

# Beating Classical Impossibility of Position Verification

Jiahui Liu ✉

Department of Computer Science, University of Texas at Austin, TX, USA

Qipeng Liu ✉

Simons Institute for the Theory of Computing, Berkeley, CA, USA

Luowen Qian ✉

Department of Computer Science, Boston University, MA, USA

---

## 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.

**2012 ACM Subject Classification** Theory of computation → Cryptographic protocols; Security and privacy → Authorization; Security and privacy → Public key (asymmetric) techniques; Theory of computation → Quantum query complexity; Theory of computation → Quantum complexity theory

**Keywords and phrases** cryptographic protocol, position verification, quantum cryptography, proof of quantumness, non-locality

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2022.100

**Related Version** *Full Version*: <https://arxiv.org/abs/2109.07517>

**Funding** *Jiahui Liu*: supported by the NSF and Scott Aaronson's Simons Investigator award.

*Qipeng Liu*: supported by the Simons Institute for the Theory of Computing, through a Quantum Postdoctoral Fellowship.

*Luowen Qian*: supported by DARPA under Agreement No. HR00112020023.

**Acknowledgements** The authors would like to thank Ran Canetti and Shih-Han Hung for their helpful discussions.

## 1 Introduction

Position verification is the central task for position-based cryptography [15], 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. [15] 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



© Jiahui Liu, Qipeng Liu, and Luowen Qian;  
licensed under Creative Commons License CC-BY 4.0  
13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman; Article No. 100; pp. 100:1–100:11

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

## 100:2 Beating Classical Impossibility of Position Verification

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 [15, 11].

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 [7, 19, 24, 25, 12, 8, 17] explored this idea by constructing protocols with BB84 states (or other similar states [13, 5, 18]), and proving them to be unconditionally 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 [21] 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 [26, 23], 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 [6, 4].

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 pre-share 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.

## 2 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.** *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. [10], 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 2.** *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 3.** *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. [9], 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 [12, 7]. 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 [25].

We further show that there are also efficient attacks against Theorems 1 and 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 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  $\text{PostBQP} = \text{PP}$  machine<sup>1</sup> [2], as a consequence, it is impossible to construct unconditionally-sound proofs of quantumness (and thus classically verifiable position verification) without proving  $\text{PP} \not\subseteq \text{BPP}$ , even if we only consider position verification protocols with classical communications and quantum verifiers.

---

<sup>1</sup> The idea is that one can capture simulation of the quantum prover as a sampling variant of the  $\text{PostBQP}$  problem as follows: simulate the quantum prover's next classical message given the current classical transcript of the protocol.

### 3 Technical Overview

#### Quantum Position Verification with One Quantum Message

We first recall the position verification protocol investigated by many works [7, 19, 24, 12, 8]. 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  $\theta, x$  are uniformly random bits), and  $V_1$  sends a classical bit  $\theta$ , so that they arrive at the prover’s claimed position at the same time.  $P$  is supposed to measure the qubit in basis  $\theta$  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”.

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  $\theta$ , and therefore he cannot immediately measure it. However, if they decide to wait until  $\theta$  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  $\theta$ .

#### 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. [10], 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 [22]. 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  $f_{pk} : \{0, 1\}^n \rightarrow \mathcal{Y}$ . “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  $\text{pk}$ , cannot produce  $y, x, d$  that passes the two checks simultaneously with probability significantly higher than  $1/2$ , i.e.  $f_{\text{pk}}(x) = y$ ,  $d \cdot (x_0 \oplus x_1) = 0$ , 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 [22] and two-tier quantum lightning [20]. 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  $\text{pk}$  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  $y, \text{ans}$ , where  $y$  is the measured image of the superposition evaluation, and  $\text{ans}$  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  $\text{pk}, b$  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  $\text{pk}$ , he can simply run the honest prover twice – once on  $b = 0$  and once on  $b = 1$ . He obtains  $y_0, \text{ans}_0$  for  $b = 0$  and  $y_1, \text{ans}_1$  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  $y_b, \text{ans}_b$  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

## 100:6 Beating Classical Impossibility of Position Verification

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  $b$ ).

### Proving Soundness of CVPV

It turns out that with this simple fix, this CVPV can be proven secure. 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  $\frac{3}{4}$ .

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  $\frac{3}{4}$ . The proof is that assume  $(A_0, A_1)$  breaks the CVPV with probability noticeably higher than  $\frac{3}{4}$ , 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. It can be shown 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  $\rho_{BC}$  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  $\rho_B$  or  $\rho_C$  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  $\frac{3}{4}$ . 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  $p' := \Pr[W'_0 \wedge W'_1]$ .  $p' \leq \frac{1}{2} + \text{negl}$  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  $p \leq \frac{3}{4} + \text{negl}$  follows by rearranging the terms.

The computational unclonability requirements in prior works [22, 20] 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  $\frac{3}{4}$  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. Note that our protocol can be attacked if the adversaries have pre-shared entanglement. The attack is simply that one adversary, upon receiving  $\mathbf{pk}$ , could prepare the state (1) honestly, and then carry out the teleportation attack against the BB84 protocol. Therefore, entangled adversaries can simulate the honest prover perfectly. Combining with this attack, 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  $\frac{1}{2}$  if  $k$  is large enough using known results [22] (which in turn uses a classical parallel repetition theorem [14]). The  $\frac{1}{2}$  soundness here is tight as the adversaries can always guess  $b$  correctly with probability  $\frac{1}{2}$ .

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  $\frac{1}{2}$ , 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 [3, 16]. 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 [1, 24], 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 [25] 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 [24].



## 4 Future Directions

### High Dimensional Position Verification

We conjecture that the following construction, inspired by the position verification protocol of Unruh [25], could be secure in higher dimensions under the quantum random oracle model (QROM) using the ideas from Unruh:

1.  $V_0$  broadcasts  $pk$ .
2.  $V_0, \dots, V_n$  sample uniformly random strings  $x_0, \dots, x_n$  respectively and broadcast them. The timing is done so that these strings arrive 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  $H(x_0 \oplus \dots \oplus x_n)$ , 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 2 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 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.

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.

---

### References

- 1 Scott Aaronson. Limitations of quantum advice and one-way communication. *Theory Comput.*, 1(1):1–28, 2005. doi:10.4086/toc.2005.v001a001.

## 100:10 Beating Classical Impossibility of Position Verification

- 2 Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings: Mathematical, Physical and Engineering Sciences*, 461(2063):3473–3482, 2005. URL: <http://www.jstor.org/stable/30047928>.
- 3 Gorjan Alagic, Andrew M. Childs, Alex B. Grilo, and Shih-Han Hung. Non-interactive classical verification of quantum computation. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*, volume 12552 of *Lecture Notes in Computer Science*, pages 153–180. Springer, 2020. doi:10.1007/978-3-030-64381-2\_6.
- 4 Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Can you sign a quantum state?, 2021. arXiv:1811.11858v3.
- 5 Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. New protocols and ideas for practical quantum position verification, 2021. arXiv:2106.12911v1.
- 6 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*, pages 449–458. IEEE Computer Society, 2002. doi:10.1109/SFCS.2002.1181969.
- 7 Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, September 2011. doi:10.1088/1367-2630/13/9/093036.
- 8 Andreas Bluhm, Matthias Christandl, and Florian Speelman. Position-based cryptography: Single-qubit protocol secure against multi-qubit attacks, 2021. arXiv:2104.06301v2.
- 9 Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011. doi:10.1007/978-3-642-25385-0\_3.
- 10 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 Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 320–331. IEEE Computer Society, 2018. doi:10.1109/FOCS.2018.00038.
- 11 Joshua Brody, Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak. Position-based cryptography and multiparty communication complexity. In Yael Kalai and Leonid Reyzin, editors, *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 56–81. Springer, 2017. doi:10.1007/978-3-319-70500-2\_3.
- 12 Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM J. Comput.*, 43(1):150–178, 2014. doi:10.1137/130913687.
- 13 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*, pages 145–158, New York, NY, USA, 2013. Association for Computing Machinery. doi:10.1145/2422436.2422455.
- 14 Ran Canetti, Shai Halevi, and Michael Steiner. Hardness amplification of weakly verifiable puzzles. In Joe Kilian, editor, *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, volume 3378 of *Lecture Notes in Computer Science*, pages 17–33. Springer, 2005. doi:10.1007/978-3-540-30576-7\_2.
- 15 Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position-based cryptography. *SIAM J. Comput.*, 43(4):1291–1341, 2014. doi:10.1137/100805005.

- 16 Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa. Classical verification of quantum computations with efficient verifier. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*, volume 12552 of *Lecture Notes in Computer Science*, pages 181–206. Springer, 2020. doi:10.1007/978-3-030-64381-2\_7.
- 17 Siddhartha Das and George Siopsis. Practically secure quantum position verification. *New Journal of Physics*, 23(6):063069, June 2021. doi:10.1088/1367-2630/ac0755.
- 18 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.
- 19 Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84:012326, 2011. doi:10.1103/PhysRevA.84.012326.
- 20 Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions, 2021. arXiv:2010.11186v3.
- 21 Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *Phys. Rev. A*, 91:042337, April 2015. doi:10.1103/PhysRevA.91.042337.
- 22 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*, pages 132–146. ACM, 2019. doi:10.1145/3318041.3355462.
- 23 Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdignes, 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. *Phys. Rev. Lett.*, 98:010504, January 2007. doi:10.1103/PhysRevLett.98.010504.
- 24 Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013. doi:10.1088/1367-2630/15/10/103002.
- 25 Dominique Unruh. Quantum position verification in the random oracle model. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, pages 1–18, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.
- 26 R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdignes, P. Trojek, and et al. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3(7):481–486, June 2007. doi:10.1038/nphys629.