In recent years considerable progress has been made in the realization of quantum technology based on a wide-range of physical settings. Most notably the demonstration of simple logic gates for quantum computing (QC) has been achieved. However, piecing these logic gates together in order to perform quantum algorithms capable of outperforming their classical analogues is still far from being practical. An approach to QC called the one-way model promises to help overcome this major problem. Here, a multipartite entangled state, the cluster state, is used as a resource to perform QC where the amount of control one needs over a quantum system is reduced to the ability of performing just single-qubit measurements. This is an important advantage for a variety of physical systems, such as those using photons, where already the model’s general features have been experimentally demonstrated in setups with bulk components. We are now faced with two key challenges. The first is to identify the minimal resources needed for performing quantum protocols so that small-scale algorithms can be demonstrated and eventually scaled up. Second, it is vital that optimal methods are found for transferring what has been done in bulk setups to more practical and ultimately scalable settings.

In this work we address these two important challenges. We show that fundamental versions of the Deutsch-Jozsa (DJ) and Bernstein-Vazirani (BV) algorithms can be demonstrated using one-way QC on a small entangled cluster state of only six qubits. Moreover, we investigate the resources needed for demonstrating general n-qubit versions of the algorithms. We then propose a versatile photonic on-chip setup where they could be realized and eventually scaled-up. Our proposal represents the first scalable method for demonstrating these algorithms in the promising context of one-way QC. Recently on-chip and waveguide setups have started to gain momentum as prominent settings for full-scale QC. Here different components - requiring expertise from a broad range of the physical sciences - must be integrated together, making this a truly multidisciplinary endeavor. However, once a given setup is fabricated it is not possible to change it. Our proposal addresses this problem by providing an architecture of minimal resources on which to realize various algorithms.

DJ Algorithm. We start by briefly reviewing the DJ algorithm which takes an n-bit binary input $x \in \{0,1\}^n$ and allows one to distinguish two types of function $f(x)$ that apply the transformation $f(x) : \{0, \ldots, 2^n - 1\} \mapsto \{0, 1\}$ implemented by an oracle. $f(x)$ is constant if it returns the same value (0 or 1) for all inputs and balanced if it returns 0 for half the inputs and 1 for the other half. Classically the oracle must be queried as many as $(2^n / 2) + 1$ times in the worst case. Quantum mechanically only one query is required in all cases.

The quantum algorithm begins with the state $2^{-n / 2} \sum_{x \in \{0,1\}^n} |x\rangle |y\rangle = |+\rangle^\otimes n |0\rangle$, where $|y\rangle$ is an ancilla qubit, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $\{0\},\{1\}$ is the single-qubit computational basis. The oracle applies the transformation $|x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$, producing the state $2^{-n / 2} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle |\cdot\rangle$. Hadamard gates $H = (\sigma_x + \sigma_z)/\sqrt{2}$ are then applied to all the query qubits ($\sigma_{x,y,z}$ are the Pauli matrices), resulting in the state $|\psi_{\text{out}}\rangle = 2^{-n} \sum_z \sum_{x} (-1)^{x \cdot z + f(x)} |z\rangle$ (where $x \cdot z$ is the bitwise inner-product of $x$ and $z$). The amplitude for the state of the query qubits as $|0\rangle^\otimes n$ is $\sum_{x} (-1)^{f(x)} / 2^n$. There are two cases: First, if $f(x)$ is constant then the amplitude for $|0\rangle^\otimes n$ is +1 or -1 depending on the constant value $f(x)$ takes. As $|\psi_{\text{out}}\rangle$ is of unit length, all other amplitudes go to zero. Second, if $f(x)$ is balanced, then the positive and negative contributions to $|0\rangle^\otimes n$ cancel, leaving an amplitude of zero. Therefore if $|\psi_{\text{out}}\rangle = |0\rangle^\otimes n$ is measured, $f(x)$ is constant, otherwise $f(x)$ is balanced. Thus, only one query is required. A refined version of the above algorithm has been suggested. Here, one identifies that the ancilla qubit $|y\rangle$ is unentangled both before and after the black box operation and can be removed. The oracle’s action then reduces to $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$, with the remainder of the algorithm performed as described above. For a one-qubit query register (DJ1), the algorithm corresponds to Deutsch’s problem, for which it is known a four-qubit cluster state can be used. Thus in what follows we consider the fundamental case of DJ2. We then discuss the corresponding refined version and finally arbitrary n-qubit versions.
The measurement basis determines the rotation \( R \) and cluster state. FIG. 1: Black box (BB) circuits for the Deutsch-Jozsa algorithm and cluster state. (a) BB’s (i) and (ii) ((iii)-(viii)) correspond to constant (balanced) functions. See Table I for \( f(x) \) in each case. (b): The six-qubit cluster state \( |\Phi_C\rangle \) depicting the input/output logical qubits. The measurements and outcomes of qubits 1, 3 and 6 constitute the algorithm. The measurements of qubits 2, 4 and 5 (and their feed-forward) are carried out by the oracle, thus boxes surround these qubits.

**Cluster state implementation.** The action of an oracle is preset or dictated by the outcome of another algorithm and is known as a *promise* problem [3]. In order to implement all the functions that it might use for DJ2, we must be able to construct them using a combination of quantum gates. In Fig. 1(a) we show all the oracle functions in terms of their quantum network. By describing each as a “black box”, one can see that all eight black boxes (BB(i)-(viii)) implement their respective oracle function given in Table I. In order to carry out the algorithm using these quantum gates, the six-qubit cluster state resource shown in Fig. 1(b) can be used, where one-way QC is carried out by performing a program of measurements. No adjustment to the resource is necessary; each BB corresponds to a different measurement program on the same resource.

For a cluster state two types of single-qubit measurements allow one-way QC to be performed. First, measuring a qubit \( j \) in the computational basis removes it from the cluster, leaving a smaller cluster state of the remaining qubits. Second, in order to perform QIP, qubits must be measured in the basis \( B_j(\alpha) = \{|\alpha, +\rangle_j, |\alpha, -\rangle_j\} \), where \(|\alpha, +\rangle_j = (|0\rangle \pm e^{i\alpha}|1\rangle)/\sqrt{2} \) (\( \alpha \in \mathbb{R} \)). Choosing the measurement basis determines the rotation \( R_\alpha = \exp(-i\alpha\sigma_z/2) \), followed by a Hadamard operation \( H \) applied to an encoded logical qubit in the cluster residing on qubit \( j \). With a suitable cluster, any quantum logic operation can be performed using a measurement program \( \mathcal{M} \) with an appropriate choice for the \( B_j(\alpha) \)’s.

The cluster state resource of Fig. 1(b) is given by \( |\Phi_C\rangle = \frac{1}{\sqrt{2}}(|\phi_2\rangle_{12}|0\rangle_{34}|\phi_2\rangle_{65} + |\phi_2\rangle_{12}|1\rangle_{34}|\phi_2\rangle_{65}) \), where \(|\phi_2\rangle_{ab} = (1/\sqrt{2})(|+\rangle_0|0\rangle \pm |\rangle_0|1\rangle)\). A set of measurement bases for the qubits in this resource can be used for each BB. In Table I we provide these bases and feed-forward (FF) operations [7, 9]. Fig. 1(b) shows the in-out states of the algorithm, where the logical input corresponding to \(|x\rangle = |x_1\rangle |x_2\rangle = |+\rangle |+\rangle \) is encoded on qubits 1 and 6. The state \(|y\rangle = |-\rangle \) is encoded on qubit 4 using a \( \sigma_z \) operation before the measurement program begins: the resource \(|\Phi_C\rangle = (\sigma_z)^4 |\Phi_C\rangle \) remains as a cluster state with the state \(|x_1\rangle |x_2\rangle |y\rangle = |+\rangle |+\rangle |-\rangle \) residing on the logical input register.

Qubits 2 and 5 in \( |\Phi_C\rangle \) play the pivotal role of the oracle by performing two-qubit gates between the logical input states \(|x_1\rangle, |x_2\rangle \) and \(|y\rangle \). For BB(i), measuring qubits 2 and 5 in the computational basis disentangles them from the cluster and \( |\Phi_C\rangle \) is transformed into \((1/2\sqrt{2})(|0\rangle + (-1)^{x_2} |1\rangle)(|0\rangle |-\rangle + (-1)^{\chi_5+\chi_6} |1\rangle |+\rangle + (1)^{\chi_5+\chi_6} |1\rangle |\rangle \) (where \( s_i \) corresponds to the outcome of qubit \( i \)’s measurement). The logical operation performed by this choice of the oracle’s measurement basis is \( I \otimes I \otimes H \) (up to FF operations). By including the \( H \) operation applied to the state \(|y\rangle \) from the measurement of qubit 4 in the basis \( B_2(0) \), the overall computation results in \( I \otimes I \otimes H |+\rangle |+\rangle |-\rangle \) which is equivalent to \(|x\rangle |y\rangle \otimes f(x) = (I \otimes I \otimes I), |+\rangle |-\rangle \) up to a local rotation \( H \) on qubit 3 incorporated into the FF stage. Qubits 1, 3 and 6 can now be taken as the output state \(|x\rangle |y\rangle \otimes f(x) \). On the other hand, for BB(iii), upon measuring qubit 5 in the \( B_5(\pi/2) \) basis and qubit 2 in the computational basis, the oracle applies the gate \((R_x(\pi/2) \otimes R_z(\pi/2))|CZ\) between \(|x_1\rangle \) and \(|y\rangle \), where \( CZ \) shifts the relative phase of the state \(|1\rangle |1\rangle \) by \( \pi \) with respect to the rest of the computational basis states. Here, \(|x_2\rangle \) remains unaffected. By including the measurement of qubit 4 again, this gives the computational \(|x_1\rangle |y\rangle \otimes f(x) \rangle = CNOT \otimes |+\rangle |-\rangle \equiv |R_x(\pi/2) \otimes R_z(\pi/2) \otimes I |CZ \otimes I \otimes H \otimes I \rangle |+\rangle |-\rangle \rangle \) up to local rotations \([R_x(-\pi/2) \otimes H \otimes R_y(-\pi/2) \otimes I] \) incorporated into the FF stage. For BB(v), the roles of qubits 2 and 5 in the program for BB(iii) are interchanged, thus implementing a CNOT between \(|x_2\rangle \) and

| \( f(x) \) | \( x \) | \( \chi_1 \) | \( \chi_2 \) | \( \chi_4 \) | \( \chi_5 \) | \( \chi_6 \) | \( \chi_{x_1} \) | \( \chi_{x_2} \) |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |

| \( M_0 \) | \( B(0) \) | \( B(0) \) | \( B(0) \) | \( B(0) \) | \( B(0) \) | \( B(0) \) |
|---|---|---|---|---|---|---|
| \( M_0 \) | \( B(0) \) | \( B(0) \) | \( B(0) \) | \( B(0) \) | \( B(0) \) |
| \( M_0 \) | \( B(0) \) | \( B(0) \) | \( B(0) \) | \( B(0) \) | \( B(0) \) |
| \( F_{x_1} \) | \( \sigma_{y_1} \) | \( \sigma_{y_1} \) | \( \sigma_{y_1} \) | \( \sigma_{y_1} \) | \( \sigma_{y_1} \) |
| \( F_{x_2} \) | \( \sigma_{y_2} \) | \( \sigma_{y_2} \) | \( \sigma_{y_2} \) | \( \sigma_{y_2} \) | \( \sigma_{y_2} \) |
| \( F_{x_3} \) | \( \sigma_{y_3} \) | \( \sigma_{y_3} \) | \( \sigma_{y_3} \) | \( \sigma_{y_3} \) | \( \sigma_{y_3} \) |
| \( F_{x_4} \) | \( \sigma_{y_4} \) | \( \sigma_{y_4} \) | \( \sigma_{y_4} \) | \( \sigma_{y_4} \) | \( \sigma_{y_4} \) |
| \( F_{x_5} \) | \( \sigma_{y_5} \) | \( \sigma_{y_5} \) | \( \sigma_{y_5} \) | \( \sigma_{y_5} \) | \( \sigma_{y_5} \) |
| \( F_{x_6} \) | \( \sigma_{y_6} \) | \( \sigma_{y_6} \) | \( \sigma_{y_6} \) | \( \sigma_{y_6} \) | \( \sigma_{y_6} \) |

Table I: Black box outputs for the DJ algorithm and measurement program \( \mathcal{M} \) for qubit \( 1 \) of the cluster state with feed-forward operations. The notation \( /0/1 \) corresponds to a measurement in the computational basis, \( \chi_i = \sigma_x^{s_i} R_z(-\pi/2), \chi = \sigma_z^{s_5} \sigma_x^{s_6} H \) and \( \chi = \chi_{x_1} \). The value \( s_i \) corresponds to the outcome of qubit \( j \)’s measurement.
Finally, for BB’s (ii), (iv), (vi) and (viii) an additional $\sigma_x$ rotation is applied to qubit 3 at the FF stage using the measurement programs of BB’s (i), (iii), (v) and (vii) respectively. The initial $\sigma_x$ rotation on qubit 4, along with the measurements and outcomes of qubits 1, 3 and 6 constitute the algorithm, although only the query qubits need to be measured. The additions to the FF and measurements of qubits 2, 4 and 5 should be viewed as being carried out entirely by the oracle.

In the refined version of the algorithm one replaces the ancilla $|y\rangle$ with an additional query qubit $|x_3\rangle$. The initial Hadamard gate is not required and qubit 4 can be removed, with qubit 3 as the input for $|x_3\rangle$. The resource requirement is therefore a five-qubit cluster state. Unfortunately, in this configuration it is not possible to implement all of the BB’s that the oracle might perform for DJ$_3$. This point will be discussed in more detail later.

$BV$ algorithm.- In this algorithm an $n$-bit binary input $x \in \{0,1\}^n$ is used and the problem is to determine the hidden value $s \in \{0,1\}^n$ of the function $f_s(x) = s \cdot x$ carried out by an oracle. The oracle’s transformation is $f_s(x) : \{0,1\}^n \rightarrow \{0,1\}$ and classically one needs to make $n$ queries in order to determine $s$. This problem can be seen as a more sophisticated database search compared to the one in Grover’s search algorithm. Here, the oracle plays the role of a database where records are represented by vectors. Record $s$ is tagged and when the oracle is queried with a specific record $x$, it responds by providing information $s \cdot x$ signifying the similarity of the guess to the tagged record $s$. This resembles the response from a web search-engine, where the pages are usually ordered by their relevance. Using the BV algorithm only one query is necessary to find the tagged record. A similar method to the DJ algorithm is employed using the same input states. Taking the output state from the oracle $|\psi_{out}\rangle = 2^{-n} \sum_s \sum_x (-1)^{s \cdot x + f_s(x)} |s\rangle |x\rangle = 2^{-n} \sum_s \sum_x (-1)^{s \cdot x} |s\rangle |x\rangle$ we have, using the relation $2^{-n} \sum_x (-1)^{x \cdot z} = \delta_{x,z}$, that $|x\rangle \rightarrow (-1)^{f_s(x)} |x\rangle$. Therefore measuring the output query register once reveals the value of $s$. As before, in the refined version, the ancilla qubit is removed and the oracle transformation is $|x\rangle \rightarrow (-1)^{f_s(x)} |x\rangle$. The remainder of the procedure is performed as described above.

$BV_1$ reduces to Deutsch’s problem, thus we consider the fundamental version of the algorithm as $BV_2$. Here the required black boxes correspond to BB’s (i), (v), (iii) and (vii) of DJ$_2$ for $s = 00, 01, 10$ and 11 respectively. Thus surprisingly the same cluster state $|\Phi_C\rangle$ can be used. For the refined version, $BV_3$, qubit 4 is again removed and qubit 3 becomes $|x_3\rangle$. However, it turns out that no two-qubit gates are required between the $|x_i\rangle$’s, only local $\sigma_z$ operations: a cluster state is not necessary for the refined version.

On-chip photonic demonstration.- We now propose a setup that could be used to generate the cluster state $|\Phi_C\rangle$ and demonstrate the algorithms. Fig. 2 (a) shows a network of photonic silica-on-silicon waveguides, where the polarization degrees of freedom of a photon in mode $i$ embody a qubit with the association $|0\rangle_i \rightarrow |H\rangle_i$ and $|1\rangle_i \rightarrow |V\rangle_i$. Initially, photons are generated in waveguide modes 1 to 6 by optically pumping individual quantum dots whose emission is directly coupled into the respective waveguide. The photons are then prepared in the state $|+\rangle$ by liquid crystal (LC) polarization rotators that are voltage-controlled by indium tin oxide (ITO) electrodes. The action of the polarization beamsplitters (PBS’s) that follow is to apply a $\pi$-rotation $|HH\rangle \rightarrow |HH\rangle + |VV\rangle \rightarrow |VV\rangle$ on two photon modes when a single photon exits each output port. This occurs with probability $1/2$. The PBS component is depicted in more detail in Fig. 2 (b), where the region between two waveguides is filled with LC having no effect on $V$-polarized photons but switching those with $H$-polarization (see caption for further details). We note that such an on-chip component has not been considered before for quantum processing and could represent a versatile component in advanced photonic quantum technology. Considering the action of the PBS’s and polarization rotations $H$ before the detection stage, it is straightforward to show that if one photon is present in each mode, leading to one photon at each detector-pair $D_i$ in coincidence, the state $|\Phi_C\rangle$ will be generated upon detection. All other possibilities do not lead to a six-photon coincidence and therefore can be post-selected out. For this purpose we consider superconducting single-photon detectors embedded within the chip. The measurement programs are realized at the detector stage using the final polarization rotator and PBS before each detector-pair.

Scalability.- We now investigate extending the method proposed here for performing arbitrary $n$-qubit versions of both algorithms. In order to be able to im-
implement all BB functions for the standard (refined) DJ algorithm with $n \geq 3$, a Toffoli ($C^2Z$) gate is required. A simple example is the balanced $CZ$ gate between $x_2$ and $x_3$ and $|y\rangle (|x_1\rangle, |x_2\rangle$ and $|x_3\rangle)$, with $|y\rangle (|x_j\rangle)$ the target and a CNOT ($Z$) gate between $|x_1\rangle$ and $|y\rangle (|x_3\rangle)$. Fortunately, it is always possible to implement a selection of constant and balanced BB's for arbitrary $n$ by using combinations of controllable-CNOT's (8) between the query qubits $|x_i\rangle$ and the ancilla $|y\rangle$ (controllable-CZ's between the query qubits), as presented for DJ$_2$. This drastically reduces the resource requirements for demonstration purposes. For the BV algorithm one can see by inspection of the oracle's action $f_s(x) = s \cdot x = (x_1 \land s_1) \oplus (x_2 \land s_2) \oplus \cdots \oplus (x_n \land s_n)$ that it is easily generalized. In the standard (refined) case, the value of $|x_i\rangle$ determines whether or not to apply a $C_x (s_x)$ operation to $|y\rangle (|x_i\rangle)$. In Fig. 3 (a) we show a graph state (23) that could be used for demonstrating both DJ$_n$ and BV$_n$. In Fig. 3 (b) we show a possible way to scale up the resource via fuse operations, which could be realized using our proposed on-chip setup. Note that as each branch is created with probability $1/4$, the success probability of generating the state decreases exponentially with $n$, however this has no effect on the performance of the algorithms. If needed, more economical generation techniques could be used for large $n$ (21). With the use of on-chip photon-number resolving detectors (24) and appropriate network for error-correction one can achieve a scalable method to demonstrate the algorithms.

We have shown that fundamental versions of the DJ and BV algorithms can be performed on a six-qubit cluster state and investigated the minimal resources for scaling up to general $n$-qubit versions. A photonic on-chip setup was then proposed for realizing our scheme in a scalable context. The techniques described here could be applied equally well to other algorithms and protocols. Although we present an on-chip setting our proposal is readily applicable to other types of waveguide and bulk setups. As these settings require researchers from a wide range of the physical sciences working together, we expect this study to stimulate progress of practical and scalable QC in both a theoretical and experimental capacity.

We thank C. Di Franco and R. Prevedel for comments and acknowledge support from UK EPSRC and QIP IRC.

Note added.- After this work was written up we became aware of a related, although not as general, cluster state experiment using bulk optics (25).

![FIG. 3: Configuration for DJ$_n$ and BV$_n$. (a): Graph state depicting the in-out logical qubits. (b): Construction by PBS fusion ($|HH\rangle\langle HH| + |VV\rangle\langle VV|_{12}$ followed by $I_1 \otimes H_2$) from one pair of photons already fused in the state $(I \otimes H)^{1/2}[|HH\rangle + |VV\rangle]_{23}$ and two single photons in $|+\rangle$.](image-url)