitive a *positional hardcore bit* (PHB) scheme.

▶ **Definition 6** (Positional Hardcore Bit, informal)**.** *A (2-verifier)* positional hardcore bit *scheme is a positional protocol between two verifiers* $\mathsf{V}_1, \mathsf{V}_2$ *and an honest prover* P*, accompanied by a hardcore bit generator* Hb *that takes the verifier messages as input and outputs a bit* b*, such that the following hold:*

- *Completeness:* P *can compute* b *at a fixed time* t^* *and also send responses back in a way that causes the verifiers to accept with high probability.*
- *Positional soundness: If the verifiers accept, then there is no algorithm* $\mathcal{A}$ *that takes as input the state of a coalition of malicious provers* $\widetilde{\mathsf{P}}_1, \ldots, \widetilde{\mathsf{P}}_k$ *at any time prior to* $\hat{t} \equiv t^* + \min_{i=1}^{k} \mathsf{d}(\mathsf{P}, \widetilde{\mathsf{P}}_i)$ *and guesses* b *correctly with probability non-negligibly better than random.*

The soundness condition is the "best possible": the time $\hat{t}$ is exactly the time when a prover at the honest location, having computed b at time t^*, can send b to the closest $\widetilde{\mathsf{P}}_i$. It is therefore impossible to require that the malicious provers not learn b at time $\hat{t}$. It remains to show the existence of this strong positional primitive.

Construction of a two-verifier PHB

It is not clear how to ensure unguessability of b for the period of time asked for in Definition 6; indeed, redirection of messages meant for P to $\widetilde{\mathsf{P}}$ may allow it to learn the bit b at a time prior to $\hat{t}$, which would violate the soundness condition.

The key insight is that we require P to send an acknowledgement of the receipt of their messages in time. A good acknowledgement should depend strongly on a secret hidden in the verifier messages, so that redirection loses the ability to compute the acknowledgement correctly. This property is reminiscent of the monogamy-of-entanglement property that quantum systems possess: if the acknowledgement can be treated as entangled with a secret private to the verifiers, then either the acknowledgement is computable by the honest prover or by the malicious prover (or none of them), but certainly not by both of them. This motivates our construction of a two-verifier PHB scheme based on the monogamy-of-entanglement game introduced by Tomamichel et al. [9].

Connection to the monogamy-of-entanglement game

A *monogamy-of-entanglement game* consists of a referee Alice and two non-communicating players Bob and Charlie.

Monogamy-of-entanglement (MoE) game, informal.

- Bob and Charlie pre-prepare a state ρ_{ABC} and send register A to Alice. Bob keeps register B and Charlie keeps register C.
- Alice measures A using a randomly chosen measurement $\mathcal{N}^\theta$, reveals θ, and Bob and Charlie attempt to independently guess the measurement outcome of A using their respective registers B and C.
- The game is won iff both guesses are equal to Alice's measurement outcome.

It is clear that the correlation of measurement outcomes provided by entangling A with B (resp. C) in ρ_{ABC} helps Bob (resp. Charlie) guess Alice's measurement outcome correctly. However, the monogamy-of-entanglement property says, that A cannot be perfectly correlated with both B and C at the same time: indeed, the game cannot be won with probability more than $\cos^2(\pi/8) = 1/2 + 1/2\sqrt{2}$ [9]. Further, the game can be repeated in parallel to amplify the hardness of winning exponentially: measuring ζ qubits independently in random bases and requiring Bob and Charlie to guess all measurement outcomes correctly reduces the winning probability to $(1/2 + 1/2\sqrt{2})^\zeta$ [9], which is negligibly small in ζ. This parallel repetition property is crucial for our construction, as it allows us to amplify the hardness of guessing the measurement outcomes to the point where we can extract a bit that is arbitrarily close to uniform from the measurement outcomes, even conditioned on any quantum side-information the malicious coalition may have about the measurement outcomes.

It turns out that a uniformly sampled hash function[2] from a 1-universal hash family suffices for this from the leftover hash lemma. We can then use the extracted bit as the hardcore bit b in Definition 6 and the measurement outcomes as the acknowledgement: guessing b requires guessing all the measurement outcomes, and sending the acknowledgement correctly also

[2] We would need to send also the seed used to generate the hash function as part of the verifier messages for the honest prover to compute said bit; this does not affect the MoE analysis since the seed is independent of the distribution of measurement outcomes.

requires guessing all the measurement outcomes. The monogamy-of-entanglement property then guarantees that up to negligible probability, exactly one of the two can be done, which is exactly what we need for the soundness property. Here is the full hardcore bit protocol for two-verifiers (say V_1 and V_2 in the toy example).

Two-verifier hardcore bit generation, informal.

- The verifiers V_1 and V_2 jointly sample random strings $x_1, \cdots, x_\zeta$ and measurement bases $\theta_1, \cdots, \theta_\zeta$. They also jointly sample a random seed s of appropriate length that fixes a 1-universal hash function $f_s : \{0,1\}^\zeta \to \{0,1\}$.
- V_1 sends ζ qubits in state $\otimes_i H^{\theta_i} |x_i\rangle$ and V_2 sends (θ, s), both to the honest prover P, in a way that both messages *arrive* at P at the same time t^*.
- P measures each qubit i in basis θ_i to obtain the mask $x_1, \cdots, x_\zeta$ and sends back x to V_2 as acknowledgement.
- V_1 and V_2 check that the acknowledgement is received correctly and in time; if so, they accept, and reject otherwise.

Note that the honest parties in this protocol only prepare and measure single-qubit states. The soundness analysis of the protocol can be reduced to the analysis of a related monogamy-of-entanglement game via a standard purification technique.

Proof sketch

The analysis of the soundness of this hardcore bit protocol comprises two key steps. The first is the establishment, via the parallel-repeated MoE game and properties of seeded extractors, of a negligible upper bound on the advantage that an adversarial coalition has in guessing the hardcore bit b when the malicious prover $\widetilde{\mathsf{P}}$ may be treated as one of the two guessing parties in the MoE game and the systems responsible for generating the acknowledgement as the other. Parallel repetition soundness is then shown to imply that the malicious prover's min-entropy of the measurement outcome x conditioned on its own quantum systems is large enough for the extracted bit b to be sufficiently close to uniform conditioned on the same quantum systems via the leftover hash lemma.

The second step is to show via geometry and timing analysis that a coalition of malicious provers can indeed be treated as one guessing party in the MoE game and the systems generating the acknowledgement the other guessing party. In particular, we need to show that the action of these two parties in the QPMIP is equivalent to them independently performing POVM measurements independently on an appropriate ρ_{ABC} with A, B and C (with A comprising the "virtual" halves of the Bell pairs that V_1 holds, and B, C naturally comprising the malicious prover and honest prover's quantum systems respectively) independent of the verifier message (θ, s).

A useful insight is that by the triangle inequality, the split between the systems that comprise the malicious provers's qubits and those that generate the acknowledgement must be done ahead of time t^*, which forces the split of B and C to be independent of (θ, s). Of course, it is crucial, since the two guessing parties must work independently in the MoE game, to show that after time t^*, the rest of the QPMIP messaging can be simulated by each of them independently in a way that preserves the distribution of messages received by the coalition and that of the acknowledgement.

2.4 Putting it all together to lower-bound QPMIP

No-signaling strategies

The soundness of a one-round MIP relies on the independence of each response from queries sent to other provers. In our situation, the PHB scheme allows us to enforce *statistical* near-independence in the sense of δ-no-signaling: the response to V_2 can depend on q_1, as long as it does not depend on q_1 in a way that allows V_2 to guess q_1 with non-negligible probability. Thus, we are able to show that $\mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathrm{d})}[\mathsf{p}]$ contains every language recognisable by no-signaling MIPs, which are MIPs with soundness guaranteed against such no-signaling strategies. Since the class of languages decidable by no-signaling MIPs is **EXP** [7], which is believed to be larger than **PSPACE**, this relaxation still demonstrates a quantum advantage: $\mathbf{MIP}^{\mathsf{ns}} = \mathbf{EXP} \subseteq \mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathrm{d})}[\mathsf{p}]$. Our proof techniques do not enable us to use standard MIP soundness, which would yield $\mathbf{NEXP} \subseteq \mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathrm{d})}[\mathsf{p}]$; we leave it as an open question to determine the precise complexity of $\mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathrm{d})}[\mathsf{p}]$.

Proof strategy

Consider a language $\mathcal{L}$ decidable by a k-prover one-round MIP with no-signaling soundness ϵ_{MIP}; the set of such languages is known to be **EXP** [7]. We construct a QPMIP for the same language $\mathcal{L}$ with the same number of provers and a position mapping that *violates* the min-ball condition; the position mapping is a ready generalization of Figure 1. The QPMIP verifiers run independent positional hardcore bit schemes in parallel, one for every bit j of every MIP query q_i; each hardcore bit $b_{i,j}$ is used to encrypt, via XOR, the corresponding query bit q_i^j, yielding masked bits $m_{i,j} = b_{i,j} \oplus \mathsf{q}_i^j$. The masked bits are then sent to the honest provers and a response to the MIP queries is requested at the earliest time that the honest provers can receive the appropriate verifier messages, decrypt the MIP queries, and send back the MIP responses.

Completeness of the QPMIP for instances in $\mathcal{L}$ is straightforward: the honest provers can compute the hardcore bits and decrypt the MIP queries in time, and respond to the MIP queries in a way that causes the verifiers to accept. The soundness analysis is as follows: for any malicious QPMIP prover strategy, we can define a corresponding colluding malicious MIP prover strategy that simply runs the QPMIP strategy and responds to the MIP queries according to the responses that the QPMIP verifiers receive in this run; clearly, the success probability of this MIP strategy is the same as that of the QPMIP strategy given that the acknowledgements all arrive. We then argue that it must be one of the two cases: either the MIP strategy thus formed is no-signaling, in which case the QPMIP strategy wins with at most ϵ_{MIP} probability, or an acknowledgement is not received correctly in time, in which case the QPMIP verifiers reject anyways. This property is guaranteed by the positional hardcore bit schemes that the verifiers run in parallel; in particular, we narrow down via a hybrid argument to one particular hardcore bit $b_{i,j}$ whose soundness is contradicted when the MIP strategy is signaling.

3 Quantum Positional MIP

In this section, we first introduce a general model called the *timed quantum communication protocol* in Section 3.1, which models multiple quantum parties communicating with each other over time. Later, we additionally model how messages takes time to travel in space, which is captured formally by a "positional transmission function" defined in Section 3.2. Equipped with these definitions, we define a "positional" proof system: *Quantum Positional Multi-Prover Interactive Proof* (QPMIP), which is a "positional" analogue of the usual MIP, and its corresponding complexity classes in Section 3.3.

3.1 Timed quantum communication protocol and game

▶ **Definition 7** (timed quantum communication protocol). *A N-party* **timed quantum communication protocol** *is given by a tuple* $\mathsf{tQCP} = (T, \Lambda, \{\mathsf{Q}_i\}_{i\in[N]}, P_{\text{output}})$*, where*

- T *is a* **timeout value**, *which bounds the total number of timesteps.*
- Λ *is a* **transmission function**, *which takes inputs $i, j \in [N]$, $t \in [T]$ and outputs $t' \in T$, $j' \in [N]$. $\Lambda(i,j,t) = (j',t')$ denotes that a message sent by party i at time t, intended for party j, is available at time t' to party j'. If such a message is never available to any party we define $\Lambda(i,j,t) := \perp$.*
- *For every $i \in [N]$, $\mathsf{Q}_i = (\Phi_i^{(1)}, \ldots, \Phi_i^{(T)})$ is a* **party** *which:*
  - *has access to the registers:*
    - $\left\{M_{i\to j}^{(t)}\right\}_{t\in[T], j\in[N], j\neq i}$, *where $M_{i\to j}^{(t)}$ is used for sending messages to the j-th party at time t. All message registers are initialized to $|\perp\rangle$.*
    - *I_i, an internal register initialized to some initial state.*
  - *follows a* **strategy** *described by a sequence of quantum channels $\Phi_i^{(1)}, \ldots, \Phi_i^{(T)}$, where:*
    - *For every $t \in [T]$, $\Phi_i^{(t)}$ is a CPTP map:*

$$\Phi_i^{(t)} : \mathcal{D}\left(\left(\bigotimes_{\substack{t'\in[T],\, j,i'\in[N] \\ \Lambda(j,i',t')=(i,t)}} \mathcal{H}_{M_{j\to i'}^{(t')}}\right) \otimes \mathcal{H}_{I_i}\right) \to \mathcal{D}\left(\left(\bigotimes_{j\neq i} \mathcal{H}_{M_{i\to j}^{(t)}}\right) \otimes \mathcal{H}_{I_i}\right) .$$

- P_{output} *is a projective measurement $\{N_x\}_x$ on the joint system of all parties' internal registers: $\mathcal{H}_I := \bigotimes_{i\in[N]} \mathcal{H}_{I_i}$.*

▶ **Definition 8** (timed quantum communication game). *Given an input state $\boldsymbol{\rho}_{\text{in}}$ on $\mathcal{H}_I := \bigotimes_{i\in[N]} \mathcal{H}_{I_i}$ (may be entangled across parties) and a timed quantum communication protocol $\mathsf{tQCP} = (T, \Lambda, \{\mathsf{Q}_i\}_{i\in[N]}, P_{\text{output}})$, the* **timed quantum communication game** *$\Gamma(\boldsymbol{\rho}_{\text{in}}, \mathsf{tQCP})$ is defined as follows:*

$\Gamma(\boldsymbol{\rho}_{\text{in}}, \mathsf{tQCP})$:

1. *Initialize the joint system of all parties' internal registers $I_1 \cdots I_N$ to $\boldsymbol{\rho}_{\text{in}}$.*
2. *For every timestep $t \in [T]$, do the following:*
   - *For every $i \in [N]$:*
     - *Apply $\Phi_i^{(t)}$ to the message registers $\left\{M_{j\to i'}^{(t')}\right\}_{\substack{t'\in[T], j,i'\in[N] \\ \Lambda(j,i',t')=(i,t)}}$ and internal register I_i and output to the message registers $\left\{M_{i\to j}^{(t)}\right\}_{j\neq i}$ and I_i.*
3. *Perform joint measurement P_{output} on all parties' internal registers $\{I_i\}_{i\in[N]}$ and output the measurement outcome.*

Throughout this paper, we use some additional notations and more intuitive descriptions about timed quantum communication protocols and quantum positional games. We elaborate on their formal meanings below:

- For every timestep $t \in [T]$, we denote by $\boldsymbol{\rho}_i^{(t)}$ the state of party i's internal register I_i after applying $\Phi_i^{(t)}$.
- *Party i sends a message to party j at time t* means that the map $\Phi_i^{(t)}$ outputs a non-$|\perp\rangle$ state to the message register $M_{i\to j}^{(t)}$.
- *Party j receives a message from party i at time t* means that the transmission function $\Lambda(i,j',t') = (j,t)$ for some $j' \in [N]$ and $t' \in [T]$.

- *Message registers available to party i at time t* refers to the set $\left\{M_{j\to i'}^{(t')}\right\}_{\substack{t'\in[T],j,i'\in[N]\\ \Lambda(j,i',t')=(i,t)}}$, and a *message is sent / available to party i at time t* means that the message is contained on registers in this set.

▶ Remark 9. Due to no-cloning, in general a quantum message can only be received by at most one party, which is reflected in the definition of the transmission function. Of course, a party may broadcast a classical or clonable message in our model by placing copies on multiple message registers.

3.2 Positional transmission functions

Two types of parties: provers and verifiers

For the timed quantum communication protocols we consider in this paper, it is useful to think of parties as "provers" and "verifiers". The provers jointly try to prove some statement (i.e. an instance being in a relation) by answering the verifier queries. At the end of the protocol, the verifiers jointly decide whether to accept or reject.

In particular, we consider $(\mathsf{l}+\mathsf{k}')$-party timed quantum communication protocols in which we partition the parties into verifiers $\mathcal{V} \coloneqq \{\mathsf{V}_i\}_{i\in[\mathsf{l}]}$ and (honest or malicious) provers $\mathcal{P} \coloneqq \{\widetilde{\mathsf{P}}_i\}_{i\in[\mathsf{k}']}$. When convenient we will sometimes associate $\mathcal{V}$ with the set $[\mathsf{l}]$ and $\mathcal{P}$ with the set $[\mathsf{l}+1,\mathsf{l}+\mathsf{k}']$. Since there is a one-to-one mapping between parties and the indices, we use the two interchangeably.

We also rewrite the timed quantum communication protocol tuple as:

$$\mathsf{tQCP} = (T, \Lambda, \{\mathsf{V}_i\}_{i\in[\mathsf{l}]}, \{\widetilde{\mathsf{P}}_i\}_{i\in[\mathsf{k}']}, P_{\mathsf{output}}) \ ,$$

in order to distinguish between these two types of parties.

Position mapping

In order to define a proof system that considers provers and verifiers in different arrangements, we introduce a metric space and imagine provers and verifiers at different positions in the metric space. More formally, the proof system additionally depends on the following two ingredients:

- $(\mathcal{X}, \mathsf{d})$ is a discrete *metric space*, equipped with an integer-valued metric d on $\mathcal{X}$, i.e., a function $\mathsf{d} : \mathcal{X}\times\mathcal{X} \to \mathbb{Z}_{\geq 0}$.
- $\widetilde{\mathsf{p}}$ is an (honest or malicious) *position mapping* from: $\mathcal{V}\cup\mathcal{P} \to \mathcal{X}$ that maps each party to an element in $\mathcal{X}$. For every $\mathsf{Q}\in\mathcal{V}\cup\mathcal{P}$, $\widetilde{\mathsf{p}}(\mathsf{Q})$ is the "position" assigned to party Q.

As a shorthand, we denote the distance between two parties $\mathsf{Q}_i, \mathsf{Q}_j \in \mathcal{V}\cup\mathcal{P}$ under the position map $\widetilde{\mathsf{p}}$ as

$$\mathsf{d}_{\widetilde{\mathsf{p}}}(\mathsf{Q}_i, \mathsf{Q}_j) \coloneqq \mathsf{d}(\widetilde{\mathsf{p}}(\mathsf{Q}_i), \widetilde{\mathsf{p}}(\mathsf{Q}_j)) \ .$$

When the position mapping is clear from context, we drop it in the notation and simply write $\mathsf{d}(\mathsf{Q}_i, \mathsf{Q}_j)$.

▶ Remark 10. We assume without loss of generality that there is at most one prover and one verifier at each point in $\mathcal{X}$, i.e. any position mapping $\widetilde{\mathsf{p}}$ we consider is such that $\bigwedge_{\mathsf{V},\mathsf{V}'\in\mathcal{V},\mathsf{V}\neq\mathsf{V}'} \mathbb{1}\left[\widetilde{\mathsf{p}}(\mathsf{V}) \neq \widetilde{\mathsf{p}}(\mathsf{V}')\right]$ and $\bigwedge_{\mathsf{P},\mathsf{P}'\in\mathcal{P},\mathsf{P}\neq\mathsf{P}'} \mathbb{1}\left[\widetilde{\mathsf{p}}(\mathsf{P}) \neq \widetilde{\mathsf{p}}(\mathsf{P}')\right]$. Since two provers (verifiers) at the same position can always be simulated by one prover (verifier) at the same position.

Positional transmission functions

Recall that the transmission function Λ is such that if $\Lambda(i, j, t) = (j', t')$ then a message sent by party i at time t, intended for party j, is available at time t' to party j' (and is $\perp$ if there is no such t', j'). Note that although we defined the transmission function in Definition 7 where i, j, j' are all party indices. Since there is a one-to-one mapping between the party indices and the parties, so in the following, we assume that the transmission function is of the form $\Lambda(\mathsf{Q}_i, \mathsf{Q}_j, t) = (\mathsf{Q}_{j'}, t')$ where $\mathsf{Q}_i, \mathsf{Q}_j, \mathsf{Q}_{j'}$ are parties in $\mathcal{P} \cup \mathcal{V}$.

In the following, we define transmission functions for positional interactions based on the principle that the time it takes for a message to travel between two parties is proportional to the distance between them. More formally, we define a *positional transmission function* $\Lambda_{(\mathcal{X},\mathsf{d}),\mathsf{p}}$, which depends on the discrete metric space $(\mathcal{X}, \mathsf{d})$ and the position mapping p that maps parties to $\mathcal{X}$.

Intuitively, the positional transmission function $\Lambda_{(\mathcal{X},\mathsf{d}),\mathsf{p}}$ should work as follows: After party Q_i sends a message to party Q_j's direction at time t, party Q_j should receive it at time $t + \mathsf{d}_\mathsf{p}(\mathsf{Q}_i, \mathsf{Q}_j)$. This intuition is precisely captured by the following definition of the *unrestricted transmission function*:

▶ **Definition 11.** *Given a set of verifiers $\mathcal{V}$ and a set of provers $\mathcal{P}$, metric space $(\mathcal{X}, \mathsf{d})$, and a position mapping $\mathsf{p} : \mathcal{V} \cup \mathcal{P} \to \mathcal{X}$, for every $\mathsf{Q}_i, \mathsf{Q}_j \in \mathcal{V} \cup \mathcal{P}$ such that $\mathsf{Q}_i \neq \mathsf{Q}_j$, and every $t \in [T]$, we define the* **unrestricted transmission function** *$\Lambda_{(\mathcal{X},\mathsf{d}),\mathsf{p}}$ as follows:*

$$\Lambda_{(\mathcal{X},\mathsf{d}),\mathsf{p}}(\mathsf{Q}_i, \mathsf{Q}_j, t) = \begin{cases} (\mathsf{Q}_j, t') & \text{if } t' \in [T] \wedge t' = t + \mathsf{d}_\mathsf{p}(\mathsf{Q}_i, \mathsf{Q}_j) \\ \perp & \text{otherwise} \end{cases},$$

i.e. a message sent by party Q_i at time t is transmitted to the intended party Q_j at time t' iff. $t' = t + \mathsf{d}_\mathsf{p}(\mathsf{Q}_i, \mathsf{Q}_j)$, and it equals $\perp$ otherwise.

Our results in the quantum setting consider prover strategies with **no pre-shared entanglement**. In particular, we work in the No-PE (no pre-shared entanglement) model introduced in [4, 9], which requires that a prover (even if malicious) send no message before it is able to receive a message from a verifier. We define the honest transmission functions under this model below:

▶ **Definition 12.** *Given a set of verifiers $\mathcal{V}$ and a set of provers $\mathcal{P}$, metric space $(\mathcal{X}, \mathsf{d})$, and a position mapping $\mathsf{p} : \mathcal{V} \cup \mathcal{P} \to \mathcal{X}$, for every $\mathsf{Q}_i, \mathsf{Q}_j \in \mathcal{V} \cup \mathcal{P}$ such that $\mathsf{Q}_i \neq \mathsf{Q}_j$, and every $t \in [T]$, we define a* **(separable) honest transmission function** *$\Lambda^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}}$ as follows:*

$$\Lambda^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}}(\mathsf{Q}_i, \mathsf{Q}_j, t) = \begin{cases} \Lambda_{(\mathcal{X},\mathsf{d}),\mathsf{p}}(\mathsf{Q}_i, \mathsf{Q}_j, t) & \text{if } \mathsf{Q}_i \in \mathcal{V} \vee t \geq \min_{\mathsf{V} \in \mathcal{V}} \mathsf{d}_\mathsf{p}(\mathsf{Q}_i, \mathsf{V}) \\ \perp & \text{otherwise} \end{cases},$$

Furthermore, we define a **separable and isolated honest transmission function** *that disallow prover-to-prover communication as follows:*

$$\Lambda^{\mathsf{si}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}}(\mathsf{Q}_i, \mathsf{Q}_j, t) = \begin{cases} \Lambda^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}}(\mathsf{Q}_i, \mathsf{Q}_j, t) & \text{if } \mathsf{Q}_i \in \mathcal{V} \vee \mathsf{Q}_j \in \mathcal{V} \\ \perp & \text{otherwise} \end{cases}.$$

However, things are more complicated if the provers are malicious: if we use a "directional" transmission function similar to the honest case, intuitively, it means that the verifiers are sending messages to a direction of their choice, i.e. having an intended receiving party. But since malicious provers may intercept and redirect any verifier messages, they can be transmitted to any party, regardless of who the intended receiver is.

To better capture the behavior of malicious provers, our malicious transmission function always transmits the verifier messages to the nearest malicious prover. This assumption is justified since for any malicious prover strategy under the "directional" transmission function, we can construct an equivalent one under our transmission function: we add a malicious prover at every verifier position so that the verifier messages will always be sent to these provers first. They can then forward the verifier messages to any party of their choice. For compatibility with the honest case, verifier messages still have an intended receiver, which is ignored.

Formally, we define the *malicious transmission function* as follows:

▶ **Definition 13.** *Given a set of verifiers $\mathcal{V}$ and a set of provers $\mathcal{P}$, metric space $(\mathcal{X}, \mathsf{d})$, and a position mapping $\widetilde{\mathsf{p}} : \mathcal{P} \cup \mathcal{V} \to \mathcal{X}$, for every $\mathsf{Q}_i, \mathsf{Q}_j \in \mathcal{P} \cup \mathcal{V}$ such that $\mathsf{Q}_i \neq \mathsf{Q}_j$, and every $t \in [T]$, we define a* **(separable) malicious transmission function** $\widetilde{\Lambda}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\widetilde{\mathsf{p}}}$ *as follows:*

$$\widetilde{\Lambda}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\widetilde{\mathsf{p}}}(\mathsf{Q}_i, \mathsf{Q}_j, t) = \begin{cases} \Lambda_{(\mathcal{X},\mathsf{d}),\widetilde{\mathsf{p}}}(\mathsf{Q}_i, \mathsf{Q}^*, t) \text{ if } \mathsf{Q}_i \in \mathcal{V} \wedge \mathsf{Q}^* = \arg\min_{\mathsf{Q} \in \mathcal{P} \cup \mathcal{V}} \mathsf{d}_{\widetilde{\mathsf{p}}}(\mathsf{Q}_i, \mathsf{Q}) \\ \Lambda_{(\mathcal{X},\mathsf{d}),\widetilde{\mathsf{p}}}(\mathsf{Q}_i, \mathsf{Q}_j, t) \text{ if } \mathsf{Q}_i \in \mathcal{P} \end{cases},$$

i.e. if party Q_i is a verifier, then a message sent by party Q_i at time t is transmitted to the nearest party Q^* according to the unrestricted transmission function. If party Q_i is a prover, then the message is transmitted to the intended party Q_j according to the unrestricted transmission function.

▶ Remark 14. The malicious transmission function defined above is more general than the honest one. In particular, for any prover strategy $\{\widetilde{\mathsf{P}}_i\}_{i\in[\mathsf{k}]}$, its behavior under the honest transmission function can be simulated by an alternative prover strategy operating under the malicious transmission function.

The simulation proceeds by introducing an auxiliary prover at each verifier position. Under the malicious transmission function, verifier messages are first delivered to these auxiliary provers. The auxiliary provers may then forward the messages to the verifier's intended party, (prover-to-prover communication is always allowed under the malicious transmission function) thereby emulating the honest transmission function's behavior. We exploit this observation in the soundness analysis.

3.3 Proof systems and complexity classes

Before we define our new "positional" proof systems and complexity classes, we specify the input generation functions and the joint measurement needed for the definitions.

Input generation functions

As initial input, the verifiers receive the instance $\mathbb{x}$, security parameter λ and common randomness ρ. Additionally, honest provers also receive the instance $\mathbb{x}$ and common randomness τ. Thus, we define input generation functions Inp and $\overline{\mathsf{Inp}}$ that generate the input state $\boldsymbol{\rho}_{\mathsf{in}}$ for the honest and malicious game respectively as:

$$\mathsf{Inp}(\mathbb{x}, \lambda, \rho, \tau) \coloneqq \left(\bigotimes_{i\in\mathcal{V}} |\mathbb{x}, \lambda, \rho\rangle\langle \mathbb{x}, \lambda, \rho|_{I_i}\right) \otimes \left(\bigotimes_{i\in\mathcal{P}} |\mathbb{x}, \tau\rangle\langle \mathbb{x}, \tau|_{I_i}\right) ,$$

$$\overline{\mathsf{Inp}}(\mathbb{x}, \lambda, \rho, \tau) \coloneqq \left(\bigotimes_{i\in\mathcal{V}} |\mathbb{x}, \lambda, \rho\rangle\langle \mathbb{x}, \lambda, \rho|_{I_i}\right) \otimes \left(\bigotimes_{i\in\mathcal{P}} |\tau\rangle\langle \tau|_{I_i}\right) .$$

Joint measurement

Since we want the verifiers to jointly decide whether to accept or reject at the end of the protocol, the measurement P_{output} should be a binary projective measurement $\{P_{\mathsf{output}}, \mathbf{I} - P_{\mathsf{output}}\}$ that acts trivially on prover internal registers, i.e.,

$$P_{\mathsf{output}} \;=\; P^{(\mathsf{V})}_{\mathsf{output}} \otimes \mathbf{I}_{\mathcal{H}_{I_{\mathsf{P}}}},\; \mathcal{H}_{I_P} := \bigotimes_{i \in \mathcal{P}} \mathcal{H}_{I_i}$$

where $P^{(\mathsf{V})}_{\mathsf{output}} = \{P^{(\mathsf{V})}_{\mathsf{output}}, \mathbf{I} - P^{(\mathsf{V})}_{\mathsf{output}}\}$ is a binary projective measurement on $\mathcal{H}_{I_V} := \bigotimes_{i \in \mathcal{V}} \mathcal{H}_{I_i}$.

Quantum positional MIPs

A **l-verifier k-prover Quantum Positional Multi-Prover Interactive Proof (separable (l, k)-QPMIP)** for a relation $\mathcal{R}$ is a tuple:

$$\mathsf{QPMIP} \coloneqq ((\mathcal{X}, \mathsf{d}), \mathsf{p}, T, \{\mathsf{V}_i\}_{i \in [\mathsf{l}]}, \{\mathsf{P}_i\}_{i \in [\mathsf{k}]}, P_{\mathsf{output}})$$

where $(\mathcal{X}, \mathsf{d})$ is a discrete metric space, and p is a position mapping to $\mathcal{X}$, T is the timeout value, verifiers $\{\mathsf{V}_i\}_{i \in [\mathsf{l}]}$ and honest provers $\{\mathsf{P}_i\}_{i \in [\mathsf{k}]}$, and the output measurement P_{output} is a binary projective measurement as specified above. The timeout value T and the number of provers k are $\mathsf{poly}(n)$, d and the verifier strategy are computable in $\mathsf{poly}(n)$-time.

We associate the following types of timed quantum communication protocols to the QPMIP:

- $\mathsf{tQCP}^{\mathsf{s}}[\mathsf{QPMIP}] \coloneqq (T, \Lambda^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}}, \{\mathsf{V}_i\}_{i \in [\mathsf{l}]}, \{\mathsf{P}_i\}_{i \in [\mathsf{k}]}, P_{\mathsf{output}})$ describes the honest prover strategy under the separable honest position transmission function $\Lambda^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}}$ (see Definition 12).
- $\mathsf{tQCP}^{\mathsf{si}}[\mathsf{QPMIP}] = (T, \Lambda^{\mathsf{si}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}}, \{\mathsf{V}_i\}_{i \in [\mathsf{l}]}, \{\mathsf{P}_i\}_{i \in [\mathsf{k}]}, P_{\mathsf{output}})$ describes the honest prover strategy under the separable and isolated honest position transmission function $\Lambda^{\mathsf{si}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}}$ (see Definition 12).
- $\overline{\mathsf{tQCP}}^{\mathsf{s}}\left[\mathsf{QPMIP}, \{\widetilde{\mathsf{P}}_i\}_{i \in [\mathsf{k}']}, \widetilde{\mathsf{p}}\right] = (T, \widetilde{\Lambda}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\widetilde{\mathsf{p}}}, \{\mathsf{V}_i\}_{i \in [\mathsf{l}]}, \{\widetilde{\mathsf{P}}_i\}_{i \in [\mathsf{k}']}, P_{\mathsf{output}})$ describes a malicious prover strategy $\{\widetilde{\mathsf{P}}_i\}_{i \in [\mathsf{k}']}$ at positions defined by $\widetilde{\mathsf{p}}$ under the malicious position transmission function $\widetilde{\Lambda}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\widetilde{\mathsf{p}}}$ (see Definition 13).

We say that QPMIP has (perfect) completeness and soundness error $\epsilon_{\mathsf{QPMIP}}$ if it satisfies the following two properties:

▶ **Definition 15.** *A separable* $\mathsf{QPMIP} = ((\mathcal{X}, \mathsf{d}), \mathsf{p}, T, \{\mathsf{V}_i\}_{i \in [\mathsf{l}]}, \{\mathsf{P}_i\}_{i \in [\mathsf{k}]}, P_{\mathsf{output}})$ *for a relation* $\mathcal{R}$ *has* **perfect completeness** *if for every instance size* $n \in \mathbb{N}$*, every instance* $\mathbb{x} \in \mathcal{L}(\mathcal{R})$ *of size* n*, every security parameter* $\lambda \in \mathbb{N}$*, the timed quantum communication protocol* $\mathsf{tQCP}^{\mathsf{s}}[\mathsf{QPMIP}]$ *satisfies:*

$$\Pr_{\substack{\rho \in \{0,1\}^{\mathsf{vr}} \\ \tau \in \{0,1\}^{\mathsf{pr}}}}\left[1 \leftarrow \Gamma(\mathsf{Inp}(\mathbb{x}, \lambda, \rho, \tau), \mathsf{tQCP}^{\mathsf{s}}[\mathsf{QPMIP}])\right] = 1 \;.$$

▶ **Definition 16.** *A separable* $\mathsf{QPMIP} = ((\mathcal{X}, \mathsf{d}), \mathsf{p}, T, \{\mathsf{V}_i\}_{i \in [\mathsf{l}]}, \{\mathsf{P}_i\}_{i \in [\mathsf{k}]}, P_{\mathsf{output}})$ *for a relation* $\mathcal{R}$ *has* **soundness error** $\epsilon_{\mathsf{QPMIP}}$*, if for every instance size* $n \in \mathbb{N}$*, every instance* $\mathbb{x} \notin \mathcal{L}(\mathcal{R})$ *of size* n*, every security parameter* $\lambda \in \mathbb{N}$*, and every prover strategy* $\{\widetilde{\mathsf{P}}_i\}_{i \in [\mathsf{k}']}$*, every position mapping* $\widetilde{\mathsf{p}} \in \{\mathsf{p} : [\mathsf{l} + \mathsf{k}'] \to \mathcal{X} \mid \forall i \in [\mathsf{l}],\, \widetilde{\mathsf{p}}(i) = \mathsf{p}(i)\}$*, i.e. maps verifiers to positions that are consistent with the honest position mapping* p*, the timed quantum communication protocol* $\overline{\mathsf{tQCP}}^{\mathsf{s}}\left[\mathsf{QPMIP}, \{\widetilde{\mathsf{P}}_i\}_{i \in [\mathsf{k}']}, \widetilde{\mathsf{p}}\right]$ *satisfies:*

$$\Pr_{\substack{\rho \in \{0,1\}^{\mathsf{vr}} \\ \tau \in \{0,1\}^{\mathsf{pr}}}}\left[1 \leftarrow \Gamma\left(\overline{\mathsf{Inp}}(\mathbb{x}, \lambda, \rho, \tau), \overline{\mathsf{tQCP}}^{\mathsf{s}}\left[\mathsf{QPMIP}, \{\widetilde{\mathsf{P}}_i\}_{i \in [\mathsf{k}']}, \widetilde{\mathsf{p}}\right]\right)\right] \leq \epsilon_{\mathsf{QPMIP}}(\mathbb{x}, \lambda) \;.$$

▶ **Definition 17.** *We say that the* QPMIP *is* **separable and isolated** *if the perfect completeness condition in Definition 15 also holds for the timed quantum communication protocol* $\mathsf{tQCP}^{\mathsf{si}}[\mathsf{QPMIP}]$.

▶ **Definition 18** (QPMIP complexity classes)**.** *For any metric space* $(\mathcal{X}, \mathsf{d})$*, define the complexity class* $\mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}]$ *to be the set of languages decidable by a separable QPMIP with metric space* $(\mathcal{X}, \mathsf{d})$ *and the honest position mapping* p*. Let* $\mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d})}$ *be the union of* $\mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}]$ *over all possible position mappings* p *defined on* $\mathcal{X}$*.*

Similarly, the complexity class $\mathbf{QPMIP}^{\mathsf{si}}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}]$ *is the set of languages decidable by a separable and isolated QPMIP with metric space* $(\mathcal{X}, \mathsf{d})$ *and the honest position mapping* p*, and* $\mathbf{QPMIP}^{\mathsf{si}}_{(\mathcal{X},\mathsf{d})}$ *is the union of* $\mathbf{QPMIP}^{\mathsf{si}}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}]$ *over all possible position mappings* p *defined on* $\mathcal{X}$*.*

▶ Remark 19. For any metric space $(\mathcal{X}, \mathsf{d})$ and honest position mapping p, by definition we always have $\mathbf{QPMIP}^{\mathsf{si}}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}] \subseteq \mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}]$ and $\mathbf{QPMIP}^{\mathsf{si}}_{(\mathcal{X},\mathsf{d})} \subseteq \mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d})}$.

We adapt the proof for $\mathbf{QMIP}^{\mathsf{ne}} \subseteq \mathbf{NEXP}$ (In $\mathbf{QMIP}^{\mathsf{ne}}$ a quantum verifier interacts with quantum but unentangled provers) in [10], and show the following theorem:

▶ **Theorem 20.** *For any metric space* $(\mathcal{X}, \mathsf{d})$*,* $\mathbf{QPMIP}^{\mathsf{si}}_{(\mathcal{X},\mathsf{d})} \subseteq \mathbf{NEXP}$*.*

4 The min-ball condition

In this section, we introduce the notion of the *min-ball* and the associated *min-ball condition*. As outlined in Section 2.1, this condition precisely captures the classical dichotomy: if the min-ball condition holds, the class of languages decidable by classical positional MIPs is **NEXP**; otherwise, it collapses to **PSPACE**.

▶ **Definition 21** (min-ball)**.** *For any position mapping* $\mathsf{p} : \mathcal{V} \cup \mathcal{P} \to \mathcal{X}$*, the* **min-ball** *of a verifier* V *under the mapping* p *is the set of points at distance at most* $r := \min_{\mathsf{P} \in \mathcal{P}} \mathsf{d}_{\mathsf{p}}(\mathsf{P}, \mathsf{V})$ *from* V*, that is, the set* $\{x \in \mathcal{X} : \mathsf{d}(x, \mathsf{p}(\mathsf{V})) \leq r\}$*.*

We use $\mathbf{PMIP}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}]$ to denote the set of languages decidable by classical positional MIPs with the honest position mapping p, and we have the following characterization of this complexity class:

▶ **Theorem 22.** *Let* $(\mathcal{X}, \mathsf{d})$ *be a metric space and* p *be a position mapping defined on* $\mathcal{X}$*. Then* $\mathbf{PMIP}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}] = \mathbf{NEXP}$ *if* p *satisfies the min-ball condition and* $\mathbf{PMIP}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}] = \mathbf{PSPACE}$ *otherwise.*

5 Positional Hardcore Bit (PHB) schemes

In this section, we define a new primitive, called a *positional hardcore bit* (PHB). A PHB scheme is a cryptographic primitive that when associated with a metric space and a position mapping, can be used to guarantee strong positional security properties. In particular, a PHB scheme defines an algorithm that constructs a bit called the "hardcore bit", such that together with a position mapping, it can be used to construct a positional protocol with the guarantee that no collusion of malicious parties can simultaneously succeed in the protocol and guess the hardcore bit with probability much better than random, until the honest party has had time to compute and send the hardcore bit to the closest malicious party. This is the strongest form of positional security one can hope for in terms of the time until which unlearnability of the hardcore bit is guaranteed.

In the second half of this section, we instantiate a PHB scheme from strong seeded extractors and prove its security using a distinguishing lemma for adversarial quantum side information. This construction is the main technical contribution of this section, and is the key ingredient in our construction of a QPMIP protocol for **EXP** in the next section.

Here is a roadmap for this section. In Section 5.1, we formally define PHB schemes and how to embed them in a metric space to obtain positional protocols. We also define the main security property of PHB schemes in Definition 28.

5.1 Definition

▶ **Definition 23** (Positional Hardcore Bit Scheme)**.** *For $\ell \in \mathbb{N}$, a* **ℓ-positional hardcore bit** *(ℓ-PHB) scheme is a tuple* $\mathsf{PHB} = (\mathsf{Gen}, \mathsf{Resp}, \mathsf{Ver}, \mathsf{Hb})$*:*

- Gen *is a* **challenge generation function** *that takes as input the amplification parameter $\zeta \in \mathbb{N}$, and outputs a list of challenges $(\mathsf{ch}_1, \cdots, \mathsf{ch}_\ell)$ and an auxiliary string aux. The length of the challenges and auxiliary can depend on ζ.*
- Resp *is a* **response function** *that takes challenges $\mathsf{ch}_1, \cdots, \mathsf{ch}_\ell$ as input and outputs a list of responses $(x_1, \cdots, x_\ell)$. These represent expected responses to the challenges from an honest prover.*
- Ver *is a* **verification algorithm** *that takes proposed responses and auxiliary input $(\widetilde{x}_1, \cdots, \widetilde{x}_\ell, \mathsf{aux})$ as input, and outputs either 0 (reject) or 1 (accept).*
- Hb *is a* **hardcore bit generator** *that takes challenges $(\mathsf{ch}_1, \cdots, \mathsf{ch}_\ell)$ as input and outputs a bit $\mathsf{hb} \in \{0,1\}$. The output of the generator is called the* **hardcore bit** *and is, by definition, fully determined by the challenges.*

Note that $\mathsf{Gen}, \mathsf{Resp}, \mathsf{Ver}, \mathsf{Hb}$ can be quantum algorithms and $\{\mathsf{ch}_i\}_{i\in[\ell]}, \mathsf{res}, \mathsf{aux}$ can be quantum information. We shall require the following natural correctness property for a PHB scheme:

▶ **Definition 24.** *A ℓ-PHB scheme $\mathsf{PHB} = (\mathsf{Gen}, \mathsf{Resp}, \mathsf{Ver}, \mathsf{Hb})$ is said to have* **perfect completeness** *if for every privacy amplification parameter $\zeta \in \mathbb{N}$,*

$$\Pr\left[\ \mathsf{Ver}(x_1, \cdots, x_\ell, \mathsf{aux}) = 1 \ \middle|\ \begin{array}{l}(\mathsf{ch}_1, \cdots, \mathsf{ch}_\ell, \mathsf{aux}) \leftarrow \mathsf{Gen}(\zeta) \\ (x_1, \cdots, x_\ell) \leftarrow \mathsf{Resp}(\mathsf{ch}_1, \cdots, \mathsf{ch}_\ell)\end{array}\right] = 1 \ .$$

PHBs can be embedded in a metric space as a special communication protocol with ℓ verifiers $\mathsf{V}_1, \cdots, \mathsf{V}_\ell$ and one honest prover P. We define this formally below:

▶ **Construction 25** (Embedded PHB)**.** *Consider a ℓ-PHB scheme $\mathsf{PHB} = (\mathsf{Gen}, \mathsf{Resp}, \mathsf{Ver}, \mathsf{Hb})$, metric space $(\mathcal{X}, \mathsf{d})$, position mapping $\mathsf{p} : [\ell+1] \to \mathcal{X}$ and message arrival time $t^* \in \mathbb{N}$. We associate $(\mathsf{PHB}, \mathsf{p}, t^*)$ with an* embedded *PHB scheme $\mathsf{EPHB} = ((\mathcal{X}, \mathsf{d}), \mathsf{p}, T, \{\mathsf{V}_i\}_{i\in\ell}, \mathsf{P}, P_{\mathsf{output}})$ with parties $\{\mathsf{V}_i\}_{i\in[\ell]}$, P, timeout T and output projector P_{output} defined as follows:*

- **Verifier strategies**. *Each verifier V_i is a party located at position $\mathsf{p}(i)$. At the start of the protocol, it measures its initial register, parsing it to obtain (ζ, ρ). It calls $\mathsf{Gen}(\zeta)$ with randomness ρ to deterministically obtain challenge ch_i (the other challenges are discarded) and auxiliary input aux. It then sends ch_i to the prover immediately. At the timeout time T defined below, V_i measures its message registers to obtain $\widetilde{x}_i$ and copies it to its internal register.*
- **Honest prover strategy**. *The honest prover P is a party located at position $\mathsf{p}(\ell+1)$. It waits until time t^* to receive all messages from the verifiers. At time t^*, the honest prover measures its message registers to obtain $(\widetilde{\mathsf{ch}}_1, \cdots, \widetilde{\mathsf{ch}}_\ell)$, computes $(x_1, \cdots, x_\ell) \leftarrow \mathsf{Resp}(\widetilde{\mathsf{ch}}_1, \cdots, \widetilde{\mathsf{ch}}_\ell)$, and sends each x_i to verifier V_i immediately.*

- *The timeout T is set to $t^* + \max_{i\in[\ell]} \mathsf{d}_{\mathsf{p}}(\mathsf{P},\mathsf{V}_i)$ to ensure that all messages from the honest prover can arrive in time if sent immediately at time t^*.*
- *The output projector accepts all final verifier states that would be accepted by the PHB verification algorithm, i.e.:*

$$P_{\text{output}} = \sum_{\substack{\mathsf{aux},\tilde{x}_1,\cdots,\tilde{x}_\ell \\ \mathsf{Ver}(\tilde{x}_1,\cdots,\tilde{x}_\ell,\mathsf{aux})=1}} |\mathsf{aux}\rangle\langle\mathsf{aux}| \otimes \bigotimes_{i=1}^{\ell} |\widetilde{x}_i\rangle\langle\widetilde{x}_i| \otimes \mathbf{I}_{\mathcal{H}_{I_{\ell+1}}}.$$

We say that an embedded PHB is perfectly complete if the honest parties can always succeed in the protocol:

▶ **Definition 26.** *Let* $\mathsf{EPHB} = ((\mathcal{X},\mathsf{d}),\mathsf{p},T,\{\mathsf{V}_i\}_{i\in\ell},\mathsf{P},P_{\text{output}})$ *be an embedded PHB associated with a PHB scheme* $\mathsf{PHB} = (\mathsf{Gen},\mathsf{Resp},\mathsf{Ver},\mathsf{Hb})$ *as in Construction 25. We say that* EPHB *has* **perfect completeness** *if for every privacy amplification parameter $\zeta\in\mathbb{N}$, the timed quantum communication protocol* $\mathsf{tQCP} = (T,\Lambda^{\mathsf{s}}_{(\mathcal{X},\mathsf{d}),\mathsf{p}},\{\mathsf{V}_i\}_{i\in\ell},\{\mathsf{P}\},P_{\text{output}})$ *satisfies*

$$\mathsf{Pr}_{\rho\in\{0,1\}^{\mathsf{vr}}}\left[1\leftarrow\Gamma((\zeta,\rho),\mathsf{tQCP})\right] = 1.$$

▶ **Proposition 27.** *Let* $\mathsf{PHB} = (\mathsf{Gen},\mathsf{Resp},\mathsf{Ver},\mathsf{Hb})$ *be a ℓ-PHB scheme with perfect completeness,* $\mathsf{p}:[\ell+1]\to\mathcal{X}$ *and* EPHB *the associated embedded PHB. Then* EPHB *has perfect completeness as defined in Definition 26.*

Proof. By the definition of perfect completeness for PHB schemes in Definition 24, for every privacy amplification parameter $\zeta\in\mathbb{N}$,

$$\mathsf{Pr}\left[\ \mathsf{Ver}(x_1,\cdots,x_\ell,\mathsf{aux})=1 \ \middle|\ \begin{array}{l}(\mathsf{ch}_1,\cdots,\mathsf{ch}_\ell,\mathsf{aux})\leftarrow\mathsf{Gen}(\zeta)\\(x_1,\cdots,x_\ell)\leftarrow\mathsf{Resp}(\mathsf{ch}_1,\cdots,\mathsf{ch}_\ell)\end{array}\right] = 1\ .$$

In the associated EPHB, by construction, at time t^*, party $\ell+1$ is able to, and computes $(x_1,\cdots,x_\ell)\leftarrow\mathsf{Resp}(\mathsf{ch}_1,\cdots,\mathsf{ch}_\ell)$. Further, party $\ell+1$ eventually sends response x_i to party i. Thus, at the end of the protocol, for every $i\in[\ell]$, party i has received x_i, i.e. for each i, $\widetilde{x}_i = x_i$. Therefore, every tuple $(\mathsf{aux},\widetilde{x}_1,\cdots,\widetilde{x}_\ell)$ that occurs at the end of the protocol satisfies $\mathsf{Ver}(\widetilde{x}_1,\cdots,\widetilde{x}_\ell,\mathsf{aux}) = 1$, so that for any set of challenges generated by Gen, the output projector P_{output} preserves the state of the system (by perfect completeness of the PHB protocol), so that the EPHB has perfect completeness as in Definition 26. ◀

We now define the main security property of PHB schemes, called the *positional hardcore property*. Intuitively, this property states that it is impossible for a collusion of malicious provers to both make the verifiers accept and guess the hardcore bit with probability significantly better than random for a time period determined by their distances from the honest prover.

▶ **Definition 28** (positional hardcore property)**.** *A ℓ-PHB scheme* $\mathsf{PHB} = (\mathsf{Gen},\mathsf{Resp},\mathsf{Ver},\mathsf{Hb})$ *is said to be* $(\epsilon_{\mathsf{PHB}},\delta)-$**positional hardcore** *on metric space $(\mathcal{X},\mathsf{d})$ and honest position mapping $\mathsf{p}:[\ell+1]\to\mathcal{X}$ (with $\mathsf{p}(\ell+1)\in\mathbf{Hull}(\{\mathsf{p}(i)\}_{i\in[\ell]})$) if there exists a negligible function $\epsilon_{\mathsf{PHB}} = \mathsf{negl}(\zeta)$ and non-negligible function $\delta = \Omega(1/\zeta^d)$ such that the following holds. For any $\mathsf{k}'\in\mathbb{N}$, prover strategy $\{\widetilde{\mathsf{P}}_i\}_{i\in[\mathsf{k}']}$, and malicious position mapping $\widetilde{\mathsf{p}}\in\{p:[\ell+\mathsf{k}']\to\mathcal{X}\mid \forall i\in[\ell],p(i)=\mathsf{p}(i)\}$. Let $\mathsf{accept} = \Gamma((\zeta,\rho),\overline{\mathsf{tQCP}}[\{\widetilde{\mathsf{P}}_i\}_{i\in[\mathsf{k}']},\widetilde{\mathsf{p}}])$ denote the random variable representing the output of the timed quantum communication game executed with input (ζ,ρ) and communication protocol $\overline{\mathsf{tQCP}}[\{\widetilde{\mathsf{P}}_i\}_{i\in[\mathsf{k}']},\widetilde{\mathsf{p}}]$. Suppose that the malicious provers succeed in making the verifiers accept in this game with probability at least $\delta(\zeta)$. That is, if*

$$\mathsf{Pr}_{\rho\in\{0,1\}^{\mathsf{vr}}}\left[\mathsf{accept}=1\right]\geq\delta(\zeta)\ ,$$

then, for every $\mathcal{S} \subseteq [\ell+1, \ell+\mathsf{k}']$*, any (quantum) algorithm* $\mathcal{A}$ *that is given the joint state* $\boldsymbol{\rho}_{\mathcal{S}}^{(t)}$ *of all* $\widetilde{\mathsf{P}}_i$ *in set* $\mathcal{S}$ *at time* $t < t^* + \min_{j\in\mathcal{S}} \mathsf{d}(\mathsf{p}(\mathsf{P}), \widetilde{\mathsf{p}}(j))$ *cannot distinguish whether* $\mathsf{hb} = \mathsf{Hb}(\mathsf{ch}_1, \cdots, \mathsf{ch}_\ell)$ *is* 0 *or* 1 *with advantage more than* $\epsilon_{\mathsf{PHB}}(\zeta)$ *over verifier random coins* ρ*. More formally, for every* $t < t^* + \min_{j\in\mathcal{S}} \mathsf{d}(\mathsf{p}(\mathsf{P}), \widetilde{\mathsf{p}}(j))$*, we have:*

$$\Big|\mathsf{Pr}_{\rho\in\{0,1\}^{\mathsf{vr}},(\mathsf{ch}_1,\cdots,\mathsf{ch}_\ell,\mathsf{aux})\leftarrow\mathsf{Gen}(\zeta,\rho)}\left[\mathcal{A}\left(\boldsymbol{\rho}_{\mathcal{S}}^{(t)},\ \ \mathsf{Hb}(\mathsf{ch}_1,\cdots,\mathsf{ch}_\ell)\right)=1 \mid \mathsf{accept}=1\right]$$

$$-\mathsf{Pr}_{\rho\in\{0,1\}^{\mathsf{vr}},(\mathsf{ch}_1,\cdots,\mathsf{ch}_\ell,\mathsf{aux})\leftarrow\mathsf{Gen}(\zeta,\rho)}\left[\mathcal{A}\left(\boldsymbol{\rho}_{\mathcal{S}}^{(t)},\neg\mathsf{Hb}(\mathsf{ch}_1,\cdots,\mathsf{ch}_\ell)\right)=1 \mid \mathsf{accept}=1\right]\Big| \leq \epsilon_{\mathsf{PHB}}(\zeta).$$

Note that the states $\boldsymbol{\rho}_{\mathcal{S}}^{(t)}$ *are generated as per the malicious tQCP game running with the same randomness that generated the challenges, i.e. on input* (ζ, ρ)*.*

6 EXP is in QPMIP

In this section, we show one of our main results: under a position map which we call the "pyramid position map" where the min-ball condition is violated, we construct a QPMIP for no-signaling MIP, and prove that its soundness at most the no-signaling MIP soundness.

▶ **Theorem 29.** *Given the following two ingredients:*

- *A* k*-prover no-signaling MIP* $\mathsf{MIP} = ((\mathbf{P}_i)_{i\in[\mathsf{k}]}, \mathbf{V})$ *for a language* $\mathcal{L}$ *with* k *provers, query size* $\mathsf{l_q}$ *and soundness error* $\epsilon^{\mathsf{ns}}_{\mathsf{MIP}}$ *against* δ*-no-signaling strategies.*
- *A 2-verifier* $\epsilon_{\mathsf{PHB}}(\zeta)$*-positional hardcore bit scheme* $\mathsf{PHB} = (\mathsf{Gen}, \mathsf{Resp}, \mathsf{Ver}, \mathsf{Hb})$ *(See Definition 23) such that the* Resp *algorithm has a single non-trivial output.*

Then, for $\zeta \in \mathbb{N}$ *such that* $\epsilon_{\mathsf{PHB}}(\zeta) < \frac{\delta}{\mathsf{k}\cdot\mathsf{l_q}}$*, Construction 31 is a separable and isolated QPMIP (see Definition 17) for language* $\mathcal{L}$ *with* k *provers,* $\mathsf{k}+1$ *verifiers and soundness error (see Definition 16) at most* $\epsilon^{\mathsf{ns}}_{\mathsf{MIP}}$*.*

Note that the positional hardcore bit scheme construction above satisfies the requirement for the second ingredient in the theorem statement. And since the above theorem is true for any number k of provers, in particular, we can pick k to be polynomial in the instance size n. By the known characterization that $\mathbf{MIP}^{\mathsf{ns}}$ with polynomially many provers captures $\mathbf{EXP}$, we have the following:

▶ **Lemma 30.** *For the position map* $\mathsf{p}_{\mathsf{pyramid}}$ *defined in Section 6.1,* $\mathbf{EXP} \subseteq \mathbf{QPMIP}^{\mathsf{s}}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}_{\mathsf{pyramid}}]$*.*

6.1 A pyramid position mapping

Below we describe a way for placing $\mathsf{k}+1$ verifiers and k provers in $\mathbb{R}^3$, so that the min-balls of verifiers pairwise intersect, and the min-balls of all verifiers do not intersect simultaneously. Intuitively, we are placing the min-balls of k verifiers on the vertices of a regular k-gon, each with radius r large enough so that they all intersect pairwise. Then, we place the last verifier "on top", so that its min-ball is tangent to all of the other min-balls. See an illustration of this in Figure 2 for the case when $\mathsf{k} = 6$.

For the 3-dimensional Euclidean metric space $(\mathbb{R}^3, \mathsf{d})$, we present a position mapping $\mathsf{p}_{\mathsf{pyramid}} : [2\cdot\mathsf{k}+1] \to \mathbb{R}^3$ for placing $\mathsf{k}+1$ verifiers and k provers in $\mathbb{R}^3$:

- Let O be the origin at $(0,0,0)$. Draw a regular k-gon centered at O, and let R be the circumradius of this polygon, i.e. the distance from O to each vertex. The position mapping p maps verifiers $\{\mathsf{V}_i\}_{i\in[\mathsf{k}]}$ to the vertices of this polygon.

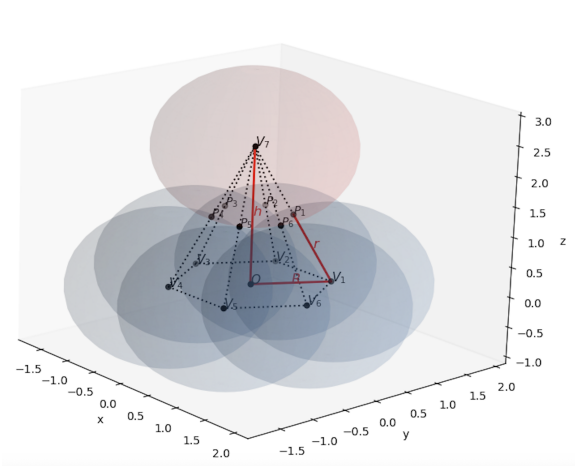

Figure 2 An illustration for $\mathsf{k} = 6$, $R = 1$, $r = 1.25$, $h = 2.291$.

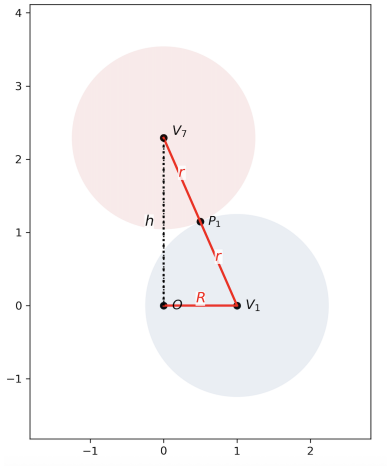

Figure 3 A slice on the plane containing O, V_1 and V_7.

- Choose radius $r > R$. Map the verifier $\mathsf{V}_{\mathsf{k}+1}$ to the coordinate $(0, 0, \sqrt{4 \cdot r^2 - R^2})$.
- For each $i \in [\mathsf{k}]$, map honest prover P_i to the midpoint of the line segment connecting V_i and $\mathsf{V}_{\mathsf{k}+1}$. See Figure 3.

More explicitly, the position mapping $\mathsf{p}_{\mathsf{pyramid}}$ is defined as follows:

$$\mathsf{p}_{\mathsf{pyramid}}(i) = \begin{cases} \left(R \cdot \cos(\frac{2\pi i}{\mathsf{k}}), R \cdot \sin(\frac{2\pi i}{\mathsf{k}}), 0\right) & i \in [\mathsf{k}] \\ (0, 0, \sqrt{4 \cdot r^2 - R^2}) & i = \mathsf{k}+1 \\ \left(\frac{1}{2} \cdot R \cdot \cos(\frac{2\pi i}{\mathsf{k}}), \frac{1}{2} \cdot R \cdot \sin(\frac{2\pi i}{\mathsf{k}}), \frac{1}{2} \cdot \sqrt{4 \cdot r^2 - R^2}\right) & i \in [\mathsf{k}+2, 2 \cdot \mathsf{k}+1] \end{cases}$$

Notice that the position mapping $\mathsf{p}_{\mathsf{pyramid}}$ does not satisfy the min-ball condition, so under the pyramid position map, $\mathbf{PMIP}_{(\mathcal{X},\mathsf{d})}[\mathsf{p}_{\mathsf{pyramid}}] = \mathbf{IP}$ as shown in Theorem 22. Moreover, notice that the mutual intersection of all min-balls is empty, thus the standard collapse condition for QPMIP with a common min-ball intersection does not apply to $\mathsf{p}_{\mathsf{pyramid}}$.

6.2 Construction

▶ **Construction 31** (QPMIP for EXP). *Given a* k*-prover no-signaling MIP* $\mathsf{MIP} = ((\mathbf{P}_i)_{i\in[\mathsf{k}]}, \mathbf{V})$ *for a language* $\mathcal{L}$ *and a 2-verifier* $\epsilon_{\mathsf{PHB}}(\zeta)$*-positional hardcore bit scheme* $\mathsf{PHB} = (\mathsf{Gen}, \mathsf{Resp}, \mathsf{Ver}, \mathsf{Hb})$ *with parameters as specified in the statement of Theorem 29, for* $\zeta \in \mathbb{N}$ *such that* $\epsilon_{\mathsf{PHB}}(\zeta) < \frac{\delta}{\mathsf{k}\cdot\mathsf{l}_\mathsf{q}}$ *and for some small delay time* $t_{\mathsf{delay}} \in \mathbb{N}$*, we construct a one-round QPMIP* $\mathsf{QPMIP} = ((\mathbb{R}^3, \mathsf{d}), \mathsf{p}_{\mathsf{pyramid}}, T, \{\mathsf{V}_i\}_{i\in[\mathsf{k}+1]}, \{\mathsf{P}_i\}_{i\in[\mathsf{k}]}, P_{\mathsf{output}})$ *as follows:*

- **Verifier strategies***:*
  1. *Initialization: Every verifier's internal register is initialized to the state* $|\mathbb{x}, \lambda, \rho\rangle\langle\mathbb{x}, \lambda, \rho|$*. Measure in computational basis and parse* ρ*. For* $i \in [\mathsf{k}]$*,* $j \in [\mathsf{l}_\mathsf{q}]$*, every verifier runs the challenge generation algorithm with randomness* ρ *to deterministically obtain the challenges:* $(\mathsf{ch}_1^{i,j}, \mathsf{ch}_2^{i,j}, \mathsf{aux}^{i,j}) \leftarrow \mathsf{Gen}(\zeta)$*.*
  2. *At time* $t^* - r$*, for every* $i \in [\mathsf{k}]$*,* V_i *sends challenges* $\{\mathsf{ch}_2^{i,j}\}_{j\in[\mathsf{l}_\mathsf{q}]}$ *to* P_i*, and* $\mathsf{V}_{\mathsf{k}+1}$ *sends challenge* $\{\mathsf{ch}_1^{i,j}\}_{j\in[\mathsf{l}_\mathsf{q}]}$ *to* P_i*.*
  3. *At time* $t^* - r + t_{\mathsf{delay}}$*,* $\mathsf{V}_{\mathsf{k}+1}$ *computes the MIP queries:* $\mathsf{q} := (\mathsf{q}_i := (\mathsf{q}_i^j)_{j\in[\mathsf{l}_\mathsf{q}]})_{i\in[\mathsf{k}]} \leftarrow \mathbf{V}(\mathbb{x}, 1^\lambda, \rho)$*. For every* $i \in [\mathsf{k}]$*,* V_i *sends the masked query bits* $\{\mathsf{q}_i^j \oplus \mathsf{Hb}(\mathsf{ch}_1^{i,j}, \mathsf{ch}_2^{i,j})\}_{j\in[\mathsf{l}_\mathsf{q}]}$ *to* P_i*.*
  4. *At time* $t^* + r$*,* $\mathsf{V}_{\mathsf{k}+1}$ *receives* $\{\widetilde{x}^{i,j}\}_{i\in[\mathsf{k}],j\in[\mathsf{l}_\mathsf{q}]}$*.*
  5. *At time* $t^* + r + t_{\mathsf{delay}}$*, for every* $i \in [\mathsf{k}]$*,* V_i *receives* $\widetilde{\mathsf{res}}_i$*.*

- **Honest prover strategies***:*
  1. *At time t^*, for every $i \in [\mathsf{k}]$, P_i computes $x^{i,j} \leftarrow \mathsf{Resp}(\mathsf{ch}_1^{i,j}, \mathsf{ch}_2^{i,j})$ for every $j \in [\mathsf{l_q}]$. Sends $\{x^{i,j}\}_{j\in[\mathsf{l_q}]}$ to $\mathsf{V}_{\mathsf{k}+1}$.*
  2. *At time $t^* + t_{\mathsf{delay}}$, for every $i \in [\mathsf{k}]$, P_i receives $\{x_1^{i,j}, x_2^{i,j}\}_{j\in[\mathsf{l_q}]}$, computes $\{\mathsf{Hb}(\mathsf{ch}_1^{i,j}, \mathsf{ch}_2^{i,j})\}_{j\in[\mathsf{l_q}]}$ and recover the MIP query q_i. Run the honest MIP provers: $\forall i \in [\mathsf{k}]$, $\mathsf{res}_i \leftarrow \mathbf{P}_i(\mathbb{x}, \mathsf{q}_i, \tau)$. Sends res_i to V_i.*
- *The timeout value T is set to $t^* + r + t_{\mathsf{delay}}$.*
- **Output projector:** *The verifier accepts if and only if:*
  - All PHB checks pass: *for each $i \in [\mathsf{k}]$ and $j \in [\mathsf{l_q}]$, $\mathsf{Ver}(\widetilde{x}^{i,j}, \mathsf{aux}^{i,j}) = 1$.*
  - The MIP verifier accepts: $\mathbf{V}(\mathbb{x}, 1^\lambda, (\widetilde{\mathsf{res}}_i)_{i\in[\mathsf{k}]}, \rho) = 1$.

  The output projector is the projector onto the subspace spanned by the joint state of the verifiers' final registers that satisfy the above two conditions.

▶ Remark 32. There exists a choice of $t_{\mathsf{delay}} \in \mathbb{N}$ so that:

$$t = t^* + r + t_{\mathsf{delay}} < t^* + \min_{i\neq j} \mathsf{d}_{\mathsf{P}_{\mathsf{pyramid}}}(\mathsf{V}_i, \mathsf{P}_j) \ .$$

Note that $\mathsf{d}_{\mathsf{P}_{\mathsf{pyramid}}}(\mathsf{V}_i, \mathsf{P}_j) = r$ iff. $i = j$; otherwise $\mathsf{d}_{\mathsf{P}_{\mathsf{pyramid}}}(\mathsf{V}_i, \mathsf{P}_j)$ is strictly larger than r. Notice that scaling r and R increases the gap between $\mathsf{d}_{\mathsf{P}_{\mathsf{pyramid}}}(\mathsf{V}_i, \mathsf{P}_j)$ and r, so we can pick $t_{\mathsf{delay}} = 1$ without loss of generality.

References

1 Pouriya Alikhani, Nicolas Brunner, Claude Crépeau, Sébastien Designolle, Raphaël Houlmann, Weixu Shi, Nan Yang, and Hugo Zbinden. Experimental relativistic zero-knowledge proofs. *Nat.*, 599(7883):47–50, 2021. doi:10.1038/S41586-021-03998-Y.

2 László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1:3–40, 1991. Preliminary version appeared in FOCS '90. doi:10.1007/BF01200056.

3 Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: how to remove intractability assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, STOC '88, pages 113–131, 1988. doi:10.1145/62212.62223.

4 Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, January 2014. doi:10.1137/130913687.

5 Claude Crépeau, Arnaud Massenet, Louis Salvail, Lucas Shigeru Stinchcombe, and Nan Yang. Practical relativistic zero-knowledge for NP. In *ITC*, volume 163 of *LIPIcs*, pages 4:1–4:18. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.ITC.2020.4.

6 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Mip* = RE. *Commun. ACM*, 64(11):131–138, 2021. doi:10.1145/3485628.

7 Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. How to delegate computations: the power of no-signaling proofs. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 485–494, 2014. doi:10.1145/2591796.2591809.

8 Joe Kilian. Strong separation models of multi prover interactive proofs. In *DIMACS Workshop on Cryptography*, 1990.

9 Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, October 2013. doi:10.1088/1367-2630/15/10/103002.

10 Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends® in Theoretical Computer Science*, 11(1–2):1–215, 2016. doi:10.1561/0400000068.