Beating Classical Impossibility of Position Verification

Jiahui Liu* Qipeng Liu† Luowen Qian‡

Abstract

Chandran et al. (SIAM J. Comput. '14) formally introduced the cryptographic task of position verification, where they also showed that it cannot be achieved by classical protocols. In this work, we initiate the study of position verification protocols with *classical* verifiers. We identify that proofs of quantumness (and thus computational assumptions) are necessary for such position verification protocols. For the other direction, we adapt the proof of quantumness protocol by Brakerski et al. (FOCS '18) to instantiate such a position verification protocol. As a result, we achieve classically verifiable position verification assuming the quantum hardness of Learning with Errors.

Along the way, we develop the notion of 1-of-2 non-local soundness for a natural non-local game for 1-of-2 puzzles, first introduced by Radian and Sattath (AFT '19), which can be viewed as a computational unclonability property. We show that 1-of-2 non-local soundness follows from the standard 2-of-2 soundness (and therefore the adaptive hardcore bit property), which could be of independent interest.

1 Introduction

Position verification is the central task for position-based cryptography [CGMO14], which aims to verify one's geographical location in a cryptographically secure way. The main technique is distance bounding, which infers the location assuming no faster-than-light communications from special relativity by placing timing constraints on the protocol.

The work of Chandran et al. [CGMO14] first formalized the task of position verification. They in addition showed that it is impossible to achieve via any classical protocol where all the parties are classical. Specifically, a few colluding adversaries can always efficiently convince the verifiers of an incorrect position, even with the help of computational assumptions. As a result, all known classical position verification protocols that are secure against multiple adversaries, make hardware assumptions on the adversaries [CGMO14, BDFP17].

However, it turns out the attack above does not extend when the parties exchange quantum information. The attack requires the adversaries to store the messages from the verifiers and at the same time forward them to the other adversaries, which violates the no-cloning theorem when the messages are quantum states unknown to adversaries. A long line of work [BK11, KMS11, TFKW13, Unr14, BCF+14, BCS21, DS21] explored this idea by constructing protocols with BB84 states (or other similar states [BFSS13, ABSL21, JKPP21]), and proving them to be unconditionally

*University of Texas at Austin. Email: jiahui@cs.utexas.edu

†Simons Institute for the Theory of Computing. Email: qipengliu0@gmail.com

‡Boston University. Email: luowenq@bu.edu

secure. Intuitively, these protocols get around the impossibility as these BB84 states are information theoretically unclonable when the adversaries receive them.

Downsides of Quantum Communications. There are a lot of drawbacks for using quantum communication, especially under the context of position verification.

First and foremost, transmitting quantum information with fault tolerance is much more challenging. As position verification is only meaningful with free-space (wireless) transmission, any practical protocol must be subject to a high loss. In fact, Qi and Siopsis [QS15] have shown that many known protocols stop working (lose either completeness/correctness, or soundness/security) when the error rate is above some threshold. Unlike quantum key distribution, the parties in position verification do not share an authenticated classical channel, and must follow strict timing constraints, so techniques there do not generically carry over. Furthermore, prior to our work, there was no known construction of fully loss tolerant position verification protocols against entangled adversaries, meaning being tolerant to any loss bounded away from 1.

Another issue arises when we consider high dimensions (2D or higher), which is that the parties must also send the quantum messages in the desired direction with high accuracy, or they would incur an even higher loss in transmission. In practice, this is usually mitigated via a tracking laser [UTS+07, SWF+07], although not perfectly. If the BB84 state is naively broadcasted, the adversaries could obtain one copy each and therefore completely break the protocol.

Finally, adding other properties to the protocol is more difficult and inefficient when the communication is quantum. For example, one could desire to authenticate the messages sent by the verifiers in order to protect the prover from revealing his location to other untrusted verifiers. Unfortunately, authenticating a quantum message is highly nontrivial [BCG+02, AGM21].

All of these issues can be trivially resolved if the communication is classical.

One approach to remove quantum communication is to have the verifiers and the prover preshare entanglement and use teleportation to transmit quantum messages over a classical channel. However, this generic approach consumes the entanglement and therefore is undesirable if they would like to run the protocol multiple times for a considerable time. Furthermore, it would require the parties to keep the entanglement coherent before the protocol begins, which can be expensive.

1.1 Our Results

In this work, we show how to construct position verification protocols with classical verifiers, showing that quantum communication is not necessary for position verification without hardware assumptions. Our main result is the following.

Theorem 1.1 (Restatement of Corollary 5.12)**.** *Assuming the quantum (polynomial) hardness of Learning with Errors (LWE), there exists a classically verifiable position verification (CVPV) protocol with almost perfect completeness and negligible soundness against polynomial-time adversaries without pre-shared entanglement.*

Our construction of the CVPV protocol is inspired by the (classically verifiable) proof of quantumness protocol by Brakerski et al. [BCM+18], which is proven secure under the same LWE assumption.

We also proved two variations of the theorem to handle adversaries with entanglement, albeit either assuming a stronger assumption or proven in an ideal model.

Theorem 1.2 (Restatement of Theorem 5.14)**.** *Assuming the quantum subexponential hardness of LWE, there exists a CVPV protocol with almost perfect completeness and inverse-subexponential soundness against bounded-entanglement subexponential-time adversaries.*

Theorem 1.3 (Restatement of Corollary 6.4)**.** *Assuming the quantum hardness of LWE, there exists a CVPV protocol with almost perfect completeness and negligible soundness against unbounded-entanglement polynomial-time adversaries in the quantum random oracle model.*

The quantum random oracle model (QROM), introduced by Boneh et al. [BDF+11], captures generic quantum attacks against cryptographic hash functions, modeled by random functions.

To the best of our knowledge, our protocols matches the state of the art in quantum position verification in terms of the entanglement bound. All previous protocols in the standard model (as opposed to the QROM) are not known to be secure even against an arbitrary polynomial amount of entanglement, and any protocol can be broken with an exponential amount of entanglement [BCF+14, BK11]. Furthermore, the only position verification protocol that is secure against any polynomial amount of entanglement that we are aware of is also proven in the QROM [Unr14].

In Section 6.1, we further show that there are also efficient attacks against Theorems 1.1 and 1.2 if the adversaries are allowed to pre-share more entanglement than what the entanglement bound allows.

Finally, for the other direction, we show that our assumption is somewhat minimal. The classical impossibility easily extends if the prover is classical. On a high level, if the adversaries can run in exponential time, the prover can always be simulated classically as her inputs and outputs are all classical; therefore, we would run into the classical impossibility.

Formally, we strengthen this intuition to Theorem 7.2 to show that proofs of quantumness are necessary for any construction of classically verifiable position verification, even if we relax the requirement for position verification to be sound only against classical adversaries. Since the prover response in a proof of quantumness could be simulated by a $\mathsf{PostBQP} = \mathsf{PP}$ machine[1] [Aar05b], as a consequence, it is impossible to construct unconditionally-sound proofs of quantumness (and thus classically verifiable position verification) without proving $\mathsf{PP} \not\subseteq \mathsf{BPP}$, even if we only consider position verification protocols with classical communications and quantum verifiers.

1.2 Technical Overview

Quantum Position Verification with One Quantum Message. We first recall the position verification protocol investigated by many works [BK11, KMS11, TFKW13, BCF+14, BCS21]. The protocol has the property that only one message is quantum, and the only quantum requirement on the verifiers is to generate BB84 states.

Consider that in one-dimensional spacetime, there are two verifiers V_0, V_1, wishing to verify that the prover P is located at a specific position somewhere between them. At the beginning of the protocol, V_0 sends a BB84 qubit $H^\theta |x\rangle$ (where θ, x are uniformly random bits), and V_1 sends a classical bit θ, so that they arrive at the prover's claimed position at the same time. P is supposed to measure the qubit in basis θ and return the measurement result to both verifiers. At the end, the verifiers check that the prover's measurement result is x, and that they have received the responses "in time".

[1]The idea is that one can capture simulation of the quantum prover as a sampling variant of the PostBQP problem as follows: simulate the quantum prover's next classical message given the current classical transcript of the protocol.

The intuition of the security proof is the following. Consider an adversary A_0 located in between V_0 and P, and another adversary A_1 in between P and V_1. When A_0 receives the qubit, he does not yet know the basis θ, and therefore he cannot immediately measure it. However, if they decide to wait until θ is received, then either A_0 or A_1 will not have enough time to know the measurement result and send it to the verifiers. Therefore, it seems if they want to answer correctly in time on both ends, A_0 must somehow produce two copies of the BB84 state, which is impossible as the state is information-theoretically unclonable without knowing the basis θ.

Computationally Unclonable States from Trapdoor Claw-free Functions (TCFs). As we have discussed, CVPVs require a proof of quantumness. Therefore, a natural starting point is to open up the construction of the LWE proof of quantumness protocol by Brakerski et al. [BCM+18], and look for a similar unclonability property.

The proof of quantumness protocol could be described under the 1-of-2 puzzle framework by Radian and Sattath [RS19]. In particular, both trapdoor claw-free functions (TCFs) and noisy trapdoor claw-free functions (NTCFs) can be used to instantiate 1-of-2 puzzles. However, we only have constructions of NTCFs from quantum LWE. For this overview, we will work with the more intuitive notion of TCFs and use the 1-of-2 puzzle framework in the main technical body.

A TCF family is a family of efficiently computable 2-to-1 functions $f_{\mathsf{pk}} : \{0,1\}^n \to \mathcal{Y}$. "Trapdoor" means that with the trapdoor td, one can efficiently invert the corresponding f_{pk} and get the two pre-images x_0, x_1. "Claw-free" means that without the trapdoor, it is hard for any polynomial-time quantum algorithms to find a collision for a random f_{pk}.

The proof of quantumness protocol works as follows. The verifier starts by sampling pk along with the trapdoor td, and sends pk to the prover. The prover prepares a uniform superposition over $\{0,1\}^n$, computes f_{pk} on the superposition coherently, measures the image register to obtain $y \in \mathcal{Y}$, and sends y as his response. As f_{pk} is 2-to-1, the residual state of the prover is

$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle), \tag{1}$$

where x_0, x_1 are the two pre-images of y. The protocol concludes with the verifier sending a uniformly random challenge b to the prover, and the prover measuring (1) either in the standard basis or the Hadamard basis.

If the prover is asked to measure in the standard basis, the measurement outcome will be a uniformly random x which is either x_0 or x_1. If the prover is asked to measure in the Hadamard basis, the measurement outcome will be a uniformly random d such that $d \cdot (x_0 \oplus x_1) = 0$ over $\mathbb{F}_2^n$. Since the verifier has the trapdoor, he can obtain x_0, x_1 by inverting y, and thus check whether the measurement outcome satisfies the requirements above.

As for security, we need an additional property called *adaptive hardcore bit*, which says that any efficient quantum algorithm given pk, cannot produce y, x, d that passes the two checks simultaneously with probability significantly higher than ½, i.e. $f_{\mathsf{pk}}(x) = y$, $d \cdot (x_0 \oplus x_1) = 0$, and $d \neq 0$. To see that this implies the proof of quantumness property, assume a classical prover can pass this proof of quantumness protocol with probability 1, then we can always extract both x and d with probability 1 by simply rewinding the classical prover.

In fact, the adaptive hardcore bit property also implies that the state (1) must be computationally unclonable. This is simply because if somehow we can prepare two copies of this state, then measuring two copies in two bases will yield both x and d. This computational unclonability property has also been observed and used in prior works, in particular in the context of semi-quantum money [RS19] and two-tier quantum lightning [KNY21]. Later we will see that the security proof for our CVPV protocol requires a stronger variant of computational unclonability than the ones considered in these works.

Constructing CVPV. Given the setup, a natural idea for achieving CVPV is that instead of sending an unclonable state prepared by V_0, perhaps we can ask the prover (and hopefully also the adversaries) to prepare a quantum state that she herself cannot clone, similar to that in the proof of quantumness protocol. Specifically, consider the CVPV protocol, where V_0 sends pk and V_1 sends b with the same timing as before. In the end, they check that whether they have received the same prover response in time and whether the prover's measurement outcome passes the proof of quantumness check. On the other hand, the prover in CVPV will run the prover in the proof of quantumness protocol and output y, ans, where y is the measured image of the superposition evaluation, and ans is the measurement outcome in the basis specified by b.

We now show that this construction already seems to get around the classical impossibility. The attack from the impossibility is following: A_0, A_1 forwards the classical messages pk, b to each other, and at the end, they run the honest prover and send the output. However, in this protocol, since the measurement performed by the prover has some nontrivial min-entropy, the verifiers will get two different responses with constant probability! It is also not clear whether this computation could be simulated (almost) deterministically with shared randomness. Certainly, if it could be simulated classically, then it would be breaking the proof of quantumness property.

Unfortunately, it turns out that a different attack completely breaks this CVPV protocol. When A_0 receives pk, he can simply runs the honest prover twice — once on $b = 0$ and once on $b = 1$. He obtains y_0, ans_0 for $b = 0$ and y_1, ans_1 for $b = 1$, and sends both of them to A_1. On the other hand, A_1 simply forwards b. Later, when both of them receive the message from each other, they pick y_b, ans_b as their responses to the verifiers. It is not hard to show that this strategy simulates the prover perfectly.

We observe that in order for this attack to work, it is crucial that the adversaries can pick y *after* seeing b, which is impossible in the proof of quantumness protocol. Therefore, to prevent this attack, our idea is to "nudge" the prover to the left, so that she can commit to y *before* seeing b. More formally, the protocol is the same as before but the timing constraints are changed. In particular, the verifiers make sure that the message pk reaches the prover a bit earlier than b, and at the end, they check that she should output y as soon as she receives pk (and before she receives b). We refer the readers to Figure 1 for an illustration of the timing.

Proving Soundness of CVPV. It turns out that with this simple fix, this CVPV can be proven secure. In Claim 4.7, we show that according to the timing constraints, we can again, without loss of generality, assume that there are two adversaries A_0, A_1, and that A_0 upon receiving pk needs to output y to the verifiers *immediately*, and after they receive a private communication from each other, they are supposed to produce two ans's to pass the verification.

We first consider a restricted set of adversarial strategies, called *challenge-forwarding* adversaries, where the only restriction is that A_1 upon receiving b simply forwards b and does nothing else. We claim that the success probability for challenge-forwarding adversaries cannot be significantly higher than ¾.

We now show that this suffices to show that the success probability for *any* adversarial strategy without pre-shared entanglement cannot be significantly higher than ¾. The proof is that assume

(A_0, A_1) breaks the CVPV with probability noticeably higher than ¾, we construct a challenge-forwarding adversary (B_0, B_1) with the same success probability, which leads to a contradiction. The construction of the reduction is similar to the attack for the first CVPV construction. B_0, upon receiving pk, runs A_0 on pk (and commits y) and simultaneously A_1 twice — once on $b = 0$ and once on $b = 1$ — and sends the residual state to the other party. We can run A_1 twice as they do not pre-share entanglement. Later, when both of them learn b, they can pick the correct execution to finish simulating (A_0, A_1).

A (Computational) Non-Local Game for TCFs. What is left to be shown is that even challenge-forwarding adversaries cannot break the CVPV protocol. In Theorem 4.9, we show that for our protocol, what the adversaries can do is more or less equivalent to the following *computational* (two-player) non-local game:

- The game begins by announcing a TCF public key pk.
- Two (computationally bounded) players B and C upon receiving pk, agree on a classical "commitment" y. They then prepare a possibly entangled bipartite state ρ_{BC} between themselves, after which they are separated.
- A *single* challenge b is then sampled uniformly at random and announced to B and C separately.
- B and C produce two answers ans_B and ans_C using ρ_B or ρ_C separately, and win the non-local game if both answers pass the proof of quantumness check with respect to pk, y, b.

Another way to view this game is that it is the same as the TCF proof of quantumness protocol, except that after halfway, we ask the prover to run two copies of himself, i.e. split himself into two executions and finish each execution separately with the same verifier randomness. If the prover's internal state was clonable, then the best prover's success probability should never decrease after the transformation. Therefore, this can also be viewed as a computational unclonability property.

To prove the non-local soundness, assume that a strategy wins this non-local game significantly higher than ¾. We construct an algorithm breaking the adaptive hardcore bit property, by asking B challenge 0 (produce x) and C challenge 1 (output d). On a high level, this reduction works because in a non-local game, the measurements made by B and C are on disjoint registers, and thus must be compatible no matter which challenges are given to them.

We now provide an informal proof that this reduction works for any non-signaling players. A strategy is non-signaling if the marginal distribution for one player is independent of what the other player does, and the no signaling principle says that any bipartite measurement of a quantum state is non-signaling. Let W_0, W_1 be the events where B or C produces a correct answer respectively in the non-local game. We can rewrite the success probability of the non-local game to be $p := \Pr[W_0 \wedge W_1]$. Then

$$p = \frac{1}{2}\Pr[W_0 \wedge W_1 | b = 0] + \frac{1}{2}\Pr[W_0 \wedge W_1 | b = 1] \leq \frac{1}{2}\Pr[W_0 | b = 0] + \frac{1}{2}\Pr[W_1 | b = 1].$$

On the other hand, let W_0', W_1' be the events where B or C produces a correct answer respectively in the reduction, where B receives challenge 0 and C receives challenge 1. Then the success probability of the reduction is $p' := \Pr[W_0' \wedge W_1']$. $p' \leq \frac{1}{2} + \mathsf{negl}$ since the reduction is efficient, and by union bound,

$$p' = 1 - \Pr[\neg W_0' \vee \neg W_1'] \geq 1 - \Pr[\neg W_0'] - \Pr[\neg W_1'] = \Pr[W_0'] + \Pr[W_1'] - 1.$$

Notice that $\Pr[W_0'] = \Pr[W_0 | b = 0]$ by construction and the no signaling principle, and similarly $\Pr[W_1'] = \Pr[W_1 | b = 1]$. The conclusion $p \leq \frac{3}{4} + \mathsf{negl}$ follows by rearranging the terms.

The computational unclonability requirements in prior works [RS19, KNY21] cannot be cast as a non-local game, since there the two players need to answer different challenges instead of the same one. Therefore, by adaptive hardcore bit property, the game is hard even if the two players can communicate. We think that this computational non-local hardness that we achieve could potentially have applications to other quantum cryptography relying on the no-cloning principle.

Soundness Amplification via Parallel Repetition. So far, we have shown how to construct a CVPV with soundness ¾ against adversaries without pre-shared entanglement.

To achieve negligible soundness, one natural attempt is to do sequential repetition. However, sequential repetitions are undesirable in our setting as (1) sequential repetitions will undesirably increase the number of rounds/time/complexity of the final protocol; (2) more crucially, adversaries can take advantages of a multiple round protocol and use quantum communication to share some entanglement even if they have no pre-shared entanglement at the beginning of the protocol. Combining with the attack that we give in Section 6.1, one can show that with sequential repetitions, the soundness does not decrease at all!

Therefore, we turn to consider parallel repetitions, which traditionally have been more technically challenging than sequential repetitions under numerous different contexts. One difficulty is that our CVPV protocol can be viewed as a four-message private-coin interactive argument with additional structures, and therefore known transformations for interactive arguments do not apply. Another difficulty is that a common technique for proving parallel repetition for private-coin arguments is to perform rejection sampling, which in our case of proving parallel repetition of CVPV, would lead to either communication or pre-shared entanglement between the adversaries, neither of which is allowed for this setting.

The key idea is that instead of proving a parallel repetition theorem for the CVPV protocol, we first establish a parallel repetition theorem for the TCF non-local game, where at least the two players are allowed to share entanglement. We then construct a CVPV protocol with a stronger variant of the non-local game. However, we still need to be careful about the reduction since in the non-local game, two players cannot communicate after y is sent.

We first consider the parallel repetition where the non-local game is repeated k times in parallel, except that we use a single challenge b for all the executions. We show that the non-local soundness can be decreased to ½ if k is large enough using known results [RS19] (which in turn uses a classical parallel repetition theorem [CHS05]). The ½ soundness here is tight as the adversaries can always guess b correctly with probability ½.

We next consider a second parallel repetition where the strengthened game from above is repeated k' times in parallel, and this time we use fresh random challenges for all the executions. As the strengthened game has soundness ½, this implies that the two quantum predicates (standard basis test and Hadamard basis test) satisfy computational orthogonality, similar to the one that has appeared under a different application of parallel repetitions for TCFs, which is quantum delegation [ACGH20, CCY20]. Therefore, using the ideas from those works, we show that the non-local soundness decreases exponentially in k'.

Finally, using the same reduction from non-local games to CVPV as before, we show that we can achieve the CVPV protocol with negligible soundness.

Handling Entangled Adversaries. We have proven that our protocol is negligibly sound against adversaries without pre-shared entanglement. It turns out that our protocol is similar enough to the previous quantum position verification that a lot of techniques there can be naturally ported here as well.

Using a standard trick [Aar05a, TFKW13], we can show that the protocol can be made secure against any adversaries with an a-priori-chosen polynomial amount of pre-shared entanglement, albeit requiring subexponential hardness of quantum LWE, as the reduction for parallel repetition needs to run in subexponential time.

On the other hand, our protocol can also be attacked with n EPR pairs where n is the length of the output of f_{pk}. The attack is very similar to the attack for the quantum position verification protocol we give in the beginning. The adversaries simply prepare the state (1) honestly (which we recall is the only non-timing-wise change to the protocol) and perform the attack against the base protocol. In particular, they teleport the state using EPR pairs to perform measurements in a homomorphic way, whose outcome later they can recover with one round of communication. Attacking the protocol after parallel repetition can be done by running the attack above in parallel.

Finally, we modify the CVPV protocol into the QROM to prove that it is sound against unbounded entanglement, where the modification is very similar to how Unruh [Unr14] modifies the base position verification protocol into the QROM. On a high level, the attack for the previous protocol works because the honest prover's operation after committing y is a Clifford. With Unruh's transformation, the operation now involves evaluating a random function, which cannot be efficiently computed by a Clifford circuit. The security proof in the QROM from Unruh's work also carries over, except here we reduce the adversarial strategy with entanglement against the QROM CVPV, to the TCF non-local game after parallel repetition (in the standard model), instead of a monogamy-of-entanglement game [TFKW13].

1.3 Future Directions

High Dimensional Position Verification. We conjecture that the following construction, inspired by the position verification protocol of Unruh [Unr14], could be secure in higher dimensions under the quantum random oracle model (QROM) using the ideas from Unruh:

1. V_0 broadcasts pk.
2. $V_0, ..., V_n$ sample uniformly random strings $x_0, ..., x_n$ respectively and broadcast them. The timing is done so that these strings arrives at the prover a bit later than pk.
3. At the end, the $(n+1)$ verifiers check that the prover answers arrive in time, and passes the check with respect to challenge $H(x_0 \oplus \cdots \oplus x_n)$, where H is the random oracle.

Time-Entanglement Trade-Offs: Upper and Lower Bounds. Classically verifiable position verification protocols have the curious feature of being completely broken against classical adversaries with unbounded computational power, as they can simulate the honest quantum execution. On the other hand, our protocol can be efficiently broken using a linear amount of entanglement but secure against adversaries with bounded entanglement. This suggests that there may be some time-entanglement trade-offs for the optimal attack. Clearly, the trivial trade-off to attack the CVPV after parallel repetition is that the adversaries can use their entanglement to break some copies, and brute-force the rest of the copies. It is interesting whether there is a significantly better time-entanglement trade-offs that could be achieved for attacking this protocol or classically verifiable position verification protocols in general.

For the other direction, we also wonder if there is a tighter lower bound on the entanglement than what we prove.

Decreasing Quantum Memory for the Prover. We have shown in Theorem 5.14 that assuming subexponential hardness of quantum LWE, we can construct classically verifiable position verification protocols that is secure against any a-priori bounded entanglement. Unfortunately, in our protocols, even the honest prover needs to keep his quantum memory (which is of length $\tilde{O}(\lambda)$ when entanglement bound is 0) coherent for some time, and the size of the quantum memory is even larger than the entanglement bound. Indeed, we have also shown that if the adversaries share as much entanglement as the size of the honest prover's quantum memory, then the protocol can be efficiently broken. However, the adversaries might need to keep the entanglement coherent long before the protocol begins, and this might be much longer than the duration needed by the honest prover.

Nevertheless, it would be interesting if we can avoid this drawback. We therefore ask whether it is possible to come up with provably secure CVPV protocols where the honest prover's quantum memory is smaller than the entanglement bound in the standard model, or maybe even without any quantum memory at all.

Weakening the Assumption. We show how to achieve CVPV assuming quantum hardness of LWE, which is a cryptographic assumption. Can we relax this assumption further? One possible assumption is the existence of a classically verifiable quantum sampling task satisfying some requirements.

Acknowledgements

The authors would like to thank Ran Canetti and Shih-Han Hung for their helpful discussions. The authors would also like to thank the anonymous reviewers from ITCS 2022 and QIP 2022 for their kind and thoughtful comments.

Jiahui Liu is supported by the NSF and Scott Aaronson's Simons Investigator award.Qipeng Liu is supported by the Simons Institute for the Theory of Computing, through a Quantum Postdoctoral Fellowship.Luowen Qian is supported by DARPA under Agreement No. HR00112020023.

2 Notations

We refer the readers to [NC10] on basic quantum information and computation concepts. As our work only works with the Learning with Error (LWE) assumption indirectly, we refer the readers to [BCM+21, Section 2.3] for further information on the assumption.

We call a function $f : \mathbb{N}^+ \to \mathbb{R}^{\geq 0}$ negligible ($f(n) = \mathsf{negl}(n)$) if for any $g(n) = \mathsf{poly}(n) := n^{O(1)}$, $f(n) \leq 1/g(n)$ for all sufficiently large n. Throughout this paper, we use λ to denote the security parameter unless specified otherwise.

Let $\mathcal{H}$ denote a finite-dimensional Hilbert space. We use Dirac notation to express vectors which represent pure states, for example $|\psi\rangle$. We let $\mathcal{S}(\mathcal{H})$ denote the set of all density operators, which are positive semidefinite operators on $\mathcal{H}$ with trace 1, and represent mixed states.

Quantum registers simply mean a collection of qubits in a given state. Consider a mixed state ρ_{AB} where the qubits are partitioned into sets A and B. We denote ρ_A to refer to the qubits in A in state ρ_{AB}.

The quantum random oracle model (QROM) [BDF+11], is the model where a single function $f : \mathcal{X}_\lambda \to \{0,1\}^\lambda$ is sampled uniformly at random. All parties get oracle access to the unitary $\mathcal{O}$ such that $\mathcal{O}|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ for all $x \in \mathcal{X}_\lambda, y \in \{0,1\}^\lambda$.

3 1-of-2 Puzzles and Non-Local Soundness

3.1 1-of-2 Puzzles

Definition 3.1 (1-of-2 Puzzles [RS19, Definition 2.1])**.** *A 1-of-2 puzzle $\mathcal{Z}$ is a tuple of four efficient algorithms* ($\mathsf{KeyGen}, \mathsf{Obligate}, \mathsf{Solve}, \mathsf{Ver}$)*, where:*

The key generation algorithm KeyGen*, is a classical algorithm that on security parameter 1^λ, outputs a public key* pk *and a secret key* sk*:* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*.*

The obligation algorithm $\mathsf{Obligate}$*, is a quantum algorithm that on input a public key* pk*, outputs a classical string y called the obligation and a quantum state ρ:* $(y, \rho) \leftarrow \mathsf{Obligate}(\mathsf{pk})$*.*

The 1-of-2 solver Solve*, is a quantum algorithm that on input a public key* pk*, an obligation y, a quantum state ρ and a challenge bit b, outputs a classical answer* ans*:* $\mathsf{ans} \leftarrow \mathsf{Solve}(\mathsf{pk}, y, \rho, b)$*.*

The verification algorithm Ver*, is a classical deterministic algorithm that on input a secret key* sk*, an obligation y, a challenge bit b and an answer* ans*, it outputs 0 or 1:* $\mathsf{Ver}(\mathsf{sk}, y, b, \mathsf{ans}) \in \{0,1\}$*.*

Furthermore, it satisfies the following completeness and 2-of-2 soundness.

Completeness[2]*: Let c be some function $c : \mathbb{N} \to \mathbb{R}$. We say that the 1-of-2 puzzle $\mathcal{Z}$ has completeness c if*

$$\Pr_{b \leftarrow \{0,1\}}\left[\mathsf{Ver}(\mathsf{sk}, y, b, \mathsf{ans}) = 1 : \begin{array}{c}(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (y, \rho) \leftarrow \mathsf{Obligate}(\mathsf{pk}) \\ \mathsf{ans} \leftarrow \mathsf{Solve}(\mathsf{pk}, y, \rho, b)\end{array}\right] \geq c(\lambda).$$

2-of-2 Soundness[3]*: Let $s : \mathbb{N} \to [0,1]$ be a function. We say that the 1-of-2 puzzle $\mathcal{Z}$ has 2-of-2 soundness s if for any QPT 2-of-2 solver $\mathcal{T}$, there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\Pr\left[\mathsf{SOLVE2}_{\mathcal{T},\mathcal{Z}}(1^\lambda) = 1\right] \leq s(\lambda) + \mathsf{negl}(\lambda),$$

[2] Our completeness slightly differs from the original definition in the sense that the negligible term is dropped from the definition, since unlike soundness, there is no additional quantifier on the adversary. This change is made also to signify the imperfect completeness.

[3] We use a slightly different notion of 2-of-2 soundness instead of the 2-of-2 hardness in the original work. In particular, the original definition of having 2-of-2 hardness $(1-h)$ is equivalent to having 2-of-2 soundness h.

where the 2*-of-*2 *solving game* $\mathsf{SOLVE2}_{\mathcal{T},\mathcal{Z}}(1^\lambda)$ *is defined as the following:*

1. *The challenger runs* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$.
2. *The* 2*-of-*2 *solver* $\mathcal{T}$ *receives public key* pk *and outputs a triple of classical messages* $(y, \mathsf{ans}_0, \mathsf{ans}_1)$.
3. *The game outputs 1 if and only if (note that* Ver *is a classical deterministic function)*

$$\mathsf{Ver}(\mathsf{sk}, y, 0, \mathsf{ans}_0) = 1 \wedge \mathsf{Ver}(\mathsf{sk}, y, 1, \mathsf{ans}_1) = 1.$$

We say $\mathcal{Z}$ *is a* (c, s)*-*1*-of-*2 *puzzle if it has completeness* c *and* 2*-of-*2 *soundness* s.

In the same work [RS19], they also show that NTCFs (Definition A.1) implies a 1-of-2 puzzle. We further elaborate the connection between NTCFs and 1-of-2 puzzles in Appendix A.

Theorem 3.2 ([RS19, Theorem 2.2] and Theorem A.2)**.** *An NTCF implies a* $(1 - \mathsf{negl}, \frac{1}{2})$*-*1*-of-*2 *puzzle. Therefore,* $(1 - \mathsf{negl}, \frac{1}{2})$*-*1*-of-*2 *puzzles exist assuming quantum hardness of LWE.*

3.2 1-of-2 Puzzle as a Non-Local Game

We now define a non-local game for 1-of-2 puzzles, and show the connection between the success probability of the non-local game and the 2-of-2 soundness of the underlying 1-of-2 puzzle.

Definition 3.3 (Non-Local Games of 1-of-2 Puzzles)**.** *Let* $\mathcal{Z}$ *be a* (c, s)*-*1*-of-*2 *puzzle. The non-local solving game* $\mathsf{NON\text{-}LOCAL\text{-}SOLVE}_{\mathcal{W},\mathcal{Z}}(1^\lambda)$ *for any non-local player* $\mathcal{W} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$*, where* $\mathcal{A}, \mathcal{B}, \mathcal{C}$ *are three quantum algorithms, is defined as follows:*

- *The challenger runs* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$.
- *The algorithm* $\mathcal{A}$ *receives public key* pk *and outputs a classical obligation* y *together with a quantum state* $\sigma_{BC} \in \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_C)$: $(y, \sigma_{BC}) \leftarrow \mathcal{A}(\mathsf{pk})$. *It commits* y *to the challenger.*

  $\mathcal{B}$ *receives* σ_B *and* $\mathcal{C}$ *receives* σ_C.
- *The challenger samples a challenge bit* $b \leftarrow \{0, 1\}$ *and sends* b *to both* $\mathcal{B}$ *and* $\mathcal{C}$.
- $\mathcal{B}$ *and* $\mathcal{C}$ *perform some local computations and then output* $\mathsf{ans}_{\mathcal{B}} \leftarrow \mathcal{B}(\sigma_B, b)$ *and* $\mathsf{ans}_{\mathcal{C}} \leftarrow \mathcal{C}(\sigma_C, b)$ *respectively.*
- *The game outputs* 1 *if and only if both* $\mathcal{B}, \mathcal{C}$ *answer correctly, i.e.*

$$\mathsf{Ver}(\mathsf{sk}, y, b, \mathsf{ans}_{\mathcal{B}}) = 1 \wedge \mathsf{Ver}(\mathsf{sk}, y, b, \mathsf{ans}_{\mathcal{C}}) = 1.$$

Definition 3.4 (1-of-2 Non-Local Soundness)**.** *Let* $\tau : \mathbb{N} \to \mathbb{R}$ *be an arbitrary function. We say that the* 1*-of-*2 *puzzle* $\mathcal{Z}$ *has* 1*-of-*2 *non-local soundness* τ *if for any QPT non-local player* $\mathcal{W}$*, there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\Pr\left[\mathsf{NON\text{-}LOCAL\text{-}SOLVE}_{\mathcal{W},\mathcal{Z}}(1^\lambda) = 1\right] \leq \tau(\lambda) + \mathsf{negl}(\lambda).$$

We now establish the connection between 1-of-2 non-local soundness and 2-of-2 soundness.

Theorem 3.5. *Let $\mathcal{Z}$ be a 1-of-2 puzzle with 2-of-2 soundness s. $\mathcal{Z}$ has 1-of-2 non-local soundness $\tau = (s+1)/2$.*

Proof. Let $\mathcal{W} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ be any QPT non-local player for $\mathsf{NON\text{-}LOCAL\text{-}SOLVE}_{\mathcal{W},\mathcal{Z}}(1^\lambda)$ that achieves success probability $\tau = \tau(\lambda)$. Let $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$ and $(y, \sigma_{BC}) \leftarrow \mathcal{A}(\mathsf{pk})$. Let $\mathsf{PB}_{\mathsf{sk},y,b}, \mathsf{PC}_{\mathsf{sk},y,b}$ be the projection acting on register B, C respectively corresponding to the predicate $\mathsf{Ver}(\mathsf{sk}, y, b, \mathsf{ans}) = 1$ where ans is either the output of $\mathcal{B}$ or $\mathcal{C}$. Using this notation, we can rewrite the success probability:

$$\tau = \Pr\left[\mathsf{NON\text{-}LOCAL\text{-}SOLVE}_{\mathcal{W},\mathcal{Z}}(1^\lambda) = 1\right] = \mathop{\mathbb{E}}_{\mathsf{KeyGen},\mathcal{A},b\leftarrow\{0,1\}} \mathrm{Tr}\left[\left(\mathsf{PB}_{\mathsf{sk},y,b} \otimes \mathsf{PC}_{\mathsf{sk},y,b}\right)\sigma_{BC}\right].$$

Here the subscripts KeyGen and $\mathcal{A}$ stands for the randomness of sampling $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$ and the measurement randomness from $(y, \sigma_{BC}) \leftarrow \mathcal{A}(\mathsf{pk})$.

Expanding the expectation on b and using the linearity of expectation and the trace operator, we get

$$2\tau = \mathop{\mathbb{E}}_{\mathsf{KeyGen},\mathcal{A}} \mathrm{Tr}\left[\left(\mathsf{PB}_{\mathsf{sk},y,0} \otimes \mathsf{PC}_{\mathsf{sk},y,0} + \mathsf{PB}_{\mathsf{sk},y,1} \otimes \mathsf{PC}_{\mathsf{sk},y,1}\right)\sigma_{BC}\right].$$

Since $\mathsf{PB}_{\mathsf{sk},y,b}, \mathsf{PC}_{\mathsf{sk},y,b} \preccurlyeq \mathbb{I}$ for any sk, y, b, we have:

$$\begin{aligned}
2\tau &\le \mathop{\mathbb{E}}_{\mathsf{KeyGen},\mathcal{A}} \mathrm{Tr}\left[\left(\mathsf{PB}_{\mathsf{sk},y,0} \otimes \mathbb{I} + \mathbb{I} \otimes \mathsf{PC}_{\mathsf{sk},y,1}\right)\sigma_{BC}\right] \\
&\le \mathop{\mathbb{E}}_{\mathsf{KeyGen},\mathcal{A}} \mathrm{Tr}\left[\left(\mathbb{I} \otimes \mathbb{I} + \mathsf{PB}_{\mathsf{sk},y,0} \otimes \mathsf{PC}_{\mathsf{sk},y,1}\right)\sigma_{BC}\right] \\
&= 1 + \mathop{\mathbb{E}}_{\mathsf{KeyGen},\mathcal{A}} \mathrm{Tr}\left[\left(\mathsf{PB}_{\mathsf{sk},y,0} \otimes \mathsf{PC}_{\mathsf{sk},y,1}\right)\sigma_{BC}\right],
\end{aligned}$$

where the second inequality is simply due to the fact that for any $P, Q \preccurlyeq \mathbb{I}$, $0 \preccurlyeq (\mathbb{I} - P) \otimes (\mathbb{I} - Q) = \mathbb{I} \otimes \mathbb{I} - P \otimes \mathbb{I} - \mathbb{I} \otimes Q + P \otimes Q$. Therefore,

$$\mathop{\mathbb{E}}_{\mathsf{KeyGen},\mathcal{A}} \mathrm{Tr}\left[\left(\mathsf{PB}_{\mathsf{sk},y,0} \otimes \mathsf{PC}_{\mathsf{sk},y,1}\right)\sigma_{BC}\right] \ge 2\tau - 1.$$

Now we construct a 1-of-2 puzzle solver $\mathcal{T}$, whose success probability is exactly the left hand side of the inequality above:

1. $\mathcal{T}$ upon receiving pk, runs $\mathcal{A}(\mathsf{pk})$ to produce (y, σ_{BC}).
2. It runs $\mathcal{B}$ and $\mathcal{C}$ on ρ with different challenge bits $0, 1$ respectively, and outputs $\mathsf{ans}_0 = \mathsf{ans}_{\mathcal{B}}, \mathsf{ans}_1 = \mathsf{ans}_{\mathcal{C}}$.
3. It outputs $(y, \mathsf{ans}_0, \mathsf{ans}_1)$.

$\mathcal{T}$ solves 2-of-2 puzzle if and only if both $\mathsf{ans}_0, \mathsf{ans}_1$ pass the verification, which in turn is at least $2\tau - 1$ as argued above.

On the other hand, since $\mathcal{W}$ is efficient, so is $\mathcal{T}$. Therefore, the success probability of $\mathcal{T}$ is at most $s + \mathsf{negl}$. Thus, $2\tau - 1 \le s + \mathsf{negl}$. We conclude the proof by simply rearranging the terms. □

Combined with Theorem 3.2, we get the following corollary:

Corollary 3.6. *Assuming the quantum hardness of LWE, there exists a 1-of-2 puzzle that has completeness $1 - \mathsf{negl}$ and 1-of-2 non-local soundness ¾.*

4 Towards Position Verification

In this section, we formally introduce the model and the definition of position verification. Starting with a 1-of-2 puzzle with completeness c and 1-of-2 non-local soundness τ, we then show how to achieve a position-robust position verification with completeness c and soundness τ against adversaries without entanglement. Combining with the 1-of-2 puzzle from LWE, this gives a non-trivial position verification with almost perfect completeness and constant soundness. We defer further decreasing soundness and handling entanglement to the next section.

4.1 The Vanilla Model

We restrict our attention to position verification in one dimension. We consider the same model as the Vanilla Model (the standard model) from [CGMO14], but augment it with quantum capabilities for the prover and the adversaries, as we only work with classically verifiable protocols. We have three types of parties: prover, verifier, and adversary.

- Space and time are continuous.
- The clocks of all parties are synchronized.
- Before the protocol begins, all parties are given as input the position of all verifiers, the claimed position of the prover, and a security parameter λ.
- The prover and adversaries have quantum computation capabilities, whereas the verifiers are entirely classical.
- The verifiers share a private trusted classical communication channel.
- All prover-verifier communications are classical broadcast messages. However, adversaries can send directional messages to any specific verifier that expects to receive a broadcast instead.
- Adversaries can also use a private (quantum) communication channel, so that the verifiers will not detect any malicious activity.
- All computations are done instantaneously, but all messages in all channels travel at speed 1 (the speed of light).

We first recall the usual completeness and soundness requirements of position verification protocols. Since physical space satisfies translational symmetry, without loss of generality, we assume the claimed position of the prover is fixed a priori (say to be 1), instead of being an input to the parties.

Definition 4.1. *Let $c : \mathbb{N}^+ \to \mathbb{R}$. We call a position verification protocol to have* completeness *c, if the prover, located at 1, can convince the verifiers with probability at least $c(\lambda)$ for any security parameter λ.*

Definition 4.2. *An* adversarial strategy *is specified by a list of pairs (p_i, A_i), where p_i is the location of adversary i and A_i is the interactive (quantum) Turing machine it runs. A family of adversarial strategies is a list of adversarial strategies indexed by the security parameter λ.*

In this work, we focus on the setting where the families can be efficiently uniformly generated, i.e. there exists a deterministic polynomial-time Turing machine M such that a useful description of the adversarial strategy for λ can be efficiently generated by M on input 1^λ. We abuse the notation to omit "family" whenever the context is clear.

Definition 4.3. *Let $s : \mathbb{N}^+ \to \mathbb{R}$ and $\mathcal{S}$ be any set of adversarial strategies. We call a position verification protocol to have* soundness *s against $\mathcal{S}$, if for any family of adversarial strategies $S \in \mathcal{S}$, using strategy S can convince the verifiers with probability at most $s(\lambda) + \mathsf{negl}(\lambda)$ for some negligible function $\mathsf{negl}(\cdot)$. If $s = 0$, we call the protocol to have negligible soundness against $\mathcal{S}$.*

In the literature, we usually consider one round protocols where the prover receives two messages, performs one computation, and sends two responses. In this case, it is easy to see that for soundness, instead of taking $\mathcal{S}$ to be the largest possible set of adversarial strategies, which is all strategies that could occupy the entire space outside of the claimed position, it is equivalent to only consider strategies with two adversaries, one on each side.

4.2 Position Robustness

We now introduce the position-robust version of these requirements. Again since the spacetime we consider here is unitless, we without loss of generality assume the prover claims that it is somewhere in $(1, 2)$.

Definition 4.4. *Let $c : \mathbb{N}^+ \to \mathbb{R}$. We call a position verification protocol to have* position-robust completeness *c, if the prover, located at* anywhere *in $(1, 2)$, can convince the verifiers with probability at least $c(\lambda)$ for all λ.*

This notion is natural from the practical point of view. Since the position measurement device always has some errors, a non-robust position verification protocol can never have any practical value. Another reason we consider this notion is that we do not know how to make our protocol non-robust — later we will see that in our construction, neither the prover nor the adversaries can occupy point 2.

Naturally, we should modify the set of adversarial strategies that we should consider for soundness under the position-robust setting.

- The most general set of strategies, denoted by $\mathcal{R}$, is the set of strategies with the only restriction that all positions lie in $(-\infty, 1) \cup (2, +\infty)$. We allow the adversaries to do quantum setup before the protocol begins, including setting up entanglement between them.

  We do not consider adversaries at 1 or 2; that is, we do not allow the prover nor the adversaries to be at point 1 or 2. While it might be interesting to try to extend either completeness or soundness to close this small gap, these two single points have measure 0 and thus we consider it to be practically irrelevant — indeed everything at the end will be subject to the precision of the devices being used, and the location gap caused by the device errors will greatly exceed these two points of failure.

- The set of polynomially bounded strategies (with pre-shared entanglement), denoted by $\mathcal{R}_P$, is the subset of $\mathcal{R}$ with further restrictions that there exists some polynomial $p(\cdot)$, such that the running time of the Turing machine that generates the strategy as well as that of every adversary is bounded by $p(\lambda)$.

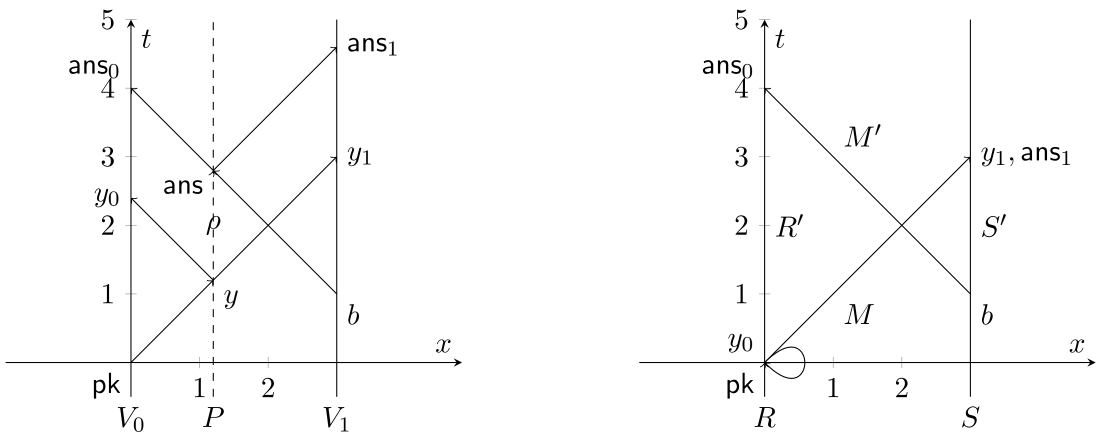

Figure 1: Spacetime diagrams for PRPV (left) and the possible adversarial behaviors shown in Claim 4.7 (right). ρ indicates the time interval for the prover to keep his quantum memory, and R, R', S, S', M, M' indicate the quantum registers in the adversarial behavior. The small loop indicates that A_0 immediately outputs y_0 upon receiving pk.

With polynomial hardness assumptions, $\mathcal{R}_P$ is the largest set of strategies that we will consider for the soundness of a *classically verifiable* protocol, as an unbounded strategy from $\mathcal{R}$ can always convince the verifiers by simulating the quantum prover classically, and then using the attack strategy from Theorem 7.2.

- The set of bounded-entanglement strategies, denoted by $\mathcal{R}_L$ for some function $L : \mathbb{N}^+ \to \mathbb{N}$, is the subset of $\mathcal{R}_P$ with further restrictions that the total *quantum* communication between the adversaries *before* the protocol begins, is bounded by $L(\lambda)$, which is an upper bound on the entanglement (measured via von Neumann entanglement entropy) that the adversaries share before the protocol begins.

Observe that for 1D, it suffices to consider at most two verifiers — one on the left of the prover, the other on the right of the prover. Indeed, if there are more than one verifiers on one side of the prover, the verifier that is closest to the prover can simulate all the interactions for the other verifiers.

Let the verifier on the left be V_0, and the one on the right be V_1. We remark that for position-robust position verification, in general V_0 could be anywhere in $(-\infty, 1]$ and V_1 could be anywhere in $[2, +\infty)$. However, since for all intents and purposes, sending a message to the right at (x, t) is equivalent to sending it at $(x - \delta, t - \delta)$ (and vice versa), we can without loss of generality assume that V_0 and V_1 are at 0 and 3.

4.3 The Base Protocol

Construction 4.5 (PRPV Protocol)**.** *Let* $\mathcal{Z} = (\mathsf{KeyGen}, \mathsf{Obligate}, \mathsf{Solve}, \mathsf{Ver})$ *be a* 1*-of-*2 *puzzle. We define the* $\mathsf{PRPV}_\mathcal{Z} = \mathsf{PRPV}_\mathcal{Z}(\lambda)$ *protocol as follows:*

1. *Starting at* $t = 0$*,* V_0 *samples a pair of keys* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*, broadcasts* pk*, and waits to receive* y_0 *from the prover before time* $t < 4$*, and* ans_0 *at time* $t = 4$*.*

2. *At $t = 1$, V_1 samples a uniformly random bit b and broadcasts it, and waits to receive y_1 from the prover at time $t = 3$, and ans_1 at time $t \leq 5$.*

3. *At $t = p_P$, the prover, located at $p_P \in [1, 2)$, receives pk, it prepares $(y, \rho) \leftarrow \mathsf{Obligate}(\mathsf{pk})$ and broadcasts y.*

4. *At $t = 4 - p_P$, the prover receives b, computes $\mathsf{ans} \leftarrow \mathsf{Solve}(\mathsf{pk}, y, \rho, b)$ and broadcasts ans.*

5. *At $t \leq 5$ when the verifiers receive all the messages in time described above, they check that $y_0 = y_1$ and $\mathsf{ans}_0 = \mathsf{ans}_1$, and the answers pass the test:*

$$\mathsf{Ver}(\mathsf{sk}, y_0, b, \mathsf{ans}_0) = 1 \, \wedge \, \mathsf{Ver}(\mathsf{sk}, y_1, b, \mathsf{ans}_1) = 1.$$

Proposition 4.6. *If $\mathcal{Z}$ have completeness c, $\mathsf{PRPV}_{\mathcal{Z}}$ has position-robust completeness c with possible prover locations $[1, 2)$.*

Proof. For any prover location $p_P \in [1, 2)$, his first broadcast y would be received by V_0 at time $2p_P < 4$, and by V_1 at time exactly 3; his second broadcast ans would be received by V_0 at time exactly 4, and by V_1 at time $1 + 2(3 - p_P) = 7 - 2p_P \leq 5$. Therefore, the verifiers should then accept with probability c by completeness of $\mathcal{Z}$. □

Before considering soundness, we first justify that any arbitrary strategy could be compiled into a strategy where there are only two adversaries A_0, A_1 being at locations 0 and 3 respectively.

Claim 4.7. *Let $S \in \mathcal{R}_P$ be any polynomially bounded adversarial strategy for* PRPV. *There exists another strategy $S' \in \mathcal{R}_P$, where for all λ, S'_λ consists of only two adversaries at location 0 and 3 respectively, and S' has the same verifier acceptance probability as S. Furthermore, the amount of entanglement shared between two adversaries in S' is the same as the entanglement shared between adversaries in $(-\infty, 1)$ and those in $(2, +\infty)$ in S.*

Proof. Without loss of generality, we assume that there is no adversaries in $(-\infty, 0) \cup (3, +\infty)$, since this is beyond where the verifiers sit and those adversaries can always be simulated by an adversary sitting at location 0 and 3. We look at all the adversaries in $[0, 1)$ (calling them "the lefties") and those in $(2, 3]$ (calling them "the righties"). We focus on when their private messages crosses the "event horizon" $[1, 2]$ (calling them CPC, short for "cross party communications"). Observe that any communication that is computed not in the two light cones[4] above $(0, 0)$ and $(3, 1)$ does not depend on either verifier's message, and therefore can be precomputed at time $t = -\infty$. Similarly, we can also discard any communication that happened outside of the two light cones below $(0, 4)$ and $(3, 3)$, since V_0 and V_1's decisions only depends on information that comes under those two light cones. Therefore, the only meaningful message from the lefties needs to reach location 1 at time 1, and the only meaningful message from the righties need to reach location 2 at time 2.

We can now see that a single adversary can be placed at location 0 that simulates all the lefties. In particular, he will at time 0, compute the actions for lefties on line $(0, 0) - (1, 1)$ in order, send the messages to the right, and simulate all the lefties' internal communications afterwards before

[4] A light cone above (x, t) includes all points in the space-time diagram (x', t') such that $t' \geq t$ and $||x - x'|| \leq t' - t$. Similarly, a light cone below (x, t) includes all points in the space-time diagram (x', t') such that $t' \leq t$ and $||x - x'|| \leq t - t'$.

$(3, 1) - (4, 0)$; at time 4, he receives the only meaningful message from the righties and compute the actions for lefties on line $(3, 1) - (4, 0)$ in order, and output the corresponding output. Using the same argument, a single simulated adversary at location 3 can also simulate the righties perfectly. Finally, since $S \in \mathcal{R}_P$, there are only polynomial number of adversaries from S, therefore the final adversaries we construct are also polynomial time. □

We now more formally characterize the behaviors of the two adversaries A_0, A_1 at position 0 and 3 respectively, as described above (also illustrated at Figure 1).

0. At $t = -\infty$, A_0 receives the security parameter λ, runs a set up U_0 to prepare state $\rho^{(0)}_{RS}$. It then sends $\rho^{(0)}_S$ to A_1.

   Thus, we can assume before the protocol begins, A_0 and A_1 possess $\rho^{(0)}_R, \rho^{(0)}_S$ respectively.

1. At $t = 0$, A_0 receives pk. It applies a quantum circuit U_1 on $|\mathsf{pk}\rangle\langle\mathsf{pk}|$ and $\rho^{(0)}_R$ to get a classical string y_0 along with the resulting overall state $\rho^{(1)}_{R'MS}$ and sends the classical y_0 to V_0 immediately at time $t = 0$ (he could delay the message, but since he does not obtain new information before he has to send y_0 (at time $t < 4$), this does not help him).

   For the residual registers R' and M, A_0 also sends $\rho^{(1)}_M$ to A_1 immediately at time $t = 0$, and stores $\rho^{(1)}_{R'}$.

2. At $t = 1$, A_1 receives b, applies U_2 on $|b\rangle\langle b|$ and $\rho^{(1)}_S$, and let the overall resulting state be $\rho^{(2)}_{R'MM'S'}$. He sends $\rho^{(2)}_{M'}$ to A_0 and stores $\rho^{(2)}_{S'}$.

3. At $t = 3$, A_1 receives register M, performs a POVM measurement U_3 on $\rho^{(2)}_{MS'}$ to obtain y_1, ans_1 to send to V_1.

4. At $t = 4$, A_0 receives register M', performs a POVM measurement U_4 on $\rho^{(2)}_{R'M'}$ to obtain ans_0 to send to V_0.

We now consider a special case of U_2, denoted by the challenge forwarding unitary F, where it on input $|b\rangle\langle b| \otimes \rho^{(1)}_S$, and outputs $|b\rangle\langle b|$ into register M' and $|b\rangle\langle b| \otimes \rho^{(1)}_S$ into register S'.

Definition 4.8. *We denote the set of adversarial strategies having $U_2 = F$ to be $\mathcal{R}_F \subseteq \mathcal{R}_P$.*

Note that for adversaries in $\mathcal{R}_F$ *can* pre-share entanglement. This is needed later in Corollary 6.4.

Theorem 4.9. *If $\mathcal{Z}$ have 1-of-2 non-local soundness τ, $\mathsf{PRPV}_{\mathcal{Z}}$ has soundness τ against $\mathcal{R}_F$.*

Proof. The idea is to reduce this adversary to the 1-of-2 non-local game defined in Definition 3.3. Note that since $U_2 = F$ is the challenge forwarding operator, we can assume the challenge b is given to both A_0, A_1 at time $t = 3, t = 4$ respectively, instead of being sent from V_1, which achieves the same acceptance probability.

Assume for contradiction that A_0, A_1 achieves success probability noticeably more than τ. We construct an adversary that breaks the 1-of-2 non-local soundness.

- The algorithm $\mathcal{A}$ upon receiving pk, it runs U_1U_0 on pk to obtain y_0 along with $\rho^{(1)}_{R'MS}$. It outputs $\rho^{(1)}_{R'}$ into register B and $\rho^{(1)}_{MS}$ into register C.

- Since M' register simply contains b, let $\mathcal{B}$ perform POVM U_4 as M' at time $t = 4$, and let $\mathcal{C}$ perform POVM U_3 .

Thus, $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ perfectly simulates (A_0, A_1) in PRPV, and thus achieves the same success probability in the non-local game as that by (A_0, A_1) in PRPV, which by assumption violates the 1-of-2 non-local soundness τ of the underlying puzzle $\mathcal{Z}$. □

We now show that this protocol is also sound with respect to a weaker restriction on the adversaries, in particular, the set of strategies where they do not pre-share entanglement.

Theorem 4.10. *If $\mathcal{Z}$ have* 1*-of-*2 *non-local soundness τ,* $\mathsf{PRPV}_{\mathcal{Z}}$ *has soundness τ against $\mathcal{R}_0$, i.e. the set of adversarial strategies where S is simply a classical string.*

Proof. The idea is to compile any such adversary into a challenge-forwarding adversary, and invoke the soundness argument of Theorem 4.9. The equivalent adversary could be constructed as follows. The key observation is that U_2's input only depends on b which can only be one of two values, and register S which only holds a classical string. Thus, A_0 can perform two executions of U_2 on $b = 0, 1$ respectively before it knows the actual b.

0. At $t = -\infty$, no set up is done.
1. At $t = 0$, A_0 runs $U_1 U_0$ on pk, in addition he also copies the classical string in register S, and runs U_2 (originally run by A_1) twice on two copies but for $b = 0, 1$ respectively. We denote the output as $\rho^{(2)}_{M'_0 S'_0} \otimes \rho^{(2)}_{M'_1 S'_1}$. He sends registers S'_0, S'_1, M as his message and keep registers R', M'_0, M'_1 to himself.
2. At $t = 1$, A_1 simply copies and forwards b, i.e. invokes F.
3. At $t = 3$, A_1 receives registers S'_0, S'_1, M and b, and runs the original POVM on registers M, S'_b.
4. At $t = 4$, A_0 receives the new second private message b, and runs the original POVM on registers R', M'_b.

It is easy to see that this compiler preserves the behavior of the adversaries perfectly, and therefore the soundness follows. □

5 Parallel Repetition

5.1 Strong 1-of-2 Puzzles

For the sake of the proof later, we identify two special properties from the underlying 1-of-2 puzzle.

Definition 5.1. *A* 1*-of-*2 *puzzle satisfies* 0-challenge-public-verifiability, *if* Ver *can be computed using only* pk *when $b = 0$, i.e. for* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$ *and any* y, ans, $\mathsf{Ver}(\mathsf{sk}, y, 0, \mathsf{ans})$ *can be efficiently computed correctly with probability 1 using only* $(\mathsf{pk}, y, \mathsf{ans})$.

We can easily verify this property by looking at the NTCF construction, as we show in Fact A.5.

The other property that we need later is that the 1-of-2 non-local soundness should be ½ instead of ¾. In order to achieve this, we recall the following theorem.

Theorem 5.2 ([RS19, Corollary 2.10])**.** *Assuming the quantum hardness of LWE, there exists a* $(1-\mathsf{negl}, 0)$*-1-of-2 puzzle* $\mathcal{Z}$*, furthermore, it satisfies 0-challenge-public-verifiability.*

In the prior work, they call this a *strong* 1-of-2 puzzle, and the proof is via constructing a flavor of parallel repetition of *any* base $(1-\mathsf{negl}, \frac{1}{2})$-1-of-2 puzzle.

Invoking Theorem 3.5, we get the following.

Lemma 5.3. *Assuming the quantum hardness of LWE, there exists a* 1*-of-*2 *puzzle with completeness* $1-\mathsf{negl}$*,* 1*-of-*2 *non-local soundness ½, and 0-challenge-public-verifiability.*

5.2 1-of-2^k Puzzles

Unfortunately, for any 1-of-2 puzzle $\mathcal{Z}$ with completeness c, there is always an adversarial strategy breaking $\mathsf{PRPV}_{\mathcal{Z}}$ (and therefore non-local soundness for $\mathcal{Z}$) with probability $c/2$ by simply guessing the challenge b, which would be correct with probability ½. Therefore, in order to beat this barrier, we consider the parallel repetition of 1-of-2 puzzles, and show that non-local soundness decreases exponentially, as a stepping stone to achieving negligibly-sound position verification.

Definition 5.4 (1-of-2^k Puzzles)**.** *A* 1*-of-*2^k *puzzle is exactly the same as a* 1*-of-*2 *puzzle, except that the challenge b is a uniformly random k-bit bitstring instead of a single random bit.*

Two main requirements of interest for 1-of-2^k puzzles are completeness and 1-of-2^k non-local soundness for 1-of-2^k puzzles, which can naturally be extended from completeness and 1-of-2 non-local soundness (see Definition 3.3, Definition 3.4) for 1-of-2 puzzles by simply changing b.

Construction 5.5 (Parallel Repetition of 1-of-2 Puzzles)**.** *Let* $\mathcal{Z} = (\mathsf{KeyGen}, \mathsf{Obligate}, \mathsf{Solve}, \mathsf{Ver})$ *be a* 1*-of-*2 *puzzle. The k-fold parallel repetition of* $\mathcal{Z}$*, denoted as* $\mathcal{Z}^k$*, is a* 1*-of-*2^k *puzzle constructed as follows:*

- $\mathsf{KeyGen}, \mathsf{Obligate}, \mathsf{Solve}$ *for* $\mathcal{Z}^k$ *simply runs* $\mathsf{KeyGen}, \mathsf{Obligate}, \mathsf{Solve}$ *for* $\mathcal{Z}$ k *times respectively.*
- Ver *for* $\mathcal{Z}^k$ *runs* Ver *on all* k *instances, and accepts if and only if all of them accept.*

We note that the parallel repetition we consider here is different from the one used in the proof of Theorem 5.2. In their case, the same challenge bit is reused across all k instances, whereas in our case, each instance has a fresh random bit. Thus, they obtain a 1-of-2 puzzle after the repetition, and here we get a 1-of-2^k puzzle.

Theorem 5.6. *Let* $\mathcal{Z}$ *be a* 1*-of-*2 *puzzle with completeness* $1-\mathsf{negl}$*,* 1*-of-*2 *non-local soundness ½, and 0-challenge-public-verifiability. Then for any* $k = \mathsf{poly}(\lambda)$*,* $\mathcal{Z}^k$ *has completeness* $1-\mathsf{negl}$ *and* 1*-of-*2^k *non-local soundness* 2^{-k}*.*

Recall that by definition, this theorem means that for any QPT adversary, there exists a negligible function negl, such that the success probability is at most $2^{-k} + \mathsf{negl}(\lambda)$.

The rest of the section will be dedicated to proving the theorem, mainly the non-local soundness. Our proof follows the ideas from the work by Alagic et al. [ACGH20, Section 4]. This work along with the one by Chia et al. [CCY20] proved that parallel repetition decreases soundness exponentially for Mahadev's quantum delegation, which is a different application of NTCFs.

We begin by showing that for $\mathcal{Z}$, the projection corresponding to challenge 0 and 1 are "computationally orthogonal".

Lemma 5.7. *Let* $\mathcal{Z}$ *be a* 1*-of-*2 *puzzle with* 1*-of-*2 *non-local soundness ½. For any efficient non-local player* $\mathcal{W} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$*, let* $|\psi_{\mathsf{pk}}\rangle_{BCY}$ *be the overall state*[5] *of* $\mathcal{A}$*'s output, where measuring* Y *register in the*

[5]Without loss of generality, we assume the state is purified where the auxiliary space is either in B or C register.

computational basis gives y. Let projection $\Pi_{\mathsf{sk},b}$ correspond to the quantum predicate $\mathsf{Ver}(\mathsf{sk}, y, b, \mathsf{ans}_{\mathcal{B}}) \wedge \mathsf{Ver}(\mathsf{sk}, y, b, \mathsf{ans}_{\mathcal{C}})$*. If*

$$\mathop{\mathbb{E}}_{\mathsf{KeyGen}}[\langle\psi_{\mathsf{pk}}|\Pi_{\mathsf{sk},0}|\psi_{\mathsf{pk}}\rangle] \geq 1 - \mathsf{negl}(\lambda),$$

then

$$\mathop{\mathbb{E}}_{\mathsf{KeyGen}}[\langle\psi_{\mathsf{pk}}|\Pi_{\mathsf{sk},1}|\psi_{\mathsf{pk}}\rangle] = \mathsf{negl}(\lambda).$$

Proof. Note that by definition, $\Pi_{\mathsf{sk},b}$ only involves running $\mathcal{B}, \mathcal{C}$ and Ver. Since $\mathcal{B}, \mathcal{C}$ does not act on the Y register, and Ver is only classically controlled on Y, $\Pi_{\mathsf{sk},b}$ commutes with the computational-basis measurement on Y for any sk, b. Therefore, the overall winning probability for $\mathcal{W}$ is exactly $\frac{1}{2}\mathbb{E}_{\mathsf{KeyGen}}[\langle\psi_{\mathsf{pk}}|(\Pi_{\mathsf{sk},0} + \Pi_{\mathsf{sk},1})|\psi_{\mathsf{pk}}\rangle]$. Suppose the lemma does not hold, then the expression above would be noticeably higher than ½. A contradiction. □

We now show that a similar version also holds for $\mathcal{Z}^k$. The notation $\Pi_{\mathsf{sk},b}$ for 1-of-2 puzzles above can be extended similarly for 1-of-2^k puzzles.

Lemma 5.8. *Let $\mathcal{Z}$ be a 1-of-2 puzzle with completeness $1 - \mathsf{negl}$, 1-of-2 non-local soundness ½, and 0-challenge-public-verifiability. For any $k = \mathsf{poly}(\lambda)$, any non-local player $\mathcal{W}$ for $\mathcal{Z}^k$, and any $a \neq b \in \{0,1\}^k$,*

$$\mathop{\mathbb{E}}_{\mathsf{KeyGen}}[\langle\psi_{\mathsf{pk}}|(\Pi_{\mathsf{sk},b}\Pi_{\mathsf{sk},a} + \Pi_{\mathsf{sk},a}\Pi_{\mathsf{sk},b})|\psi_{\mathsf{pk}}\rangle] = \mathsf{negl}(\lambda).$$

Proof. Since a, b is symmetric, without loss of generality, assume that there exists i so that $a_i = 1$ and $b_i = 0$. We claim that

$$\mathop{\mathbb{E}}_{\mathsf{KeyGen}}[\langle\psi_{\mathsf{pk}}|\Pi_{\mathsf{sk},b}\Pi_{\mathsf{sk},a}\Pi_{\mathsf{sk},b}|\psi_{\mathsf{pk}}\rangle] = \mathsf{negl}(\lambda). \tag{2}$$

Assume for contradiction that there is a player strategy that makes this term noticeable, say $1/\eta(\lambda)$ for some polynomial η. Define $\Sigma_{\mathsf{sk},a}$ projector to be same as $\Pi_{\mathsf{sk},a}$ except that it only checks the i-th repetition and acts as identity on every other repetition. By definition $\Pi_{\mathsf{sk},a} \preccurlyeq \Sigma_{\mathsf{sk},a}$, and thus $\mathbb{E}_{\mathsf{KeyGen}}[\langle\psi_{\mathsf{pk}}|\Pi_{\mathsf{sk},b}\Sigma_{\mathsf{sk},a}\Pi_{\mathsf{sk},b}|\psi_{\mathsf{pk}}\rangle] \geq 1/\eta$. Consider the single-copy non-local player $\mathcal{W}^* = (\mathcal{A}^*, \mathcal{B}^*, \mathcal{C}^*)$ as follows:

- For $\mathcal{A}^*$, on input pk^*, it runs KeyGen $(k-1)$ times, and set pk to be a list of k public keys with pk^* inserted at the i-th position.
- Repeat the following for at most $q := \max\{4\eta^2, \lambda^2\}$ times: prepare $|\psi_{\mathsf{pk}}\rangle_{BCY}$, apply measurement $\Pi_{\mathsf{sk},b}$, and abort the loop if the measurement accepts. This is efficient as we know all the secret keys except for index i, which we can still verify by 0-challenge-public-verifiability as $b_i = 0$.

  If the loop has not succeeded after q iterations, $\mathcal{A}$ simply invokes the honest prover, guesses the challenge is 0, and sends the ans corresponding to 0-challenge to $\mathcal{B}$ and $\mathcal{C}$, so that later they simply output ans.
- Measure Y register of the residual state as y, and send B, C registers as input registers for the next round. Let the overall residual state be denoted as $|\phi\rangle$.
- For $\mathcal{B}^*, \mathcal{C}^*$, if the challenge is 0 (or 1), run $\mathcal{B}, \mathcal{C}$ on b (or a respectively), and output index i.

By construction, the probability that $\mathcal{W}$ succeeds when challenge is 0 is $1 - \mathsf{negl}$.

Now consider the case for challenge 1. Let

$$\Omega := \left\{(\mathsf{pk}, \mathsf{sk}) : \langle \psi_{\mathsf{pk}} | \Pi_{\mathsf{sk},b} | \psi_{\mathsf{pk}} \rangle > q^{-1/2}\right\}$$

denote the set of "good" keys for the parallel scheme. For $(\mathsf{pk}, \mathsf{sk}) \in \Omega$, the probability of not terminating within q iterations is at most $(1 - q^{-1/2})^q \le e^{-\sqrt{q}} \le e^{-\lambda}$ and thus $|\phi\rangle$ is exponentially close to $\Pi_{\mathsf{sk},b} |\psi_{\mathsf{pk}}\rangle$. By Lemma 5.7, we have

$$\mathop{\mathbb{E}}_{\mathsf{KeyGen} \wedge \Omega} [\langle \phi | \Sigma_{\mathsf{sk},a} | \phi \rangle] \le \mathop{\mathbb{E}}_{\mathsf{KeyGen}} [\langle \phi | \Sigma_{\mathsf{sk},a} | \phi \rangle] = \mathsf{negl}(\lambda),$$

where $\mathbb{E}_{\mathsf{KeyGen} \wedge \Omega}[f(\mathsf{pk}, \mathsf{sk})] = \mathbb{E}_{\mathsf{KeyGen}}[f(\mathsf{pk}, \mathsf{sk}) \cdot \mathbf{1}_{(\mathsf{pk},\mathsf{sk}) \in \Omega}])$. However,

$$\begin{aligned}
\eta^{-1} &\le \mathop{\mathbb{E}}_{\mathsf{KeyGen}} [\langle \psi_{\mathsf{pk}} | \Pi_{\mathsf{sk},b} \Sigma_{\mathsf{sk},a} \Pi_{\mathsf{sk},b} | \psi_{\mathsf{pk}} \rangle] \\
&= \mathop{\mathbb{E}}_{\mathsf{KeyGen} \wedge \Omega} [\langle \psi_{\mathsf{pk}} | \Pi_{\mathsf{sk},b} \Sigma_{\mathsf{sk},a} \Pi_{\mathsf{sk},b} | \psi_{\mathsf{pk}} \rangle] + \mathop{\mathbb{E}}_{\mathsf{KeyGen} \wedge \neg\Omega} [\langle \psi_{\mathsf{pk}} | \Pi_{\mathsf{sk},b} \Sigma_{\mathsf{sk},a} \Pi_{\mathsf{sk},b} | \psi_{\mathsf{pk}} \rangle] \\
&\le \mathsf{negl}(\lambda) + q^{-1/2} \\
&\le \mathsf{negl}(\lambda) + \eta^{-1}/2,
\end{aligned}$$

which contradicts with that η^{-1} is noticeable. Therefore, (2) must hold. It then follows that

$$\begin{aligned}
\mathop{\mathbb{E}}_{\mathsf{KeyGen}} [\langle \psi_{\mathsf{pk}} | (\Pi_{\mathsf{sk},b} \Pi_{\mathsf{sk},a} + \Pi_{\mathsf{sk},a} \Pi_{\mathsf{sk},b}) | \psi_{\mathsf{pk}} \rangle] &= 2 \mathop{\mathbb{E}}_{\mathsf{KeyGen}} [\Re \left(\langle \psi_{\mathsf{pk}} | \Pi_{\mathsf{sk},b} \Pi_{\mathsf{sk},a} | \psi_{\mathsf{pk}} \rangle \right)] \\
&\le 2 \mathop{\mathbb{E}}_{\mathsf{KeyGen}} [| \langle \psi_{\mathsf{pk}} | \Pi_{\mathsf{sk},b} \Pi_{\mathsf{sk},a} | \psi_{\mathsf{pk}} \rangle |] \\
&\le 2 \mathop{\mathbb{E}}_{\mathsf{KeyGen}} \left[\langle \psi_{\mathsf{pk}} | \Pi_{\mathsf{sk},b} \Pi_{\mathsf{sk},a} \Pi_{\mathsf{sk},b} | \psi_{\mathsf{pk}} \rangle^{1/2} \right] \\
&\le 2 \mathop{\mathbb{E}}_{\mathsf{KeyGen}} [\langle \psi_{\mathsf{pk}} | \Pi_{\mathsf{sk},b} \Pi_{\mathsf{sk},a} \Pi_{\mathsf{sk},b} | \psi_{\mathsf{pk}} \rangle]^{1/2} \\
&\le \mathsf{negl}(\lambda)
\end{aligned}$$

as claimed. □

We now recall a key technical lemma from the prior work before proving the main theorem.

Lemma 5.9 ([ACGH20, Lemma 4.3]). *Let $A_1, ..., A_m$ be projectors and $|\psi\rangle$ be a quantum state. Suppose there are real numbers $\delta_{ij} \in [0, 2]$ such that $\langle \psi | (A_i A_j + A_j A_i) | \psi \rangle \le \delta_{ij}$ for all $i \ne j$. Then $\langle \psi | (A_1 + \cdots + A_m) | \psi \rangle \le 1 + \left(\sum_{i<j} \delta_{ij} \right)^{1/2}$.*

Proof of Theorem 5.6. Completeness follows immediately by running the honest 1-of-2 solver in parallel and a union bound on the failure probability.

For soundness, consider any 1-of-2^k non-local player $\mathcal{W}$, and let its success probability be

$$\tau = 2^{-k} \mathop{\mathbb{E}}_{\mathsf{KeyGen}} \left[\langle \psi_{\mathsf{pk}} | (\sum_c \Pi_{\mathsf{sk},c}) | \psi_{\mathsf{pk}} \rangle \right].$$

Define an arbitrary total order "$<$" on $\{0,1\}^k$. Then by Lemma 5.9 and Lemma 5.8, we have

$$\begin{aligned}\tau &\leq 2^{-k} + 2^{-k} \mathop{\mathbb{E}}_{\mathsf{KeyGen}}\left[\langle\psi_{\mathsf{pk}}|\sum_{a<b}(\Pi_{\mathsf{sk},a}\Pi_{\mathsf{sk},b}+\Pi_{\mathsf{sk},b}\Pi_{\mathsf{sk},a})|\psi_{\mathsf{pk}}\rangle\right]^{1/2}\\ &\leq 2^{-k} + 2^{-k}\sqrt{2^{2k}\cdot\mathsf{negl}(\lambda)}\\ &= 2^{-k} + \mathsf{negl}(\lambda),\end{aligned}$$

concluding the proof. □

5.3 0-Entanglement Soundness from Polynomial Hardness

We now consider the k-fold pararell repetition of PRPV.

Construction 5.10. *Let $\mathcal{Z}$ be a 1-of-2 puzzle. $\mathsf{PRPV}_{\mathcal{Z}}^k$ is the position verification protocol where the two verifiers and the prover runs k instances of $\mathsf{PRPV}_{\mathcal{Z}}$ in parallel. At the end, the verifiers accept if and only if all k instances accept.*

One can also naturally define $\mathsf{PRPV}_{\mathcal{Z}'}$ for any 1-of-2^k puzzle $\mathcal{Z}'$ by simply changing b to be a k-bit bitstring. By construction, $\mathsf{PRPV}_{\mathcal{Z}^k}$ results in the exact same protocol as $\mathsf{PRPV}_{\mathcal{Z}}^k$ for any 1-of-2 puzzle $\mathcal{Z}$.

Theorem 5.11. *Let $\mathcal{Z}$ be a 1-of-2 puzzle with completeness $1-\mathsf{negl}$ and 1-of-2 non-local soundness $1/2$. Then for any $k=\mathsf{poly}(\lambda)$, $\mathsf{PRPV}_{\mathcal{Z}}^k$ has position-robust completeness $1-\mathsf{negl}$ with possible prover locations $[1,2)$, and soundness 2^{-k} against both $\mathcal{R}_F$ and $\mathcal{R}_0$.*

Proof. Completeness follows directly by invoking the honest prover in parallel. Since the protocol has the exact same timing constraints as before, the adversarial behavior can be described exactly the same as Claim 4.7. Therefore, soundness against $\mathcal{R}_F$ can be proven exactly the same as Theorem 4.9 as the proof does not rely on b being a single bit, except that we instead reduce to 1-of-2^k non-local soundness of $\mathcal{Z}^k$, which we prove in Theorem 5.6.

As for soundness against $\mathcal{R}_0$, we also employ the same idea, which is to compile any such adversary into a challenge forwarding adversary, and invoke the soundness against $\mathcal{R}_F$. Note that the proof of Theorem 4.10 requires running U_2 on all possible challenges b, and in this case, the challenge space is as large as 2^k. The compiler from Theorem 4.10 trying all possible coins will give a forwarding adversarial strategy with run-time/communication blow up in 2^k. Therefore, the proof immediately extends if $k=O(\log\lambda)$.

Assume $k=\omega(\log\lambda)$, then we need to prove that any efficient adversary strategy can only succeed with probability at most $2^{-k}+\mathsf{negl}(\lambda)$, which is overall a negligible function. Assume if an $\mathcal{R}_0$ adversary is able to break the protocol with probability $1/p$ for some polynomial $p(\lambda)$, then we can come up with an adversary that breaks $\mathsf{PRPV}_{\mathcal{Z}}^m$ with the same probability $1/p$ for any $m\leq k$, by simply simulating the other $(m-k)$ executions and running the original adversary. Pick $m=\log p+1=O(\log\lambda)$, and we get an $\mathcal{R}_F$ adversary for $\mathsf{PRPV}_{\mathcal{Z}}^m$ with success probability $1/p$. However, as we argued, $\mathsf{PRPV}_{\mathcal{Z}}^m$ has soundness $2^{-m}=2^{1-\log p}=1/2p$ against $\mathcal{R}_F$. This leads to a contradiction as $1/2p$ is noticeable. □

Combining this with Lemma 5.3, we get the following.

Corollary 5.12. *Assuming polynomial quantum hardness of LWE, there is a classically-verifiable position verification scheme having position-robust completeness* $1 - \mathsf{negl}$ *with possible prover locations* $[1, 2)$ *and negligible soundness against* $\mathcal{R}_F$ *and* $\mathcal{R}_0$.

5.4 Bounded-Entanglement Soundness from Subexponential Hardness

The soundness could be decreased further if we assume stronger hardness on quantum LWE. For $c > 0$ and $L : \mathbb{N}^+ \to \mathbb{N}$, let $\mathcal{R}_{L,c}$ be the same as $\mathcal{R}_L$, except that the adversaries can run in time $\mathsf{poly}\left(2^{\lambda^c}\right)$ instead of $\mathsf{poly}(\lambda)$. We denote c-subexponential hardness [JKKZ21, HLR21] to mean that any $\mathsf{poly}\left(2^{\lambda^c}\right)$-time adversary achieving advantage at most $\mathsf{negl}\left(2^{\lambda^c}\right)$.

Lemma 5.13. *Assuming c-subexponential quantum hardness of LWE, there is a classically-verifiable position verification scheme having position-robust completeness* $1 - \mathsf{negl}$ *with possible prover locations* $[1, 2)$ *and c-subexponential soundness against* $\mathcal{R}_{0,c}$.

Proof. Most of the reduction extends immediately as they are all black-box reductions, in particular, they do not explicitly depend on the adversary's running time nor its success probability. There are three exceptions: Theorem 5.2, Theorem 5.6 and Theorem 5.11.

We show how to adapt the proof for Theorem 5.6 for the subexponential case, and the same approach could be applied to Theorem 5.2 as well, which corresponds to the parallel repetition of the base 1-of-2 puzzles. The non-black-box reduction in the proof for Theorem 5.6 occured in Lemma 5.8, where the reduction needs to repeat running the adversary q times, where $q = \max\{\lambda^2, (2/p)^2\}$ and p is the adversary's success probability in (2). By assumption, there exists some constant $c > 0$, such that for any $\mathsf{poly}\left(2^{\lambda^c}\right)$-time adversary, he can win the 1-of-2 non-local game with probability at most $1/2 + \mathsf{negl}\left(2^{\lambda^c}\right)$. Let the adversary's running time be $T = \mathsf{poly}\left(2^{\lambda^c}\right)$ and assume that $p = 1/\mathsf{poly}\left(2^{\lambda^c}\right)$, then we can see that the reduction still runs in time $O(Tq) = O(T/p^2) = \mathsf{poly}\left(2^{\lambda^c}\right)$. The rest of the proof goes through and at the end, we conclude that $p = \mathsf{negl}\left(2^{\lambda^c}\right)$, a contradiction.

The non-black-box step in the proof for Theorem 5.11 occurred in the step where the reduction reduces a general adversary into a challenge forwarding adversary. Recall that k is the number of repetitions. Again, if $k = O(\lambda^c)$, the reduction runs in time $2^k \cdot \mathsf{poly}\left(2^{\lambda^c}\right) = \mathsf{poly}\left(2^{\lambda^c}\right)$ and the proof goes through. Assume $k = \omega(\lambda^c)$ and the adversary's success probability p is noticeably larger than 2^{-k} which is again negligible in 2^{λ^c}, then the reduction runs in time $O(\log 1/p) \cdot \mathsf{poly}\left(2^{\lambda^c}\right) = \mathsf{poly}\left(2^{\lambda^c}\right)$ and the proof also goes through.

Finally, we remark that the "statistical security parameter" in the instantiation of NTCFs, which is the ratio $\frac{B_P}{B_V} = \frac{B_V}{B_L}$, needs to be set to be at least $2^{\lambda^{c'}}$ for any $c' > c$ in order for the NTCF construction to be c-subexponentially secure. We refer the readers to [BCM+21, Remark 4.2] for the relevant discussions on the choice of the parameters for the NTCF. □

We now leverage standard techniques [Aar05a, TFKW13] to show that this can be bootstrapped to handle bounded entanglement adversaries.

Theorem 5.14. *Assuming c-subexponential quantum hardness of LWE, for any polynomial* $L : \mathbb{N}^+ \to \mathbb{N}$, *there is a classically-verifiable position verification scheme having position-robust completeness* $1 - \mathsf{negl}$ *with possible prover locations* $[1, 2)$ *and c-subexponential soundness against* $\mathcal{R}_{L,c}$.

Proof. By assumption, there exists an 1-of-2 puzzle $\mathcal{Z}$ such that for any polynomial $k(n) = \omega(n^c)$, for any adversarial strategy $S \in \mathcal{R}_{0,c}$, S succeeds in breaking $\mathsf{PRPV}^k_{\mathcal{Z}}$ with probability at most

$\mathsf{negl}\left(2^{n^c}\right) = 2^{-\omega(n^c)}$. In particular, S has success probability at most 2^{-n^c} for all sufficiently large n against $\mathcal{R}_{0,c}$.

Pick $n = (L(\lambda) + \lambda^c)^{1/c}$, and we claim that for every adversarial strategy $S \in \mathcal{R}_{L,c}$, its success probability in breaking $\mathsf{PRPV}^k_{\mathcal{Z}}(n)$ is $\mathsf{negl}\left(2^{-\lambda^c}\right)$, in particular, it is at most $2^{-\lambda^c}$ for all sufficiently large λ. Assume this is not the case, then its success probability is higher than $2^{-\lambda^c}$ infinitely often. We can replace the entanglement with maximally mixed state, and therefore we have an adversarial strategy $S' \in \mathcal{R}_{0,c}$ with success probability higher than $2^{-\lambda^c} \cdot 2^{-L} = 2^{-L-\lambda^c} = 2^{-n^c}$ infinitely often. This is because any pre-shared entanglement of dimension 2^L can be extended into a basis for a 2^L-dimension state space, which means that the entanglement can be replaced by a maximally mixed state (a non-entangled state), and reduces the probability by at most a factor 2^L. This contradicts with the conclusion in the last paragraph. □

6 Attacks and Countermeasures

6.1 Attack with Polynomial Entanglement

In this section, we present an adversarial strategy in $\mathcal{R}_L$ for $\mathsf{PRPV}^k_{\mathcal{Z}}$ achieving winning probability as good as the completeness of the protocol for any $k = \mathsf{poly}(\lambda)$ and any 1-of-2 puzzle $\mathcal{Z}$ satisfying a specific property defined below, with L being only as large as the number of qubits in ρ. Note that this does not contradict the bounded-entanglement soundness from Theorem 5.14, as there L is determined by the security parameter λ, and therefore cannot depend on the specific protocol construction (and therefore the length of ρ).

Definition 6.1. *We call a* 1*-of-*2 *puzzle having an* XZ-solver *if* $\mathsf{Solve}(\mathsf{pk}, y, \rho, b)$ *simply measures* ρ *(as a string of qubits) in standard basis if* $b = 0$*, or Hadamard basis if* $b = 1$*, and outputs the measurement result.*

Note that the 1-of-2 puzzle based on NTCFs both have an XZ-solver (see Fact A.4). This holds also for the strong 1-of-2 puzzle, as by construction, it is simply running an XZ-solver several times in parallel. We now describe the attack for $\mathsf{PRPV}_{\mathcal{Z}}$ when $\mathcal{Z}$ has an XZ-solver.

1. At $t = -\infty$, A_0 prepares L EPR pairs, and keeps the first half in register R and sends the other half to A_1 in register S.

2. At $t = 0$, A_0 receives pk and prepares (y, ρ) by running $\mathsf{Obligate}$ as normal. In addition, he also teleports ρ using R, getting measurement results (k_0, k_1). He sends y to V_0, and (y, k_0, k_1) to A_1.

3. At $t = 1$, A_1 receives b, and measures S in standard basis if $b = 0$, or else in Hadamard basis if $b = 1$. He obtains measurement results r and sends (b, r) to A_0.

4. At $t = 3$, A_1 receives (y, k_0, k_1), and sends $(y, r \oplus k_b)$ to V_1.

5. At $t = 4$, A_0 receives (b, r), and sends $r \oplus k_b$ to V_0.

The correctness of the attack follows from the fact that the teleportation gadget commutes with the X/Z measurements the prover performs at the end of the computation.

In order to attack $\mathsf{PRPV}^k_{\mathcal{Z}}$, we can simply repeat this attack k times in parallel.

6.2 Unbounded-Entanglement Soundness in the QROM

In this section, we employ the idea from Unruh's work [Unr14] for constructing position verification with quantum communication against unbounded entanglement in the quantum random oracle model (QROM). Following the idea there, we change the construction $\mathsf{PRPV}_{\mathcal{Z}}^k$ so that the random k-bit challenge b is sampled by the random oracle, i.e. $b = H(x_0 \oplus x_1)$ for random x_0, x_1. We prove that the resulting construction achieve negligible soundness against efficient adversaries with *any* polynomial amount of entanglement in the QROM.

The following construction ROPRPV is a variant of PRPV in the QROM. We highlight the differences in this construction with underlines.

Construction 6.2 (ROPRPV Protocol)**.** *Let $\mathcal{Z}$ be an 1-of-2^k puzzle and let $H : \{0,1\}^\lambda \to \{0,1\}^k$ be a random oracle, where λ is the security parameter. The protocol $\mathsf{ROPRPV}_{\mathcal{Z}}$ is defined as follows:*

1. *Starting at $t = 0$, V_0 samples a pair of keys $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$ $\underline{\text{and } x_0 \leftarrow \{0,1\}^\lambda}$, broadcasts pk $\underline{\text{and } x_0}$, and waits to receive y_0 from the prover before time $t < 4$, and ans_0 at time $t = 4$.*
2. *At $t = 1$, V_1 samples $\underline{x_1 \leftarrow \{0,1\}^\lambda}$ and broadcasts it, and waits to receive y_1 from the prover at time $t = 3$, and ans_1 at time $t \leq 5$.*
3. *At $t = p_P$, the prover, located at $p_P \in [1, 2)$, receives pk $\underline{\text{and } x_0}$, it prepares $(y, \rho) \leftarrow \mathsf{Obligate}(\mathsf{pk})$ and broadcasts y.*
4. *At $t = 4 - p_P$, the prover receives $\underline{x_1}$, $\underline{\text{let } b = H(x_0 \oplus x_1)}$; it computes $\mathsf{ans} \leftarrow \mathsf{Solve}(\mathsf{pk}, y, \rho, b)$ and broadcasts ans.*
5. *At $t \leq 5$ when the verifiers receive all the messages in time described above, they check that $y_0 = y_1$ and $\mathsf{ans}_0 = \mathsf{ans}_1$, and the answers pass the test:*
$$\mathsf{Ver}(\mathsf{sk}, y_0, b, \mathsf{ans}_0) = 1 \wedge \mathsf{Ver}(\mathsf{sk}, y_1, b, \mathsf{ans}_1) = 1, \quad \underline{\text{where } b = H(x_0 \oplus x_1)}.$$

Theorem 6.3. *For any $k > 0$ and any 1-of-2 puzzle $\mathcal{Z}$, if $\mathsf{PRPV}_{\mathcal{Z}}^k$ has completeness c and soundness s against $\mathcal{R}_F$, $\mathsf{ROPRPV}_{\mathcal{Z}^k}$ has completeness c and soundness s against $\mathcal{R}_P$, i.e. the set of polynomially bounded strategies (and therefore having at most polynomial amount of pre-shared entanglement) in the QROM.*

Proof. The completeness of the protocol extends since the only change is how b is sampled.

Since the timing constraints remain the same, similar to Claim 4.7, any arbitrary strategy can be compiled into a strategy where there are only two adversaries A_0, A_1 being at locations 0 and 3 respectively. In particular, besides the set up U_0, A_0's behavior can be characterized as an action U_1 at time 0 when it receives pk, x_0 from V_0 and a POVM measurement U_4 at $t = 4$; similarly, A_1's behavior can be characterized as an action U_2 at time 1 when it receives pk, x_1 from V_1 and a POVM measurement U_3 at $t = 3$.

The proof is through a sequence of hybrid arguments. We give the hybrids below, and show the success probability in each hybrid is negligibly close to the previous one.

Hybrid 0 Execute the original protocol with V_0, V_1, A_0, A_1 and a random oracle H.

Hybrid 1 It is the same as Hybrid 0 except that at time $t = 2$, a random challenge $b \leftarrow \{0,1\}$ is chosen randomly. Then the random oracle H is immediately reprogrammed such that $H(x_0 \oplus x_1) = b$.

The indistinguishability comes from a variant of the one-way to hiding (O2H) lemma [Unr14, Lemma 3]. Let A_0, A_1 be $T(\lambda)$-time bounded (with possible shared-entanglement), where $T = \mathsf{poly}(\lambda)$ since the adversaries are efficient. With this O2H lemma, we can argue that Hybrid 1 and Hybrid 0 are $O(T(\lambda) \cdot 2^{-\lambda/2}) = \mathsf{negl}(\lambda)$ close.

Hybrid 2 We can without loss of generality assume A_0, A_1 get access to two but identical random oracles instead of one random oracle. The hybrid is the same as Hybrid 1 except that the random oracle H accessed by A_1 is reprogrammed immediately before time $t = 3$, and the same random oracle H accessed by A_0 is reprogrammed immediately before time $t = 4$.

After time $t > 2$, A_0 only does computation at time $t = 4$ and A_1 only does computation at time $t = 3$. Thus, the output distributions of Hybrid 1 and Hybrid 2 are identical.

Assume that the adversaries' success probability in breaking $\mathsf{ROPRPV}_{\mathcal{Z}^k}$ is $p = p(\lambda)$, then by the hybrid argument, they will also succeed in breaking Hybrid 2 with probability at least $p - \mathsf{negl}(\lambda)$. We now consider compiling any adversary strategy in Hybrid 2 can be converted into a (challenge-forwarding) adversary strategy in $\mathcal{R}_F$ for $\mathsf{PRPV}^k_{\mathcal{Z}}$ with the same success probability.

- Recall that B_0 is at 0 and B_1 is at 3. B_0 samples random x_1 and executes $U_2 U_0$ and obtain outputs in registers R, M', S'. B_0 also samples a random x (and let $x_0 := x \oplus x_1$), and a random oracle H. Note that although the description of H is inefficient, H can be perfectly simulated with a $2T$-wise independent function [Zha12, Theorem 3.1], whose description is efficient.

  B_0 possesses registers R, M' and classical information H, x and sends to B_1 register S' and classical information H, x.

- At time $t = 0$, when B_0 gets pk from V_0, it runs U_1 on input pk, x_0 and register R with oracle access to H, and sends the resulting y to V_0 and M register to B_1.

- At time $t = 1$, B_1 simply runs F, i.e. forwards b to B_0.

- At time $t = 3$, B_1 receives M and perform the POVM on M, S' with oracle access to $H_{x,b}$, where $H_{x,b}$ denotes the reprogrammed function H that on input x outputs b, and runs H on input anything else.

- At time $t = 4$, B_0 receives b and perform the POVM on R', M' with oracle access to the reprogrammed $H_{x,b}$.

We can see that this perfectly simulates the output distribution of Hybrid 2, and thus $p - \mathsf{negl}(\lambda) \leq s + \mathsf{negl}(\lambda)$ as desired. □

Combining this with Corollary 5.12, we get the following.

Corollary 6.4. *Assuming polynomial quantum hardness of LWE, there is a classically-verifiable position verification scheme having position-robust completeness* $1 - \mathsf{negl}$ *with possible prover locations* $[1, 2)$ *and negligible soundness against* $\mathcal{R}_P$ *in the QROM.*

7 Necessity of Proofs of Quantumness

In this section, we argue that the proof of quantumness is necessary to construct classically-verifiable position verification protocol even in one dimension. We first recall the definition of proofs of quantumness. The motivation is to test whether an untrusted efficient[6] device truly has quantum capabilities.

Definition 7.1. *A proof of quantumness is an interactive protocol with an efficient classical verifier satisfying:*

- ***Completeness*** c*: There exists a polynomial-time quantum prover that can convince the verifier with probability at least* c*;*
- ***Soundness*** s*: Any polynomial-time classical prover convinces the verifier with probability at most* $s + \mathsf{negl}$ *for some negligible function* negl.

Theorem 7.2. *Assuming the existence of any 1D position verification protocol satifying:*

1. *Without loss of generality, there are two verifiers* V_0, V_1 *at location 0 and 1 respectively;*
2. *It has completeness* c *for an efficient prover at location* $p_P \in (0, 1)$*;*
3. *It has soundness* s *against two efficient classical adversaries, one located in* $[0, p_P)$ *and the other located in* $(p_P, 1]$*;*
4. *Verifiers are classical and efficient.*

There exists a proof of quantumness protocol with completeness c *and soundness* s*.*

Proof. The construction for the proof of quantumness is very simple: it simply runs both V_0, V_1, sending and receiving the messages in the order enforced by the timing constraints for the prover in the position verification protocol. We emphasize that the resulting proof of quantumness protocol is a standard interactive protocol without timing constraints, since we are only using the timing constraints from position verification protocol to define the order of the messages. Therefore, completeness follows immediately; the verifier is efficient and classical as the position verification protocol is efficient and classically verifiable.

For soundness, the idea is essentially extending the impossibility of classical position verification [CGMO14]. Assume there is a classical prover that wins this protocol with probability w. We construct an adversarial strategy with two classical adversaries, A_0 at location $p_0 \in L \cap [0, p_P)$, and A_1 at location $p_1 \in L \cap (p_P, 1]$. They sample and pre-share their random tape used to run the classical prover. In the security game, they receive the broadcast message from the verifiers, and A_b will send the message computed to V_b for $b = 0, 1$.

To see that this adversary simulates the classical prover perfectly, it suffices to show that the adversaries can obtain all the information they need *in time* to simulate the prover's responses. Consider any message computed by the prover at location p_P at time $t = \tau$. It can only depend on messages sent from V_0 before $t \leq \tau - p_P$, and from V_1 before $t \leq \tau - (1 - p_P)$; this response will be received by V_0 at $t = \tau + p_P$ and by V_1 at $t = \tau + (1 - p_P)$. Therefore A_0 needs to simulate

[6]Indeed, an unbounded classical device can always simulate the quantum strategy, and no tests can tell the difference.

the response before $t = \tau + p_P - p_0$. Since $\tau + p_P - p_0 > \tau$, he has all the information from V_0. Since the last message from V_1 (for honest computation happens at time $t = \tau$) will reach A_0 at $t = \tau + p_P - p_0$, he also has all the information from V_1. By symmetry, A_1 also has enough time to gather all the information. Finally, because they pre-share the identical randomness tape, their response will be consistent as a single classical prover. Therefore, this adversarial strategy has success probability w, and the only setup they need is some pre-shared classical randomness. By soundness of the protocol, $w \leq s + \mathsf{negl}(\lambda)$. $\square$

We remark that these requirements except classical verifiability are rather minimal, and all known position verification protocols, including ours, satisfy these properties. Furthermore, the position verification protocol could be arbitrarily many rounds.

References

[Aar05a] Scott Aaronson. "Limitations of Quantum Advice and One-Way Communication". In: *Theory Comput.* 1.1 (2005), pp. 1–28. DOI: `10.4086/toc.2005.v001a001` (cit. on pp. 8, 23).

[Aar05b] Scott Aaronson. "Quantum Computing, Postselection, and Probabilistic Polynomial-Time". In: *Proceedings: Mathematical, Physical and Engineering Sciences* 461.2063 (2005), pp. 3473–3482. ISSN: 13645021. URL: `http://www.jstor.org/stable/30047928` (cit. on p. 3).

[ABSL21] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. *New Protocols and Ideas for Practical Quantum Position Verification*. 2021. arXiv: `2106.12911v1 [quant-ph]` (cit. on p. 1).

[ACGH20] Gorjan Alagic, Andrew M. Childs, Alex B. Grilo, and Shih-Han Hung. "Non-interactive Classical Verification of Quantum Computation". In: *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*. Ed. by Rafael Pass and Krzysztof Pietrzak. Vol. 12552. Lecture Notes in Computer Science. Springer, 2020, pp. 153–180. DOI: `10.1007/978-3-030-64381-2_6` (cit. on pp. 7, 19, 21).

[AGM21] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. *Can you sign a quantum state?* 2021. arXiv: `1811.11858v3 [quant-ph]` (cit. on p. 2).

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. "Position-Based Quantum Cryptography: Impossibility and Constructions". In: *SIAM J. Comput.* 43.1 (2014), pp. 150–178. DOI: `10.1137/130913687` (cit. on pp. 1, 3).

[BCG+02] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam D. Smith, and Alain Tapp. "Authentication of Quantum Messages". In: *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings*. IEEE Computer Society, 2002, pp. 449–458. DOI: `10.1109/SFCS.2002.1181969` (cit. on p. 2).

[BCM+18] Zvika Brakerski, Paul F. Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. "A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device". In: *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*. Ed. by Mikkel Thorup. IEEE Computer Society, 2018, pp. 320–331. DOI: `10.1109/FOCS.2018.00038` (cit. on pp. 2, 4, 31).

[BCM+21] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. *A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device*. 2021. arXiv: `1804.00640v4 [quant-ph]` (cit. on pp. 9, 23, 32).

[BCS21] Andreas Bluhm, Matthias Christandl, and Florian Speelman. *Position-based cryptography: Single-qubit protocol secure against multi-qubit attacks*. 2021. arXiv: `2104.06301v2 [quant-ph]` (cit. on pp. 1, 3).

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. "Random Oracles in a Quantum World". In: *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. Lecture Notes in Computer Science. Springer, 2011, pp. 41–69. DOI: `10.1007/978-3-642-25385-0_3` (cit. on pp. 3, 10).

[BDFP17] Joshua Brody, Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak. "Position-Based Cryptography and Multiparty Communication Complexity". In: *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I*. Ed. by Yael Kalai and Leonid Reyzin. Vol. 10677. Lecture Notes in Computer Science. Springer, 2017, pp. 56–81. DOI: `10.1007/978-3-319-70500-2_3` (cit. on p. 1).

[BFSS13] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. "The Garden-Hose Model". In: *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*. ITCS '13. Berkeley, California, USA: Association for Computing Machinery, 2013, pp. 145–158. ISBN: 9781450318594. DOI: `10.1145/2422436.2422455` (cit. on p. 1).

[BK11] Salman Beigi and Robert König. "Simplified instantaneous non-local quantum computation with applications to position-based cryptography". In: *New Journal of Physics* 13.9 (Sept. 2011), p. 093036. DOI: `10.1088/1367-2630/13/9/093036` (cit. on pp. 1, 3).

[CCY20] Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa. "Classical Verification of Quantum Computations with Efficient Verifier". In: *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*. Ed. by Rafael Pass and Krzysztof Pietrzak. Vol. 12552. Lecture Notes in Computer Science. Springer, 2020, pp. 181–206. DOI: `10.1007/978-3-030-64381-2_7` (cit. on pp. 7, 19).

[CGMO14] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. "Position-Based Cryptography". In: *SIAM J. Comput.* 43.4 (2014), pp. 1291–1341. DOI: `10.1137/100805005` (cit. on pp. 1, 13, 27).

[CHS05] Ran Canetti, Shai Halevi, and Michael Steiner. "Hardness Amplification of Weakly Verifiable Puzzles". In: *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*. Ed. by Joe Kilian. Vol. 3378. Lecture Notes in Computer Science. Springer, 2005, pp. 17–33. DOI: `10.1007/978-3-540-30576-7_2` (cit. on p. 7).

[DS21] Siddhartha Das and George Siopsis. "Practically secure quantum position verification". In: *New Journal of Physics* 23.6 (June 2021), p. 063069. DOI: `10.1088/1367-2630/ac0755` (cit. on p. 1).

[HLR21] Justin Holmgren, Alex Lombardi, and Ron D. Rothblum. "Fiat-Shamir via list-recoverable codes (or: parallel repetition of GMW is not zero-knowledge)". In: *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*. Ed. by Samir Khuller and Virginia Vassilevska Williams. ACM, 2021, pp. 750–760. DOI: `10.1145/3406325.3451116` (cit. on p. 23).

[JKKZ21] Ruta Jawale, Yael Tauman Kalai, Dakshita Khurana, and Rachel Zhang. "SNARGs for bounded depth computations and PPAD hardness from sub-exponential LWE". In: *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*. Ed. by Samir Khuller and Virginia Vassilevska Williams. ACM, 2021, pp. 708–721. DOI: `10.1145/3406325.3451055` (cit. on p. 23).

[JKPP21] Marius Junge, Aleksander M. Kubicki, Carlos Palazuelos, and David Pérez-García. *Geometry of Banach spaces: a new route towards Position Based Cryptography*. 2021. arXiv: `2103.16357v2 [quant-ph]` (cit. on p. 1).

[KMS11] Adrian Kent, William J. Munro, and Timothy P. Spiller. "Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints". In: *Phys. Rev. A* 84 (1 2011), p. 012326. DOI: `10.1103/PhysRevA.84.012326` (cit. on pp. 1, 3).

[KNY21] Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. *Secure Software Leasing from Standard Assumptions*. 2021. arXiv: `2010.11186v3 [quant-ph]` (cit. on pp. 5, 7).

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: `10.1017/CBO9780511976667` (cit. on p. 9).

[QS15] Bing Qi and George Siopsis. "Loss-tolerant position-based quantum cryptography". In: *Phys. Rev. A* 91 (4 Apr. 2015), p. 042337. DOI: `10.1103/PhysRevA.91.042337` (cit. on p. 2).

[RS19] Roy Radian and Or Sattath. "Semi-Quantum Money". In: *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, October 21-23, 2019*. ACM, 2019, pp. 132–146. DOI: `10.1145/3318041.3355462` (cit. on pp. 4, 5, 7, 10, 11, 19, 33).

[SWF+07] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter. "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km". In: *Phys. Rev. Lett.* 98 (1 Jan. 2007), p. 010504. DOI: `10.1103/PhysRevLett.98.010504` (cit. on p. 2).

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. "A monogamy-of-entanglement game with applications to device-independent quantum cryptography". In: *New Journal of Physics* 15.10 (2013), p. 103002. DOI: `10.1088/1367-2630/15/10/103002` (cit. on pp. 1, 3, 8, 23).

[Unr14] Dominique Unruh. "Quantum Position Verification in the Random Oracle Model". In: *Advances in Cryptology – CRYPTO 2014*. Ed. by Juan A. Garay and Rosario Gennaro. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 1–18. ISBN: 978-3-662-44381-1 (cit. on pp. 1, 3, 8, 25, 26).

[UTS+07] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, and et al. "Entanglement-based quantum communication over 144 km". In: *Nature Physics* 3.7 (June 2007), pp. 481–486. ISSN: 1745-2481. DOI: `10.1038/nphys629` (cit. on p. 2).

[Zha12] Mark Zhandry. "Secure Identity-Based Encryption in the Quantum Random Oracle Model". In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*. Ed. by Reihaneh Safavi-Naini and Ran Canetti. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 758–775. DOI: `10.1007/978-3-642-32009-5_44` (cit. on p. 26).

A NTCFs and 1-of-2 Puzzles

The following definition of NTCF families is taken verbatim from [BCM+18, Definition 6]. For a more detailed exposition of the definition, we refer the readers to the prior work.

Definition A.1 (NTCF family)**.** *Let λ be a security parameter. Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Let $\mathcal{K}_{\mathcal{F}}$ be a finite set of keys. A family of functions*

$$\mathcal{F} = \left\{ f_{k,b} : \mathcal{X} \to \mathcal{D}_{\mathcal{Y}} \right\}_{k \in \mathcal{K}_{\mathcal{F}}, b \in \{0,1\}}$$

is called a noisy trapdoor claw free (NTCF) family *if the following conditions hold:*

1. ***Efficient Function Generation.*** *There exists an efficient probabilistic algorithm $GEN_{\mathcal{F}}$ which generates a key $k \in \mathcal{K}_{\mathcal{F}}$ together with a trapdoor t_k:*

$$(k, t_k) \leftarrow GEN_{\mathcal{F}}(1^\lambda).$$

2. ***Trapdoor Injective Pair.*** *For all keys $k \in \mathcal{K}_{\mathcal{F}}$ the following conditions hold.*

   (a) Trapdoor: There exists an efficient deterministic algorithm $INV_{\mathcal{F}}$ such that for all $b \in \{0,1\}$, $x \in \mathcal{X}$ and $y \in \mathsf{SUPP}(f_{k,b}(x))$, $INV_{\mathcal{F}}(t_k, b, y) = x$. Note that this implies that for all $b \in \{0,1\}$ and $x \neq x' \in \mathcal{X}$, $\mathsf{SUPP}(f_{k,b}(x)) \cap \mathsf{SUPP}(f_{k,b}(x')) = \emptyset$.

   (b) Injective pair: There exists a perfect matching $\mathcal{R}_k \subseteq \mathcal{X} \times \mathcal{X}$ such that $f_{k,0}(x_0) = f_{k,1}(x_1)$ if and only if $(x_0, x_1) \in \mathcal{R}_k$.

3. ***Efficient Range Superposition.*** *For all keys $k \in \mathcal{K}_{\mathcal{F}}$ and $b \in \{0,1\}$ there exists a function $f'_{k,b} : \mathcal{X} \to \mathcal{D}_{\mathcal{Y}}$ such that the following hold.*

(a) *For all* $(x_0, x_1) \in \mathcal{R}_k$ *and* $y \in \mathsf{SUPP}(f'_{k,b}(x_b))$, *INV*$_\mathcal{F}(t_k, b, y) = x_b$ *and INV*$_\mathcal{F}(t_k, b \oplus 1, y) = x_{b\oplus 1}$.

(b) *There exists an efficient deterministic procedure CHK*$_\mathcal{F}$ *that, on input* k, $b \in \{0,1\}$, $x \in \mathcal{X}$ *and* $y \in \mathcal{Y}$, *returns* 1 *if* $y \in \mathsf{SUPP}(f'_{k,b}(x))$ *and* 0 *otherwise. Note that CHK*$_\mathcal{F}$ *is not provided the trapdoor* t_k.

(c) *For every* k *and* $b \in \{0,1\}$,

$$\mathop{\mathbb{E}}_{x \leftarrow_U \mathcal{X}} \left[H^2(f_{k,b}(x), f'_{k,b}(x))\right] \leq \mu(\lambda),$$

for some negligible function $\mu(\cdot)$. *Here* H^2 *is the Hellinger distance. Moreover, there exists an efficient procedure SAMP*$_\mathcal{F}$ *that on input* k *and* $b \in \{0,1\}$ *prepares the state*

$$\frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{(f'_{k,b}(x))(y)}\, |x\rangle\, |y\rangle\, .$$

4. ***Adaptive Hardcore Bit.*** *For all keys* $k \in \mathcal{K}_\mathcal{F}$ *the following conditions hold, for some integer* w *that is a polynomially bounded function of* λ.

(a) *For all* $b \in \{0,1\}$ *and* $x \in \mathcal{X}$, *there exists a set* $G_{k,b,x} \subseteq \{0,1\}^w$ *such that* $\Pr_{d \leftarrow_U \{0,1\}^w}[d \notin G_{k,b,x}]$ *is negligible, and moreover there exists an efficient algorithm that checks for membership in* $G_{k,b,x}$ *given* k, b, x *and the trapdoor* t_k.

(b) *There is an efficiently computable injection* $\mathcal{J} : \mathcal{X} \to \{0,1\}^w$, *such that* $\mathcal{J}$ *can be inverted efficiently on its range, and such that the following holds. If*

$$H_k = \left\{(b, x_b, d, d \cdot (\mathcal{J}(x_0) \oplus \mathcal{J}(x_1))) \mid b \in \{0,1\}, (x_0, x_1) \in \mathcal{R}_k, d \in G_{k,0,x_0} \cap G_{k,1,x_1}\right\},$$
$$\overline{H}_k = \left\{(b, x_b, d, c) \mid (b, x, d, c \oplus 1) \in H_k\right\},$$

then for any quantum polynomial-time procedure $\mathcal{A}$ *there exists a negligible function* $\mu(\cdot)$ *such that*

$$\left| \Pr_{(k,t_k) \leftarrow GEN_\mathcal{F}(1^\lambda)}[\mathcal{A}(k) \in H_k] - \Pr_{(k,t_k) \leftarrow GEN_\mathcal{F}(1^\lambda)}[\mathcal{A}(k) \in \overline{H}_k] \right| \leq \mu(\lambda).$$

Theorem A.2 ([BCM+21, Theorem 4.1])**.** *Assuming the post-quantum hardness of Learning with Errors (LWE) problem, NTCF families exist.*

Construction A.3. *Let* $\mathcal{F}$ *be an NTCF. An 1-of-2 puzzle can be constructed as follows.*

- *The* KeyGen *algorithm in 1-of-2 puzzle generates a public key* k *and a secret key (trapdoor)* t_k *for NTCF* $f_k = \{f_{k,b} : \mathcal{X} \to \mathcal{D}_\mathcal{Y}\}_{k \in \mathcal{K}_\mathcal{F}, b \in \{0,1\}}$. *Let* $\mathsf{pk} = k$ *and* $\mathsf{sk} = (k, t_k)$.

- *The* Obligate *algorithm prepares the evaluation of* f'_k *(instead of* f_k*) on the uniform superposition over all inputs, measures the image register to obtain* y *and apply* $\mathcal{J}$ *on the input. Let* ρ *be the post-measurement state of the input register, where* $\rho \approx |\psi\rangle\langle\psi|$, *and*

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle\, |\mathcal{J}(x_0)\rangle + |1\rangle\, |\mathcal{J}(x_1)\rangle)\, |y\rangle\, .$$

This is because f_k *has the trapdoor injective pair property and efficient range superposition property of* f'; $\mathcal{J}$ *is an injective procedure.*

- $\mathsf{Solve}(\mathsf{pk}, y, \rho, 0)$ *corresponds to measuring the two registers in state* ρ *in computational basis and outputting* $\mathsf{ans} = (b, \mathcal{J}(x_b)), b \in \{0, 1\}, x_b \in \{x_0, x_1\}$.

  $\mathsf{Ver}(\mathsf{sk}, y, 0, \mathsf{ans})$ *takes in secret key* $\mathsf{sk} = (k, t_k)$*, an obligation value* y*, the challenge bit* $b = 0$ *and* ans*. In this case* $\mathsf{ans} = (b, v)$*. The verification algorithm first obtains* $x' = \mathcal{J}^{-1}(v)$ *and outputs* 1 *if and only if* $y \in \mathsf{SUPP}(f'_{k,b}(x))$.

- $\mathsf{Solve}(\mathsf{pk}, y, \rho, 1)$ *corresponds to measuring state in Hadamard basis and outputting the measurement result* $\mathsf{ans} = (b, d)$.

  $\mathsf{Ver}(\mathsf{sk}, y, 1, \mathsf{ans})$ *takes in secret key* $\mathsf{sk} = (k, t_k)$*, an obligation value* y*, the challenge bit* $b = 1$ *and* ans*. In this case,* $\mathsf{ans} = (b, d)$*. It outputs* 1 *if and only if* $d \neq 0$ *and* $d \cdot (\mathcal{J}(x_0) + \mathcal{J}(x_1)) = b$.

We remark that Construction A.3 differs from [RS19, Algorithm 1] where we move the evaluation of $\mathcal{J}$ from Solve to $\mathsf{Obligate}$. Since evaluating $\mathcal{J}$ only acts on ρ and is independent of b, this is only a conceptual change and all the properties of the 1-of-2 puzzle preserve.

We can deduce the following facts by staring at the construction.

Fact A.4. *Construction A.3 has an XZ-solver.*

Fact A.5. *Construction A.3 has* 0*-challenge-public-verifiability.*

Proof. By NTCF definition, we can use procedure $\mathsf{CHK}_{\mathcal{F}}$ to check if $y \in \mathsf{SUPP}(f'_{k,b}(x))$ using only $\mathsf{pk} = k$. □