1 Introduction

An urgent question in the near future of quantum computing is the question of how a classical verifier can test a quantum device. This verifier could be an experimentalist running a new experimental setup, a consumer who has purchased a quantum device, or a client who wishes to delegate some task to a server who claims to have a quantum computer. For example, an experimentalist may test that a particular experiment is producing a certain predicted quantum state by performing a series of measurements, i.e. by state tomography, but this assumes some level of trust in the measurement apparatus being used. For a classical party to truly test a quantum system, that system should be models as having classical inputs, for example, representing measurement settings, and classical outputs, for example, representing measurement results.

Such tests of some quantum mechanical properties of a system first appeared in the form of Bell tests []. While violating Bell inequalities can be seen as a test of the existence of entanglement, the area of self-testing, first introduced in [**?**], allows for much stronger statements about precisely which measurements are being performed, on precisely which states. Informally, a *robust rigidity theorem* is a statement about precisely which kind of quantum strategy must be used to win a non-local game with close to optimal probability. Given such a theorem for a particular game, this game is a means of testing that such a strategy is being employed.

In 2012, Reichardt, Unger and Vazirani proved a robust rigidity theorem for playing a sequence of n CHSH games [**?**]. This rigidity theorem had two important consequences. One was the first was a device-independent protocol for quantum key distribution. The second, and perhaps surprising consequence of this rigidity theorem was a protocol whereby a completely classical verifier can test a universal quantum computer, consisting of two space-like separated devices. This latter test also models a situation in which a classical verifier wants to delegate an arbitrary quantum computation to an untrusted pair of non-communicating provers.

However, the overhead required, while polynomial, is prohibitively large. This is largely due to a very small (although still inverse polynomial) gap between the completeness and soundness of the rigidity theorem. The protocol in [**?**] requires resources that scale like $O(m^{8192})$ to perform an m-gate quantum circuit, making the approach infeasible for even a 2-gate circuit. Subsequent work has presented signifcantly mor efficient protocols for achieving the same functionality [**?**, **?**, **?**, **?**, **?**] (see Table 1, but the most efficient of these still requires resources that scale like $O(m^4 \log m)$ (**Stacey:** find the constant so we can claim that this is still infeasible for $m = 2$. Also check subsequent protocols. In particular, do they scale like m^4, or n^4?) .

In contrast, more efficient schemes for verifiable delegation exist in the cases where we allow the verifer the ability to generate single-qubit states []. (**Stacey:** more detail) For a survey, see [**?**].

(**Stacey:** The dog walker protocol might have a property called "cheat sensitivity", meaning a prover that tries to learn the input will be caught.)

Our contributions We present new self-testing results, and use them to modify Broadbent's EPR protocol to get two new two-prover classical-verifier protocols in which the complexity of verifiably delegating an m-gate quantum circuit is $O(m)$ []. (**Stacey:** Since constants have been an issue in the past, maybe we should give an upper bound on the hidden constant.) Specifically, we show the following:

Theorem 1 (Informal)**.** *Let $\varepsilon > 0$ and $n \in \mathbb{Z}_{>0}$. For any finite set of pairs of commuting two-qubit Clifford observables $\mathcal{G}$, there exists a constant c and a test* E-CLIFF$(\mathcal{G}, n)$ *with questions $\mathcal{G}^n$ such that any strategy that succeeds with probability $1 - \varepsilon$ must be ε^c-close to a strategy in which the players begin with $2n$ EPR-pairs and each player, on input W, applies the observable W, up to isometry.*

	sc-gap	provers	rounds	total resources	blind
RUV 2012 [**?**]	$1/\mathrm{poly}(n)$	2		$\geq m^{8192}$	yes
McKague 2013 [**?**]	$1/\mathrm{poly}(n)$	$\mathrm{poly}(n)$		$\geq 2^{153}g^{22}$	yes
HPF 2015 [**?**]	$1/\mathrm{poly}(n)$	$\mathrm{poly}(n)$		$m^4 \log m$	yes
GKW 2015 [**?**]	$1/\mathrm{poly}(n)$	2		m^{2048}	yes
HH 2016 [**?**]	$1/\mathrm{poly}(n)$			$m^4 \log m$	yes
FH 2015 [**?**]		5	1	$> n^4$	no
NV 2016 [**?**]	$\mathrm{const}(n)$	7		$> n^4$	no
V-on-a-leash (Section **??**)	$\mathrm{const}(n)$	2	T-depth$+1$	m	yes
Dog walker (Section **??**)	$\mathrm{const}(n)$	2	2	m	no

Table 1: **(Stacey:** I think a explicit comparison with previous results is useful, but I don't know exactly how we want to present it (i.e., which columns). For example, right now, I have the round complexity reflecting the number of rounds in the protocol, but this increases if you want to amplify the gap, so perhaps it's misleading. I think the total resources is actually our most impressive thing.) Above, m is the number of gates in the delegated circuit, g is the number of vertices of a graph state, $n \leq m$ is the size of the input to the circuit. **(Stacey:** tab:comparison)

This theorem is proven in Section **??**.

As a first application, we give a protocol in which a classical verifier delegates a quantum computation to a pair of entangled provers, one of which plays the role of Broadbent's prover, and the other of which plays the role of Broadbent's verifer. We ensure the correct behavior of the verifier-simulating prover using the new self-tests from Theorem **??**. We call this protocol the *Verifier-on-a-Leash Protocol*. This protocol has constant soundness-completeness gap, and requires $d+1$ rounds of linear interaction (in n), where d is the T-depth of the circuit being delegated. The input to the circuit is hidden from the provers, meaning that the protocol can be made blind by encoding the circuit in the input, and delegating a universal circuit.

Next, we modify Broadbent's protocol in a different way to achieve a second classical-verifier two-prover protocol. This protcol also has constant soundness gap, and in contrast to the Verifier-on-a-leash protocol, it uses only two rounds of linear communication, one round with each prover. One drawback of this protocol is that it is not blind.

This second protocol is similar to the first in that it has one prover simulating the prover in Broadbent's protocol, and one simulating the verifier. We are able to achieve much better round complexity, at the expense of a slightly more complicated proof, but the key ideas are still the same: we use a combination of the new self-testing results, and the techniques of Broadbent's protocol to control the two provers. Because of a more complicated "leash" structure in this protocol, we call it the *Dog Walker Protocol*.

The remainder of this paper is organized as follows. In Section **??**, we give the necessary preliminaries including outlining Broadbent's EPR protocol (Section **??**). In Section **??**, we present our new rigidity theorems. In Section **??**, we present our first protocol, the leash protocol, and in Section **??**, we present our second protocol, the dog walker protocol. In Section **??** we mention several open problems.

Open Questions One way to unconditionally force the two provers to refrain from communicating would be to ensure that they are far enough apart that messages from one will not reach the other before he must prepare his answer. In our schemes, this is not sufficient, because the input to one prover depends on the output of the other.