Device-Independent Verifiable Blind Quantum Computation

Michal Hajdušek,† Carlos A. Pérez-Delgado,‡ and Joseph F. Fitzsimons$^{1,2}$

$^1$Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682
$^2$Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543

As progress on experimental quantum processors continues to advance, the problem of verifying the correct operation of such devices is becoming a pressing concern. Although recent progress has resulted in several protocols which can verify the output of a quantum computation performed by entangled but non-communicating processors, the overhead for such schemes is prohibitive, scaling at least as the 22nd power of the number of gates. We present a new approach based on a combination of verified blind quantum computation and Bell state self-testing. This approach has significantly reduced overhead, with resources scaling as a quartic polynomial in the number of gates.

In recent years, significant progress has been made on the development of quantum information processing technologies. Basic operations with fidelities exceeding those required for fault-tolerant quantum computation have already been demonstrated in both ion-traps [1,2] and superconducting systems [3]. The number of qubits available in a single device is also approaching the limit of our ability to fully characterize the device, due to the exponential growth in the size of the state space. Quantum algorithms running on large scale quantum computers hold the promise of dramatic reductions in run time for certain problems. However, as the size of a quantum processor begins to exceed our ability to fully characterize it, the question of whether one can trust results produced in this manner naturally arises. For certain problems, such as integer factorization via Shor’s algorithm [4], the results of the computation can be verified efficiently by a classical computer. However, this property does not extend to a number of important problems such as the simulation of chemistry and other quantum systems [5].

While there is currently no known way to verify a single adversarial quantum processor, two distinct approaches have begun to emerge to the problem of verifying quantum processors based on interrogation performed during computation. In the first approach, a quantum processor is repeatedly queried by some other smaller quantum device, generally of fixed size, which can be characterized by conventional means. Aharonov, Ben-Or and Eban introduced an approach to such quantum prover interactive proofs based on quantum authentication using a fixed-sized quantum processor for the verifier [6]. An alternative route to verification is based on the universal blind quantum computation (UBQC) protocol of Broadbent, Fitzsimons and Kashefi [7], which provides an unconditionally secure [8] protocol for hiding quantum computations delegated to a remote server. By constructing the delegated computation to include certain traps it is possible to verify that the computation has been performed correctly, with exponentially small probability of error [9,10]. These protocols have extremely modest requirements for the verifier, simply the ability to prepare or measure single qubits in a finite set of bases. As such, it has proven possible to implement blind computation [11] and verification [12] in a system of four photonic qubits.

The second approach to verification is based on the interrogation of two or more entangled but non-communicating quantum processors. Reichardt, Unger and Vazirani [13] showed that arbitrary quantum processing could be verified entirely classically utilizing the statistics of CHSH games [14]. McKague [15] discovered an alternative approach using entangled processors based on measurement-based computation, through a self-testing protocol for certain graph states.

These two approaches have complimentary strengths and weaknesses. The second approach provides a stronger security, since the prohibition on communication between processors can be enforced through space-like separation of the devices. This removes the need for the verifier to place trust in any pre-existing device, no matter how simple, and can be said to be truly device independent: if the tests are passed, the verifier can be confident in the result of the computation even if quantum devices were constructed by an adversary, without need for any characterization. However the known protocols are only efficient in the theoretical sense, the required resources scale as an extremely high degree polynomial of the circuit dimensions. On the other hand, approaches to verification based on blind computation are characterized by far better resource scaling, with overhead scaling as low as linearly in the circuit size. Here we present a hybrid approach, in which self-testing is used to prepare the initial resource for verifiable blind computation, and then the computation is implemented using an existing blind computation scheme. The resulting protocol is entirely device independent, while requiring resources many orders of magnitude less than existing protocols.

When purely classical output is required, several blind quantum computation protocols [7,9,16] have the property that they can be decomposed into two phases: an initial state distribution phase, where direct quantum communication is used to prepare a fixed classical-quantum (CQ) correlation between the verifier’s classical system and the quantum processor to be tested, followed by an execution phase during which purely classical communication is used to implement and verify the computation. Our approach is to replace the first phase of an existing verification protocol, introduced in [9], with an alternate method of creating the same correlation which ad-
mits a self-testing strategy. The second phase of the protocol remains unaltered, and so security is guaranteed if the initial state can be prepared with sufficiently high fidelity.

Our remote state preparation procedure is inspired by a two-device variant of the UBQC protocol \[ \text{(17)} \]. Rather than directly transmitting a quantum state from the verifier to the server, measurements on one half of an entangled pair shared between two devices are used to project the remote system in a particular basis, thereby generating the desired correlations. We will assume that the verifier’s device consists of a simple measurement device capable of measuring individual qubits in an arbitrary basis, similar to blind computation approach taken by Morimae and Fujii \[ \text{(8)} \]. We will treat both the quantum part of the verifier’s device and the quantum processor to be verified as two (potentially collaborating but non-communicating) adversaries, yielding a situation in which there is a purely classical verifier and two quantum provers. We shall refer to the verifier as Alice and the quantum device to be verified as Bob, with the distinction between the quantum and classical systems of the verifier clear from context. We retain the terminology of the single prover setting, since, due to the asymmetry of the provers, it is natural to think of our approach as a blind quantum computing protocol in which Alice self-tests her own device.

At each step of phase one, Alice will receive a qubit from Bob. She chooses randomly to either use that qubit for verification purposes, or for the purpose of helping remotely create the resource state that will be used in phase two. The two procedures can be intuitively thought of, and are best analysed, as two distinct protocols. However it is crucial to keep in mind that the two protocols are randomly interwoven and executed in the same phase. This ensures that Bob has no knowledge about which qubits are used for self-testing and which for remote state preparation.

The self-testing procedure compares two experiments. The reference experiment consists of a bipartite state \(|\psi\rangle\) on Hilbert space \(Q\) and local observable \(T_{j}J\), where \(j\) labels the subsystem. The physical experiment consists of a bipartite state \(|\psi'\rangle\) on Hilbert space \(S\) and local observable \(T_{j}'\). In order to self-test operations and states with complex coefficients we also require Hilbert space \(R\), which is used to determine that the devices either both apply the desired operator or they both apply its complex conjugate. The physical experiment is \(\epsilon\)-equivalent to the reference experiment, if there exists a local isometry \(\Phi = \Phi_{A} \otimes \Phi_{B}\), such that

\[
\begin{align*}
|\Phi(T_{j}'|\psi'\rangle|S) & - \frac{1}{\sqrt{2}}(|\text{junk}_{1}\rangle_{S} \otimes T_{j}J|\psi\rangle_{Q}|00\rangle_{R} + |\text{junk}_{2}\rangle_{S} \otimes T_{j}'|\psi\rangle_{Q}|11\rangle_{R}| \leq \epsilon, \\
\end{align*}
\]

where \(\| \cdot \|_{2}\) is the vector distance defined for two vectors \(|a\rangle\) and \(|b\rangle\) as \(\|a\rangle - |b\rangle\|_{2} = \sqrt{(|a\rangle - |b\rangle)(|a\rangle - |b\rangle)}\), and \(T_{j}'\) is the complex conjugate of \(T_{j}J\). The state \(|\text{junk}\rangle_{S} \otimes T_{j}J|\psi\rangle_{Q}\) represents the ideal state up to local isometry \(\Phi_{id}\). This isometry is identical to \(\Phi\), however it uses the ideal statistics obtained from the reference experiment.

At every step of phase one, Bob is asked to prepare a Bell pair \(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\), and send half of it to Alice. At every step that is chosen for verification, Alice will measure the received qubit in a randomly chosen basis \(M' \in \{X_{A}, Y_{A}^{'}, Z_{A}^{'}, D_{A}', E_{A}', F_{A}'\}\), where \(D_{A}' = \frac{1}{2}(|X_{A} + Z_{A}^{'})\), \(E_{A}' = \frac{1}{2}(|X_{A} + Y_{A}^{'})\) and \(F_{A}' = \frac{1}{2}(|Y_{A} + Z_{A}^{'})\). After her measurement, Alice announces that the current step is for verification, and requests Bob to measure his half in the basis \(N' \in \{X_{B}', Y_{B}', Z_{B}'\}\) and send her the result. Here we use \(Y_{A}' = Y_{A} - Y_{B}\). Since the state that is being verified is symmetric, Alice does not need to test \(Y_{A}', Y_{B}', Z_{A}^{'}, Z_{B}^{'}, X_{A}^{'}, X_{B}'\) or \(Z_{A}^{'}, Y_{B}^{'}, Y_{A}'\). Furthermore, measurement settings \(D_{A}', E_{A}', F_{A}'\) are not necessary in our analysis, therefore she only needs to test the remaining 12 measurement settings.

Alice collects all measurement results, and at the end of phase one she performs a statistical verification, deciding whether, with some confidence \(p\), every single one of the qubits she received were part of a state \(\epsilon\)-close to a Bell pair. If this is the case, she announces this to Bob, and proceeds to phase two, otherwise she aborts. The verification protocol used in this phase is based on the approach of Mayers and Yao in \[\text{(19, 20)}\], which was greatly simplified and further developed by McHugh et al. in \[\text{(21, 22)}\]. This does not require a trusted measurement device, and can be tailored for any security parameters \(p\) and \(\epsilon\).

The graph state generation proceeds similarly to the UBQC protocol \[\text{(4, 5)}\]. However, instead of Alice sending a prepared qubit to Bob, Alice measures her half of the Bell pair in order to collapse Bob’s half of the pair to one of the valid input states. Specifically, the verification protocol for classical inputs and outputs which we will make use of (Protocol 6 of \[\text{(9)}\]), requires Alice to prepare and send to Bob, for each qubit \(1 \leq j \leq m\) needed in the computation stage, a state \(|\psi_{j}\rangle\) chosen uniformly at random either from the set \(|0\rangle, |1\rangle\) or the set \(|\theta_{j}\rangle\rangle_{\theta_{j} \in A}\), where \(|\theta_{j}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i \theta_{j}}|1\rangle)\) and \(A = \{0, \pi/4, ..., 7\pi/4\}\). Here, instead of directly preparing the state \(|\psi_{j}\rangle\), Alice instructs her measurement device to measure her half of the Bell pair in the basis \(|\theta_{j}\rangle, |\theta_{j}\rangle\), where \(\theta_{j} = |\theta_{j}, \pi\rangle\), if she wants to prepare a qubit in the \(x-y\) plane, and in the computational basis if she wants to prepare a dummy qubit. If she measures her half to be in the state \(|\theta_{j}\rangle\), then she knows that Bob’s state is (with high probability) in the state \(|\theta_{j}\rangle\). Similarly, if she measures \(|\theta_{j}\rangle\), then she knows that Bob’s half is in the state \(|\theta_{j}\rangle\). The case of measurements in the computational basis is even simpler. If Alice measures \(|s\rangle\), where \(s \in \{0, 1\}\), then Bob’s qubit will also be prepared in the same state. Since Alice does not announce the angle \(\theta_{j}\), and since the outcome of her measurement is uniformly random, Bob has no information about the input state. The state that they share is given by a CQ correlation, with Alice holding a classical label for Bob’s state, given by \(\frac{1}{2} \sum_{s \in \{0, 1\}} |s\rangle_{A} \otimes |s\rangle_{B}\) for dummy qubits and \(\frac{1}{2} \sum_{\theta_{j} \in A} |\theta_{j}\rangle_{A} \otimes |\theta_{j}\rangle_{B}\) for qubits used in computation. Tracing out Alice’s subsystem reveals that Bob’s state is maximally mixed.

Protocol \[\text{(1)}\] shows how Alice can remotely prepare single qubit states in Bob’s subsystem, up to isometry, without revealing such states to Bob and in a completely device-
Protocol 1 Device-Independent Remote State Preparation

**Input:** Security parameters $p$ and $\epsilon$, and constant $c \geq 1$.

**Steps:**

1. Alice initialises counters $k^{\alpha\beta} = 0$ and a correlation estimator $\hat{C}^{\alpha\beta} = 0$ for all $\alpha \in M'$ and $\beta \in N'$. She randomly partitions the $N = m + 12cm$ qubits that she will receive from Bob into $m$ qubits to be used for input preparation, and $N - m$ qubits to be used for verification from which she will randomly draw $n$ qubits per measurement setting.

2. For $1 \leq i \leq N$
   
   (a) Bob is asked to prepare a Bell pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and sends one half to Alice.
   
   (b) If the received qubit is for verification, then
   
   i. Alice randomly chooses an observable $\alpha$ from $M'$ and an observable $\beta$ form $N'$, and increments the counter $k^{\alpha\beta}$.
   
   ii. Alice measures her state according to $\alpha$, recording the outcome $a^{\alpha\beta}_{k^{\alpha\beta}} \in \{-1,1\}$.
   
   iii. Alice instructs Bob to measure his qubit according to $\beta$.
   
   iv. Bob measures his half of the prepared Bell pair in the instructed basis, and sends his result $b^{\alpha\beta}_{k^{\alpha\beta}} \in \{-1,1\}$ to Alice.
   
   v. Alice updates her correlation estimator for this particular measurement setting
   
   $\hat{C}^{\alpha\beta} = \frac{1}{k^{\alpha\beta}} \left( (k^{\alpha\beta} - 1)\hat{C}^{\alpha\beta} + a^{\alpha\beta}_{k^{\alpha\beta}} \cdot b^{\alpha\beta}_{k^{\alpha\beta}} \right)$.

   (c) If the received qubit is for remote state preparation, then
   
   i. Alice measures her half of the Bell pair in the basis $\{ |+\theta_{s}\rangle, |-\theta_{s}\rangle \}$, where $\theta_{s}$ is chosen uniformly at random from $A$, if Bob’s corresponding qubit is to be used for computation or for trap preparation. If his qubit is to be used for dummy qubit preparation, Alice measures in $\{ |0\rangle, |1\rangle \}$. If she’s measurement outcome is $|+\theta_{s}\rangle$, then Bob’s input qubit is $|+\theta_{s}\rangle$, whereas if her measurement outcome is $|\theta_{s}\rangle$, then Bob’s input qubit is $|\theta_{s}\rangle$. If, instead, Alice measures the computational basis and the outcome is $|s\rangle$, where $s \in \{0,1\}$, then Bob’s input qubit is $|s\rangle$. Alice stores a classical label for Bob’s state in memory.

   ii. If Alice’s measurement outcome is $|+\theta_{s}\rangle$, then Bob’s input qubit is $|+\theta_{s}\rangle$, whereas if her measurement outcome is $|\theta_{s}\rangle$, then Bob’s input qubit is $|\theta_{s}\rangle$. If, instead, Alice measures in the computational basis and the outcome is $|s\rangle$, where $s \in \{0,1\}$, then Bob’s input qubit is $|s\rangle$. Alice stores a classical label for Bob’s state in memory.

3. If $(1 - \exp(-\epsilon^2 n/8))^3 (1 - 2\exp(-\epsilon^2 n/8))^9 \geq p$, and $|\hat{C}^{\alpha\beta} - \mu^{\alpha\beta}| \leq \epsilon$, for all $\alpha$ and $\beta$, and $\mu^{\alpha\beta}$ is the value of ideal correlation for a particular $\alpha$ and $\beta$, then the protocol succeeds, otherwise it aborts. Alice also aborts if she does not gather enough statistics about a certain subset of correlations. The probability of this occurring decreases exponentially with increasing $c$.

Theorem 1. Let $|\psi\rangle$ be the untrusted state shared by Alice and Bob, and $\Pi_{M_A}$ be the projection corresponding to Alice’s measurement. At the end of Protocol 1 there exists a local isometry $\Phi$, such that

$$\|\Phi(\Pi_{M_A} |\psi\rangle) - \frac{1}{\sqrt{2}}(|\text{junk}_1\rangle_{3}\Pi_{M_A} |\phi^+\rangle_{Q}(00)\rangle + |\text{junk}_2\rangle_{3}\Pi_{M_A} |\phi^+\rangle_{Q}(11)\rangle)\|_2 \leq \min\{\tilde{\epsilon}, \sqrt{2}\},$$

with probability at least $p = (1 - \delta)^3 (1 - 2\delta)^9$. Here, the state of register $S$ is conditioned on the state of register $R$, register $Q$ contains the desired state, $\Pi^*$ denotes complex conjugate of $\Pi$, $\epsilon$ is the deviation from ideal statistics, $\delta = \exp(-\epsilon^2 n/8)$ is the probability that the real correlation differs from the ideal one by more than $2\epsilon$, $n$ is the number of qubits used for self-testing per measurement setting, and $\tilde{\epsilon} = O(\epsilon^{1/4})$.

Proof. The local isometry $\Phi$ captures the fact that the statistics remain unchanged under local change of basis, addition of ancillae, change of the action of the observables outside of the support of the state, and local embedding of the observables and states in a different Hilbert space. Explicit construction of $\Phi$ is discussed in Appendix A.

The first step uses a result obtained by McKague et al. in [21] which establishes a bound on the maximum distance between an untrusted shared state and an ideal Bell pair, up to local isometry, given statistics for correlations of measurements $\{X_A, X_A', D_A'\}$ on one subsystem and $\{X_B, X_B', D_B'\}$ on the other. Primed measurement observables and states signify that they are transformed, and states in a different Hilbert space. Explicit construction of $\Phi$ is discussed in Appendix A.

What remains to be shown is the scaling of Alice’s confidence about Bob’s state given the gathered statistics from self-testing. We forgo the use of a Chernoff bound as this would require the assumption of independent behaviour and would compromise device-independence. Rather we adopt a similar approach to Pironio et al. [23]. The measurement process can be modelled as a martingale which allows the application of the corresponding Azuma-Hoeffding inequality [24,25]. This leads to exponentially decreasing probability of error $\delta = \exp(-\epsilon^2 n/8)$. There are 12 correlations that need to be tested which leads to Alice’s confidence being at least $(1 - \delta)^3 (1 - 2\delta)^9$. A precise construction of the martingale and derivation of $\delta$ can be found in Appendix B.

Theorem 1 bounds the maximum distance between the ideal state, shared between Alice and Bob, which we denote $|\psi_{AB}^\prime\rangle$, and the actual state $|\phi_{AB}^\prime\rangle$ that they share, up to local isometry
Protocol 2 Device-Independent Blind Quantum Computation

Input: On Alice’s side:

1. A quantum computation expressed as a measurement based computation on a cylindrical brickwork state of $m$ qubits, with measurement angles $\phi = (\phi_i)_{1 \leq i \leq m}$ with $\phi_i \in A$, incorporating a random trap position $t$.
2. Security parameters $p$ and $\epsilon$.
3. $m$ random variables $\theta_i$ with values taken uniformly at random from $A$.
4. A fixed function $C_G$ that for each non-output qubit $i$ $(1 \leq i \leq m - n)$ computes the angle of the measurement of qubit $i$ to be sent to Bob. This function depends on $\phi_i, \theta_i, r_i, x_i$ and the result of the measurements that have been performed so far $(s_{<i})$.

Steps:

1. Alice and Bob engage in Protocol 1.
2. Bob takes his $m$ states prepared in the previous step and entangles them according to the cylindrical brickwork graph.
3. Alice sets all the values in $s$ to be $0$.
4. For $i$: $1 \leq i \leq m$
   a. Alice computes the angle $\delta_i = C_G(i, \phi_i, \theta_i, r_i, x_i, s)$ and sends it to Bob.
   b. Bob measures qubit $i$ with angle $\delta_i$ and sends Alice the result $b_i$.
   c. Alice sets the value of $s_{i}$ in $s$ to be $b_i \oplus r_i$.
5. After obtaining all the output qubits from Bob, if the trap qubit, $t$, is an output qubit, Alice measures with angle $\delta_t = \theta_t + r_t \pi$ to obtain $b_t$.
6. Alice accepts if $b_t = r_t$.

on Bob’s side (since the classical labels are stored in Alice’s classical memory rather than her quantum device). It is important to keep in mind that $|\psi_{AB}^B\rangle$ represents the ideal two-qubit state up to local isometry $\Phi_{id}$. In other words, $|\psi_{AB}^B\rangle$ is not itself a two-qubit state, just as performing a partial trace of it over Alice’s subsystem does not result in a single-qubit state on Bob’s subsystem. For any fixed value of Alice’s classical register the reduced state on Bob’s side is pure, denoted by $|\psi_j^B\rangle$, provided he follows the protocol honestly. Expressing the distance between this ideal state and the state obtained from a run of the protocol, in which Bob is not constrained to be honest, in terms of the vector distance makes it straightforward to obtain a lower bound on the fidelity of Bob’s input state. As shown in Appendix C, infidelity leads to an additive error in the probability of the verification protocols of [9] accepting an incorrect outcome.

This concludes phase one of our protocol which tests the operation of Alice’s device and produces a separable input state on Bob’s quantum computer with high probability. Alice then proceeds with the computation by instructing Bob to entangle the prepared qubits into a graph state, and use that graph state to perform verifiable blind computation. The protocol they follow is given in Protocol 2. It is based on Protocol 6 in [9]. We have modified the protocol found there to have classical input and output only, and in order to make it device-independent. Correctness follows directly from the correctness of the unmodified protocol.

The authentication protocol for a computation on $x \cdot y$ qubits, where $x$ is the number of rows and $y$ the number of columns of the brickwork state, relies on using a cylindrical brickwork state. The new cylindrical resource state introduces a sublinear overhead $m = (x + 2) \cdot y$. Alice chooses a random trap qubit $t$. She then randomly prepares all qubits in the same and neighbouring row of $t$ in $|0\rangle$ or $|1\rangle$. This ensures that after instructing Bob to entangle the resource state, the trap $t$ remains disentangled from the rest of the graph. Bob has no knowledge which qubit is used to detect his potential deviation from the protocol. Alice accepts only if Bob reports the correct measurement outcome for the trap qubit.

As a corollary of Theorem 1 we now show that Protocol 2 rejects incorrect outcomes with high probability.

**Corollary 1.** In Protocol 2 the probability that an incorrect outcome is accepted at the end of the verification procedure is

\[
p_{\text{error}} \leq 1 - \frac{p}{m} + p \sqrt{m \epsilon},
\]

where $p = (1 - \delta)^3(1 - 2\delta)^n$, $\delta = \exp(-\frac{1}{2} \epsilon^2 n)$, and $n = O(m^4)$ is the number of Bell pairs needed for self-testing per measurement setting.

**Proof.** Expanding the expression for the bound on the vector distance between the shared state $\|\psi_{AB}^j - \phi_{AB}^j\|_2 \leq \tilde{\epsilon}$, for all $j$, we get $\text{Re}(\langle \psi_{AB}^j | \phi_{AB}^j \rangle) \geq 1 - \frac{1}{2} \epsilon^2$, which can be used to obtain a lower bound on the fidelity between the states,

\[
F(|\psi_{AB}^j|, |\phi_{AB}^j|) \geq 1 - \frac{1}{2} \epsilon^2,
\]

where we used $F(|\psi_{AB}^j|, |\phi_{AB}^j|) = |\langle \psi_{AB}^j | \phi_{AB}^j \rangle|^2 \geq \text{Re}^2(|\psi_{AB}^j | \phi_{AB}^j \rangle)$. The fidelity is non-decreasing under partial trace which leads immediately to $F(|\psi_j^B|, |\rho_j^B|) \geq 1 - \frac{1}{2} \epsilon^2$. Thus, the fidelity of the entire $m$ qubit state is then given by

\[
F(\rho_{\leq m}^B - |\psi_B^B\rangle \langle \psi_B^B|) = \langle \psi_B^B | \rho_{\leq m}^B | \psi_B^B \rangle \geq 1 - m \epsilon^2.
\]

Using the relationship between trace distance and fidelity,

\[
\frac{1}{2} \| \rho_B^B - |\psi_B^B\rangle \langle \psi_B^B| \|_\text{tr} \leq \sqrt{1 - F(|\psi_B^B|, |\rho_B^B|)},
\]

it follows that

\[
\frac{1}{2} \| \rho_B^B - |\psi_B^B\rangle \langle \psi_B^B| \|_\text{tr} \leq \sqrt{m \epsilon}.
\]

The maximum probability of Alice accepting an incorrect outcome given an ideal input state is bounded by $\Delta \leq 1 - \frac{1}{m}$ as...
shown in [3]. Therefore the total probability of Alice accepting an incorrect outcome is bounded by
\[
p_{\text{error}} \leq p\Delta + \frac{P}{2}||\rho^{B}_{\tilde{\epsilon}} - |\psi^B||_{\text{tr}} + (1 - p) \leq 1 - \frac{P}{m} + p\sqrt{m}\hat{e}.
\]
From the expression for \( p \) we know that the number of Bell pairs per measurement setting in the verification of remote state preparation scales as \( n = O(\epsilon^{-2}) \). Requiring that \( \tilde{\epsilon} = O(m^{-2}) \) and using Theorem 1 which states that the \( \tilde{\epsilon} = O(\epsilon^{1/4}) \), we obtain the final result \( n = O(m^4) \).

Our scheme offers a large improvement over current schemes [13, 15] that achieve a similar function. Splitting the computation into two parts, namely device-independent remote state preparation followed by authenticated computation, presents a distinct advantage. At all stages of phase one we only need to self-test individual EPR pairs, unlike the approach in [15] that self-tests the entire graph state. This results in the number of repetitions of their protocol to be \( N \geq 3^{16} \cdot 10^{10.7} \cdot n^{32} \), where \( n \) is the number of vertices of the graph. It is worth noting that the client in [13] is completely classical and the protocol requires \( n \) non-communicating servers, each holding one vertex of the graph state. The protocol of Reichardt et al. [13] also considers a fully classical client and a constant number of non-communicating quantum servers. The client relies on CHSH games to test the shared states as well as the operation of the servers. To authenticate the whole computation, the client uses the servers to implement state and process tomography. This introduces a large overhead, where the leading term is of the order of at least \( n^{8192} \), where \( n \) counts the number of gates needed to implement the computation. In contrast to these earlier methods, the protocol described here requires an overhead in resources that scales as \( n^4 \). While this represents a drastic increase in efficiency over previous schemes, further reducing overhead remains an important open question.

Shortly before submission of this preprint, the authors became aware of parallel and independent research by Gheorghiu, Kashefi and Wallden, which also addresses device-independent verifiable blind quantum computation, and appears simultaneously. The authors acknowledge support from Singapore’s National Research Foundation and Ministry of Education. This material is based on research funded by the Singapore National Research Foundation under NRF Award NRF-NRFF2013-01.

[1] T. Harty, D. Allcock, C. Ballance, L. Guidoni, H. Janacek, N. Linke, D. Stacey, and D. Lucas, Physical Review Letters 113, 220501 (2014).
[2] C. Ballance, T. Harty, N. Linke, and D. Lucas, arXiv preprint arXiv:1406.5473 (2014).
[3] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. White, J. Mutus, A. Fowler, B. Campbell, et al., Nature 508, 500 (2014).
[4] P. W. Shor, in Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on (IEEE, 1994), pp. 124–134.
[5] S. Aaronson, in Proceedings of the forty-second ACM symposium on Theory of computing (ACM, 2010), pp. 141–150.
[6] D. Aharonov, M. Ben-Or, and E. Eban, in Innovations in Computer Science (Tsinghua University Press, 2010), p. 543.
[7] A. Broadbent, J. Fitzsimons, and E. Kashefi, in Foundations of Computer Science, 2009. FOCS’09. 50th Annual IEEE Symposium on (IEEE, 2009), pp. 517–526.
[8] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, in Advances in Cryptology–ASIACRYPT 2014 (Springer, 2014), pp. 406–425.
[9] J. F. Fitzsimons and E. Kashefi, arXiv preprint arXiv:1203.5217 (2012).
[10] T. Morimae, Physical Review A 89, 060302 (2014).
[11] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science 335, 303 (2012).
[12] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Nature Physics 9, 727 (2013).
[13] B. W. Reichardt, F. Unger, and U. Vazirani, Nature 496, 456 (2013).
[14] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Physical Review Letters 23, 880 (1969).
[15] M. McKague, arXiv preprint arXiv:1309.5675 (2013).
[16] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, Physical review letters 111, 230502 (2013).
[17] T. Morimae and K. Fujii, Physical review letters 111, 020502 (2013).
[18] T. Morimae and K. Fujii, Physical Review A 87, 050301 (2013).
[19] D. Mayers and A. Yao, in Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on (IEEE, 1998), pp. 503–509.
[20] D. Mayers and A. Yao, Quantum Information & Computation 4, 273 (2004).
[21] M. McKague, T. H. Yang, and V. Scarani, Journal of Physics A: Mathematical and Theoretical 45, 455304 (2012).
[22] M. McKague and M. Mosca, in Theory of Quantum Computation, Communication, and Cryptography (Springer, 2011), pp. 113–130.
[23] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al., Nature 464, 1021 (2010).
[24] W. Hoefding, Journal of the American Statistical Association 58, 13 (1963).
[25] K. Azuma, Tohoku Mathematical Journal, Second Series 19, 357 (1967).
[26] The definition of the function \( C_G \) is identical to the one found in [4], and its full description can be found there.

Appendix A: Derivation of \( \tilde{\epsilon} \) in Theorem 1

The derivation of \( \tilde{\epsilon} \) begins by applying the robustness results of McKague et al. from [21] for the real plane of the Bloch sphere, that is where \( |\psi| \). \( X'_{A,B} \), \( Z'_{A,B} \) and \( D'_A \) all have real coefficients. Assume the gathered cor-
relations satisfy \( \langle \psi' | X_A' | \psi' \rangle \geq 1 - 2\varepsilon, \langle \psi' | Z_A' | \psi' \rangle \geq 1 - 2\varepsilon, \langle \psi' | X_A' | Z_A' | \psi' \rangle \geq 1 - 4\varepsilon, \langle \psi' | D_A' | \psi' \rangle - \frac{1}{\sqrt{2}} \leq 2\varepsilon, \langle \psi | D_A' | \psi \rangle - \frac{1}{\sqrt{2}} \leq 2\varepsilon \) with high probability. This leads to bounds on the action of the measured observables,

\[
\begin{align*}
\| (X_A' + Z_A') | \psi' \rangle \| & \leq 2\varepsilon_1, \\
\| (X_A'Z_A' + Z_A'X_A') | \psi' \rangle \| & \leq 2\varepsilon_1 - 4\varepsilon_2, \\
\| (X_A' - Z_A') | \psi \rangle \| & \leq \varepsilon_2, \\
\| (Z_A' + X_A') | \psi \rangle \| & \leq \varepsilon_2,
\end{align*}
\]

where \( \varepsilon_1 = (1 + \sqrt{2}) \sqrt{2(1 + 2\sqrt{2})} + 2\sqrt{2\varepsilon} + 4\sqrt{\varepsilon} \) and \( \varepsilon_2 = 2\sqrt{\varepsilon} \). Using the above bounds it is possible to construct a local isometry \( \Phi \) that "extracts" the desired state into a new register \( | \psi \rangle \). \( \Phi \) is a reduced swap operation as shown in [21].

\[
\Phi(|\psi\rangle_S) = \frac{1}{4} (I + A) (I + B) | \psi \rangle_S | 00 \rangle_Q + \frac{1}{4} X_A' (I + A) (I + Z_B) | \psi \rangle_S | 01 \rangle_Q + \frac{1}{4} X_A' (I - A) (I + Z_B) | \psi \rangle_S | 10 \rangle_Q + \frac{1}{4} X_A' Z_B' (I - A) (I - B) | \psi \rangle_S | 11 \rangle_Q.
\]

We start by testing the device by obtaining statistics of measurements in the \( x = 0 \) plane. We denote the observable corresponding to these measurements as \( R_A' (\theta) = \cos \theta X_A' + \sin \theta Y_A' \). With repeated application of triangle inequality, we obtain \( \| \Phi(R_A'(\theta)|\psi\rangle_S) - | \text{junk} \rangle_S R_Q(\theta) | \phi^+ \rangle_Q \|_2 \leq \frac{1}{2} (17\varepsilon_1 + 5\varepsilon_2) \), where the state of the register \( S \) is \( | \text{junk} \rangle_S = \frac{1}{\sqrt{2}} (I + Z_A') (I + Z_B') | \psi \rangle_S \), while register \( Q \) holds the desired state. This is the usual Mayer-Yao test which allows us to establish that \( R_A \rightarrow R_{Q_A} R_Q \rightarrow Z_{Q_B} \rightarrow Z_{Q_B} R_Q \) and \( | \psi \rangle_S \rightarrow | \text{junk} \rangle_S | \phi^+ \rangle_Q \), as well as the bound on the vector distance between the real and the ideal states.

Assuming that the gathered statistics for \( Y_{A,B} \), \( E_A' \) and \( E_B' \) obey similar bounds, \( \langle \psi' | Y_A Y_B' | \psi' \rangle \geq 1 - 2\varepsilon \), \( \langle \psi' | X_A' X_B' | \psi' \rangle \leq 2\varepsilon \), etc., the above method can be extended to the complex plane [22]. This is achieved by introducing a new register \( R \), initialized in \( | 00 \rangle_R \), and using bounds on anti-commutation between \( Y_A' \) and \( X_A' \), \( Z_A' \) to establish that \( Y_A' \rightarrow Y_{Q_A} M_{S_A} \), where \( M_{S_A} \) is a unitary. This step introduces an error of at most \( 4\varepsilon_1 \). The isometry \( \Phi \) is composed with a phase kick-back isometry \( \Phi' \),

\[
\Phi'(| \text{junk} \rangle_S | \phi^+ \rangle_Q) = \frac{1}{4} (I + M_{S_A}) (I + M_{S_B}) | \text{junk} \rangle_S | \phi^+ \rangle | 00 \rangle_R + \frac{1}{4} (I + M_{S_A}) (I - M_{S_B}) | \text{junk} \rangle_S | \phi^+ \rangle | 01 \rangle_R + \frac{1}{4} (I - M_{S_A}) (I + M_{S_B}) | \text{junk} \rangle_S | \phi^+ \rangle | 10 \rangle_R + \frac{1}{4} (I - M_{S_A}) (I - M_{S_B}) | \text{junk} \rangle_S | \phi^+ \rangle | 11 \rangle_R.
\]

This step introduces an error of at most \( \frac{1}{2} \varepsilon_2 \). Adding these errors together gives the final bound of \( \varepsilon = \frac{1}{2} (25\varepsilon_1 + 10\varepsilon_2) \).

**Appendix B: Alice’s sampling**

To avoid cluttered notation, we omit the superscript \( \alpha \beta \), labeling the measurement setting. Denote the outcome of Alice’s measurement at step \( i \) by \( a_i \in \{-1, 1\} \) and similarly let \( b_i \in \{-1, 1\} \) denote Bob’s measurement outcome. Define a random variable \( C_i = a_i b_i \). The quantity \( \hat{C} = \frac{1}{n} \sum_{i=1}^{n} C_i \) is an estimate of the actual correlation between the devices. The behaviour of the devices is governed by the actual correlation \( C(W^i) = \Pr \{ a_i = b_i | W^i \} - \Pr \{ a_i \neq b_i | W^i \} \), where \( W^i \) is the full history of previous measurement settings and their outcomes up to and including step \( i - 1 \). The ideal value of the correlation is denoted by \( \mu \).

Define a new random variable,

\[
Y_n = \sum_{i=1}^{n} (\hat{C}_i - C(W^i)).
\]

The expected value of \( Y_n \) is finite and one can check that \( E(Y_{n+1} | W^{n+1}) = Y_n \). Therefore \( \{ Y_i \}_{i=1}^{n} \) forms a martingale with respect to \( \{ W^i \}_{i=2}^{n} \).

The increment \( c_i = Y_{i+1} - Y_i \leq 2 \) is bounded and so we can apply the Azuma-Hoeffding inequality for martingales,

\[
\Pr (Y_n \geq \gamma) \leq \exp \left( - \frac{\gamma^2}{2 \sum_{i=1}^{n} \epsilon_i^2} \right).
\]

Setting \( \gamma = n \epsilon \),

\[
\Pr \left( \frac{1}{n} \sum_{i=1}^{n} C(W^i) \leq \frac{1}{n} \sum_{i=1}^{n} \hat{C}_i + \epsilon \right) \leq \exp \left( - \frac{1}{8} \epsilon^2 n \right).
\]

This means that the probability of the actual value of correlation being lower than \( \epsilon \) from the measured value decreases exponentially. This bound can be used to determine the minimum confidence of Alice in her sampling of correlated measurement settings.

Defining the martingale as \( \delta_n = \sum_{i=1}^{n} (C(W^i) - \hat{C}_i) \) leads to a similar expression bounding the probability of the actual correlation being greater than the measured by \( \epsilon \).

\[
\Pr \left( \frac{1}{n} \sum_{i=1}^{n} C(W^i) \geq \frac{1}{n} \sum_{i=1}^{n} \hat{C}_i + \epsilon \right) \leq \exp \left( - \frac{1}{8} \epsilon^2 n \right).
\]

Combining these two expressions we arrive at the bound for the actual correlation being within \( 2\epsilon \) of the ideal value \( \mu \),

\[
\Pr \left( \left| \frac{1}{n} \sum_{i=1}^{n} C(W^i) - \mu \right| \leq 2\epsilon \right) \leq 2 \exp \left( - \frac{1}{8} \epsilon^2 n \right).
\]

Alice can conclude from her measurement data that \( \langle \psi | X_A X_B | \psi \rangle \geq 1 - 2\epsilon \) with probability at least \( 1 - \delta \), where \( \delta = \exp (-\epsilon^2 n / 8) \), and similarly for the other 2 correlated measurement settings. Applying the more general bound, Alice can also conclude that \( \langle | \psi' | X_A' X_B' | \psi' \rangle \leq 2\epsilon \) with probability at least \( 1 - 2\delta \), and similarly for the remaining 8 measurement settings. Assuming that the various \( \delta \) for different measurement settings are the same, Alice’s confidence that Bob is in possession of a state, that is \( \epsilon \)-close to the ideal one up to local isometry, is at least \( (1 - \delta)^{2(1 - 2\delta)} \).
Appendix C: Verification with imperfect states

Each of the verification protocols considered in [9] can be viewed as a quantum channel \( \mathcal{P}(\rho) \) which acts on a fixed CQ correlated state. The probability of accepting a state orthogonal to the output in the case of an honest run is then given by the expectation value of the projector \( P_{\perp} \) onto the orthogonal but accepted subspace. The initial state of Bob’s subsystem is \( \rho^B = p\rho^B_{\leq \tilde{\epsilon}} + (1-p)\rho^B_{\geq \tilde{\epsilon}} \), where \( p = (1-\delta)^{1/2} \) is the probability of preparing a state \( \rho^B_{\leq \tilde{\epsilon}} \) which is the result from Alice’s measurement on her subsystem, where the bipartite system \( |\phi_j^{AB}\rangle \) was \( \tilde{\epsilon} \)-close in vector distance to the ideal state \( |\psi_j^{AB}\rangle \) for all \( j \in \{1, \ldots, m\} \). \( \rho^B_{\geq \tilde{\epsilon}} \) is defined in a similar fashion. The probability of accepting an incorrect outcome is given by

\[
p_{\text{error}} = \text{Tr} \left( P_{\perp} \mathcal{P}(\rho^B) \right) = p \text{Tr} \left( P_{\perp} \mathcal{P}(\rho^B_{\leq \tilde{\epsilon}}) \right) + (1-p) \text{Tr} \left( P_{\perp} \mathcal{P}(\rho^B_{\geq \tilde{\epsilon}}) \right)
\]

where \( P_{\perp} \) is the projector onto the space orthogonal to the ideal output which is nonetheless accepted by the verification procedure, \( \Delta \) is the maximum probability of accepting an incorrect outcome using the ideal initial state \( |\psi^B\rangle \). We have also assumed the pessimistic case that the computation on an initial state far away from the ideal input results in a wrong output, but also get accepted.