Experimental Realization of Simon's Problem Functions in a One-way Quantum Computer

M. S. Tame,[1,2,*] B. A. Bell,[3] C. Di Franco,[4] W. J. Wadsworth,[5] and J. G. Rarity[3]

[1]*University of KwaZulu-Natal, School of Chemistry and Physics, 4001 Durban, South Africa*
[2]*National Institute for Theoretical Physics, University of KwaZulu-Natal,Durban 4001, South Africa*
[3]*Photonics Group, Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK*
[4]*Quantum Optics and Laser Science Group, Imperial College London, Blackett Laboratory, SW7 2AZ London, UK*
[5]*CPPM, Department of Physics, University of Bath, Claverton Down, Bath, BA2 7AY, UK*

(Dated: September 19, 2014)

We report an experimental demonstration of a one-way implementation of a quantum algorithm solving Simon's Problem - a black box period-finding problem which has an exponential gap between the classical and quantum runtime. Using an all-optical setup and modifying the bases of single-qubit measurements on a five-qubit cluster state, key representative functions of the logical two-qubit version's black box can be queried and solved. To the best of our knowledge, this work represents the first experimental realization of the quantum algorithm solving Simon's Problem. The experimental results are in excellent agreement with the theoretical model, demonstrating the successful performance of the algorithm. With a view to scaling up to larger numbers of qubits, we analyze the resource requirements for an n-qubit version. This work helps highlight how one-way quantum computing can provide a practical route to experimentally investigating the quantum-classical gap in the query complexity model.

PACS numbers: 03.67.-a, 03.67.Mn, 42.50.Dv, 03.67.Lx

Quantum information science promises to radically change the way we communicate and process information in future devices based on quantum technology [1–3]. One of its major goals is to realize multi-qubit quantum algorithms, involving large numbers of logic gates, that outperform their classical analogues [4, 5]. While there has been steady experimental progress made during recent years in demonstrating basic quantum logic gates in various settings [3], the process of piecing them together in order to perform useful algorithms is still far from practical. Demonstrations of few-qubit quantum algorithms therefore play an important role in stimulating further advances in experimental quantum computing (QC) and help open up viable routes toward full-scale quantum information processing. Photonic systems in particular provide a reliable and rapid test bed for emerging quantum technologies with excellent prospects for scalability [6].

In this work we report the first experimental demonstration of a one-way based implementation of the quantum algorithm solving Simon's Problem (SP) [5]. This is a period-finding problem of great importance in quantum algorithm design as it provides a clear exponential gap between the classical and quantum runtime. It was a motivation for Shor's factoring algorithm [4] and has played a major role in the evolution of quantum algorithm design [7]. Here, we exploit the one-way model to experimentally demonstrate SP using a multipartite entangled state, the cluster state, as a resource for running a program represented by single-qubit measurements [8–10]. This measurement-based approach is appealing as it reduces the amount of control one needs over a quantum system to the ability of carrying out measurements only, an important advantage for a number of physical settings, most notably those using ion-traps [11, 12] and photons [13–17]. The one-way model thus continues to generate much interest, both at a theoretical [18, 19] and experimental [12–17] level. The algorithm we experimentally demonstrate for SP illustrates the unique role that parallelism in QC plays in the speed-up given by quantum algorithms solving classical decision problems. Despite being one of the first quantum algorithms introduced and the first to show that an exponential gap can exist in the runtime between solving problems classically and quantum mechanically, the quantum algorithm for SP has surprisingly never been experimentally demonstrated before. One of the main reasons behind this may be due to the complexity of the quantum circuitry required, even for the smallest instance of the algorithm [5]. Here we show that a measurement-based approach, due to its great flexibilty, finally enables the realization of the algorithm using current technology. Thus, to the best of our knowledge, our work not only represents the first implementation of the algorithm in the promising context of one-way QC, but also the algorithm's first experimental realization in any physical system.

In our experiment we show that five qubits in a specific cluster state configuration are sufficient to realize key representative functions of the problem's black box acting on a logical four-qubit register; two query and two ancilla qubits. A complex modification to the experimental setup for each function is not necessary, only a small change to the program of measurements, an important advantage over other QC techniques. Our experimental results are in excellent agreement with the theoretical model, demonstrating successful performance of the algorithm in a photonic setting. As photonic technology is a highly promising platform for realizing quantum computing, our demonstration is of great significance for helping open up a practical route to probing larger and more complex quantum algorithms. Along these lines, we also discuss extending our scheme to implement all black box functions for the two-qubit version, not just representatives, in addition to arbitrary sized registers and the resources required.

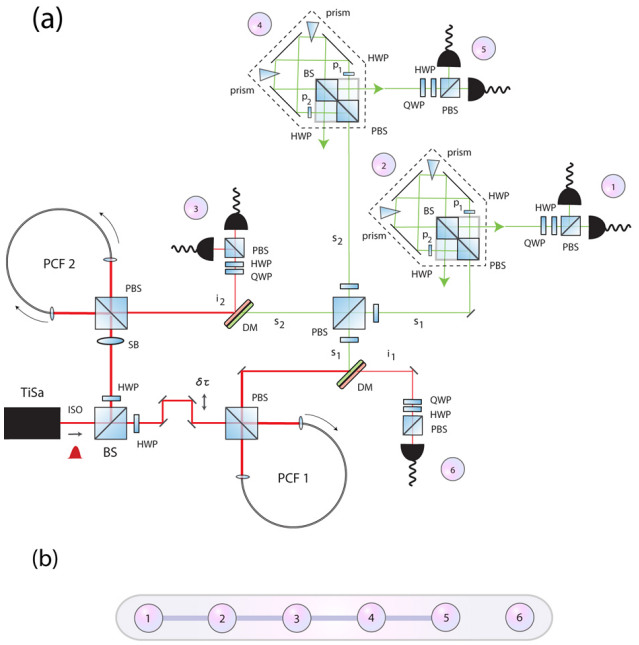

FIG. 1: Experimental setup. **(a):** Two photonic crystal fibres produce photon pairs which are fused using a polarizing beamsplitter (PBS) to generate the five-qubit entangled cluster state plus additional qubit 6 shown in (b). The cluster state consists of three polarization qubits, 1, 3 and 5 (s_1, i_2 and s_2). The paths of photons s_1 and s_2 represent qubits 2 and 4 respectively. The algorithm is executed by measuring the path qubits in the Z or Y bases depending on the oracle's black box using a Sagnac configuration (dashed regions). The output of the algorithm resides on qubits 1 and 5, and is obtained via polarization measurements. The setup is based on one recently used to generate a quantum error correction graph code [22], the main differences here being the use of an additional photon (qubit 6) and the waveplate configuration used to generate the different entangled resource. **(b):** Cluster state generated by the setup. Edges correspond to controlled-phase operations, $CZ = \mathrm{diag}\{1, 1, 1, -1\}$, applied to qubits (the vertices) initialized in the state $|+\rangle$.

Thus, we show that one-way quantum computing provides a flexible and practical route to experimentally investigating the quantum-classical interface in the query complexity model.

Model.- The problem considers an oracle that implements a function mapping an n-bit string to an m-bit string $f : \{0,1\}^n \rightarrow \{0,1\}^m$, with $m \geq n$, where it is promised that f is a $1-1$ type function (each input gives a different output) or $2-1$ type function (two inputs give the same output) with non-zero period $s \in \{0,1\}^n$ such that for all $x \neq x'$ we have $f(x) = f(x')$ if and only if $x' = x \oplus s$, where $\oplus$ corresponds to addition modulo 2. The problem is to determine the type of the function f and if it is $2-1$, to determine the period s. Using classical query methods the probability of solving the problem is given by $p_s \leq 1/2 + \delta$, with $\delta = 2^{-n/2}$ if one queries the oracle at least $2^{n/4}$ times. As $n \rightarrow \infty$, $\delta \rightarrow 0$ and the number of queries needed to obtain $p_s > 1/2$ grows exponentially. Quantum mechanically, the number of queries needed is $O(n)$ to solve the problem with $p_s = 1$ [5].

The quantum algorithm used to solve SP considers the oracle as a black box (BB) implementing the following operation $U : |x\rangle|z\rangle \mapsto |x\rangle|z \oplus f(x)\rangle$, with $|x\rangle$ the query register and $|z\rangle$ an ancilla. The oracle is queried with a superposition of all inputs $|x\rangle$, and the ancilla state is $|0\rangle^{\otimes m}$ (where $\{|0\rangle, |1\rangle\}$ is the qubit computational basis):$2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle^{\otimes m}$, which it transforms into $2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle = 2^{-n/2}(|x_0\rangle + |x_0 \oplus s\rangle)|f(x_0)\rangle + 2^{-n/2}(|x_1\rangle + |x_1 \oplus s\rangle)|f(x_1)\rangle + \ldots$.

Hadamard rotations $H = (X + Z)/\sqrt{2}$ are then applied to the oracle's output query qubits (X, Y and Z are the Pauli matrices). Taking the first term as an example we have $(|x_0\rangle + |x_0 \oplus s\rangle) \rightarrow \sum_{y=0}^{2^n-1}[(-1)^{x_o \cdot y} + (-1)^{(x_o \oplus s)\cdot y}]|y\rangle$, where $\cdot$ is the bitwise inner product. Using the relation $(x_0 \oplus s)\cdot y = (x_0 \cdot y) \oplus (s \cdot y)$ we have that all terms with $(s \cdot y) = 1$ interfere and cancel, leaving terms with $(s \cdot y) = 0$ only. This cancellation occurs for the remaining terms involving $x_1, x_2, \ldots x_{2^n-1}$. Thus measuring the query qubits gives a state $|y\rangle$ where $s \cdot y = 0$. By running the algorithm until $n-1$ linearly independent binary vectors y_i are obtained (which occurs with $p_s \geq 1/4$ for $\geq n$ repetitions [5]) one can solve the list of $s \cdot y_i$'s to obtain s, in the case f is $2-1$. If f is $1-1$, a uniform distribution is found for the y_i outcomes.

Experimental implementation.- The setup we use to demonstrate the algorithm is shown in Fig. 1 (a). Recently part of this setup was used to demonstrate a quantum error correction code using a 2D graph state [22]. Here, the setup has been modified using a number of additional components in order to generate a different multipartite entangled state, a linear 1D cluster state. Using this different entangled state we are then able to demonstrate the quantum algorithm for SP. The ability to carry out a range of different protocols using cluster and graph states in this context shows their great flexibility for quantum information processing tasks [19].

In the setup a Ti:Sapphire laser emits 8nm pulses at a wavelength of 724.5 nm with a repetition rate of 80 MHz, which are filtered to 1 nm. The pulses are split at a 50:50 beamsplitter and used to pump two birefringent photonic crystal fibre (PCF) sources. After filtering, attenuation, and coupling into the fibres, approximately 6mW/9mW is used to pump the first/second source. The PCF sources produce correlated pairs of photons via spontaneous four-wave mixing (FWM) at a signal and idler wavelength of 626 nm and 860 nm respectively [20]. Here, the advantages of using FWM in a PCF to generate correlated photons compared to spontaneous parametric down-conversion in bulk crystals, such as BBO, include the ability to achieve pure state phase-matching [21], as well as improved collection efficiencies and a lower pump power requirement [20]. Each source is in a Sagnac loop around a polarizing beamsplitter (PBS). In the first source the polarization of the pump is set to horizontal by a half-wave plate (HWP) and produces the state $|H\rangle_{i_1}|H\rangle_{s_1}$ [21]. The photon pairs are separated into different paths using a dichroic mirror (DM) and the signal polarization is rotated to $|+\rangle$ using a HWP, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$. The detected rate of photon pairs in the state $|H\rangle_{i_1}|+\rangle_{s_1}$ is $\sim 9,000$ per second, and the measured lumped efficiencies for the signal and idler paths are $\sim 8\%$ and $\sim 12\%$ respectively. The second PCF is

pumped with diagonal polarization which produces the state $\frac{1}{\sqrt{2}}(|H\rangle|H\rangle + e^{i\theta}|V\rangle|V\rangle)_{i_2 s_2}$ [20]. A Soleil Babinet birefringent compensator (SB) placed before the loop is used to set the phase $\theta = 0$, so that the Bell state $|\phi^+\rangle$ is produced. A DM separates the two wavelengths. The detected rate of photon pairs in this state is also ∼9,000 per second and the fidelity with respect to the ideal state is ∼0.88. When both PCFs simultaneously produce a photon pair, the combined state is $|H\rangle_{i_1}|+\rangle_{s_1}\frac{1}{\sqrt{2}}(|H\rangle_{i_2}|H\rangle_{s_2} + |V\rangle_{i_2}|V\rangle_{s_2})$. A tunable filter window set to 4 nm bandwidth at 860 nm is applied to the idlers. The idler modes are collected into single-mode fibres and used with coincidence detections at the signal modes to trigger the event in which four photons are generated.

The signal photons from each PCF are then fused using a PBS to make the three-photon linear cluster state $\frac{1}{\sqrt{2}}(|+H+\rangle + |-V-\rangle)_{s_1 i_2 s_2}$ [22]. Here, the signal photons pass through 40 nm bandwidth filters. These filters are used only to remove any remaining light coming from the bright pump beam, as the intrinsically pure state phase-matching from the FWM process ensures that narrow filtering is unnecessary for the signal photons, which have a bandwidth of 0.3 nm [21]. Further details about the spectrum of the signal and idler photons can be found in Refs. [20, 21]. The coherence length of the signal photons interfering is 1 mm [22]. After the PBS part of the fusion, HWPs set at 45° apply Hadamard rotations to the polarization states of the signal photons. The remaining idler photon i_1 is used as an additional qubit in the algorithm. Both signal photons are expanded into two qubits via a Sagnac configuration [17] (dashed boxes in Fig. 1 (a)). For the signal mode s_1, a PBS applies the transformations $|H\rangle_{s_1} \rightarrow |H\rangle_{s_1}|p_1\rangle_{s_1}$ and $|V\rangle_{s_1} \rightarrow |V\rangle_{s_1}|p_2\rangle_{s_1}$, where $|p_{1(2)}\rangle_{s_1}$ corresponds to the photon in path 1 (2). HWPs set at 45° then apply Hadamard rotations to the polarization states in modes p_1 and p_2 to give $|+\rangle_{s_1}|p_1\rangle_{s_1}$ and $|-\rangle_{s_1}|p_2\rangle_{s_1}$ respectively. Applying the same transformations to s_2 we have

$$|\psi_\ell\rangle = \frac{1}{2\sqrt{2}}[(|+\rangle|0\rangle + |-\rangle|1\rangle)|0\rangle(|0\rangle|+\rangle + |1\rangle|-\rangle) + (|+\rangle|0\rangle - |-\rangle|1\rangle)|1\rangle(|0\rangle|+\rangle - |1\rangle|-\rangle)]_{12345}|+\rangle_6 \quad (1)$$

where the polarization of photon s_1 represents qubit 1 ($|0/1\rangle \leftrightarrow |H/V\rangle$) and its path is qubit 2 ($|0/1\rangle \leftrightarrow |p_1/p_2\rangle$), and similarly for photon s_2, whose polarization represents qubit 5 and its path is qubit 4. The polarization of photon $i_{1(2)}$ is qubit 6 (3). The Hadamard basis $|+/-\rangle \leftrightarrow |H/V\rangle$ is used for qubit 6. The state $|\psi_\ell\rangle$ is a five-qubit linear cluster state with an additional qubit, $|\psi_\ell\rangle = |\phi_C\rangle_{12345}|+\rangle_6$, as shown in Fig. 1 (b). The state is generated with a rate of ∼0.25 per second.

To measure the polarization qubits for the algorithm, each mode contains an analysis section made up of a quarter waveplate (QWP), HWP and PBS, allowing measurements in the X, Y, and Z bases [23]. For the path qubits, Z measurements are performed by blocking path p_1 or p_2 before the beamsplitter and measuring the relative populations [17]. For X measurements, the paths are combined at the beamsplitter, which applies the transformation $|p_1\rangle \rightarrow |+\rangle$ and $|p_2\rangle \rightarrow |-\rangle$, with the output ports giving the relative populations. Instead of monitoring both output ports we modify the phase of one path relative to the other in order to swap the relative populations [17]. This allows measurements in the Y basis also. For detecting the photons we use avalanche photodiodes and a coincidence counter monitors the 8 possible four-fold detections corresponding to one photon in each mode [24].

Before carrying out one-way QC on the cluster state, we characterize it, checking for the presence of genuine multipartite entanglement (GME) to ensure all photons are involved in the state generation. To do this, we measure the expectation value of the two setting witness, $\mathcal{W}_2$ [25], which if negative detects the presence of GME. The witness is evaluated using the local measurements $XZXZX$ and $ZXZXZ$, and we find $\langle\mathcal{W}_2\rangle = -0.12 \pm 0.02$, clearly showing the presence of GME. The error has been calculated using maximum likelihood estimation and a Monte Carlo method with Poissonian noise on the count statistics, which is the dominant source of error in our photonic experiment [23]. We also obtain the fidelity of the experimental cluster state with respect to the ideal state using seventeen measurement bases [27] and find a fidelity of $F = 0.70 \pm 0.01$.

With the cluster state characterized we implement the quantum algorithm. The action of the oracle is known as a promise problem [2]. In order to implement all the configurations that it might perform in an $n = m = 2$ version of SP (SP_{22}), we must be able to construct them using a combination of quantum gates. There are a total of fifteen different oracle black boxes (BBs) for SP_{22} [27]. However, in order to demonstrate the speedup achieved by the quantum algorithm it is not necessary to implement all BBs: the gap between the number of classical and quantum queries required to solve the problem is small for low n and for $n = 2$ there is no speedup if $1-1$ functions are included. SP stills applies to the case with only $2-1$ functions and a speedup exists for all $n \geq 2$ [5]. In Fig. 2 (c), (d) and (e), we identify three BBs for f as $2-1$ in terms of their equivalent quantum network, covering all periods $s = 01$, 10 and 11 respectively. In order to carry out the algorithm using the necessary logic quantum gates, the five-qubit cluster state shown in Fig. 2 **(a)** is 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 program.

For cluster states, two types of measurements allow one-way QC to be performed: (i) Measuring a qubit j in the computational basis allows it to be disentangled and removed from the cluster, leaving a smaller cluster of the remaining qubits, and (ii) In order to perform QC, qubits must be measured in the equatorial basis $B_j(\alpha) = \{|\alpha_+\rangle_j, |\alpha_-\rangle_j\}$, where $|\alpha_\pm\rangle_j = (|0\rangle \pm e^{i\alpha}|1\rangle)_j/\sqrt{2}$ ($\alpha \in \mathbb{R}$). Choosing the basis determines the rotation $R_z(\alpha) = \exp(-i\alpha\sigma_z/2)$, which is followed by a Hadamard operation being simulated on a logical qubit in the cluster residing on qubit j [28]. Using the cluster state generated, the input states corresponding to $|x\rangle = |x_1\rangle|x_2\rangle = |+\rangle|+\rangle$ are naturally encoded on qubits 1 and 5. The states $|z_1\rangle|z_2\rangle = |0\rangle|0\rangle$ are encoded on qubits 3 and 6, with the Hadamard operations from the BBs automatically ap-

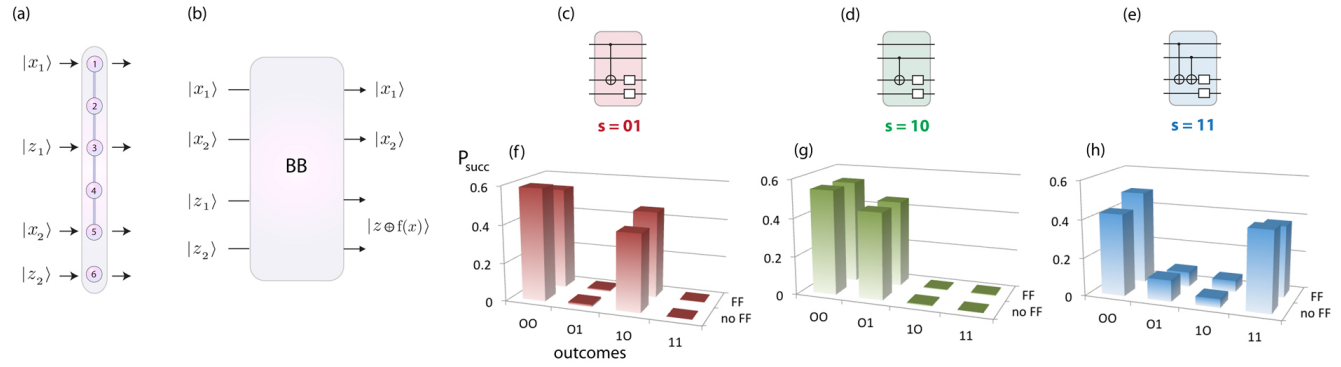

FIG. 2: Black box (BB) circuit diagrams for SP_{22} and experimental results. **(a):** The cluster state resource used with additional qubit 6. **(b):** General scenario for the oracle's BB, showing the inputs and outputs (reordered). **(c)-(e):** Circuits corresponding to $2-1$ functions with $s = 01$, 10 and 11 (the symbol $\square$ corresponds to either a $\mathbb{1}$ or X operation). See Tab. I for values of $f(x)$ in each of these cases. **(f)-(h):** Success probabilities measured in our experiment. Ideally the probabilities are equally split between outcomes $y_i = 00$ and 10 for $s = 01$ (panel (f)), 00 and 01 for $s = 10$ (panel (g)), and 00 and 11 for $s = 11$ (panel (h)).

plied before a particular measurement program begins. Thus, the state $|x_1\rangle|z_1\rangle|x_2\rangle|z_2\rangle \equiv |+\rangle(H|0\rangle)|+\rangle(H|0\rangle)$ resides on the logical input register of the resource $|\psi_\ell\rangle$. Qubits 2 and 4 play a pivotal role for the oracle by allowing it to apply (or not apply) two-qubit gates between the logical input states $|x_1\rangle$ and $|z_1\rangle$, and $|x_2\rangle$ and $|z_1\rangle$. For each BB, measuring a qubit in the computational basis prevents any two-qubit gate from being applied between its neighboring qubits. For example, in the BB of Fig. 2 (c), the oracle can measure qubit 4 in the computational basis, removing it from the cluster and leaving it with the ability to perform only a two-qubit gate between $|x_1\rangle$ and $|z_1\rangle$. When the oracle measures qubit 2 in $B(\pi/2)$ this enables it to apply the gate $(R_z(\pi/2)\otimes R_z(\pi/2))\mathsf{CZ}$ between $|x_1\rangle$ and $|z_1\rangle$ [29], where $\mathsf{CZ} = \mathrm{diag}(1,1,1,-1)$. This gives the computation $|x_1\rangle|z_1\rangle|x_2\rangle|z_2\rangle \rightarrow [R_z(\pi/2)\otimes R_z(\pi/2)\otimes\mathbb{1}\otimes\mathbb{1}][\mathsf{CZ}\otimes\mathbb{1}\otimes\mathbb{1}][\mathbb{1}\otimes H\otimes\mathbb{1}\otimes H]|+\rangle|0\rangle|+\rangle|0\rangle \equiv \mathsf{CNOT}\otimes\mathbb{1}\otimes\mathbb{1}|+\rangle|0\rangle|+\rangle|0\rangle$, up to local rotations $[R_z(-\pi/2)\otimes H\, R_z(-\pi/2)\otimes\mathbb{1}\otimes H]_{1356}$ incorporated into a 'feed-forward' (FF) stage. These FF rotations are realised in the experiment by modifying the basis of the measurements of the corresponding qubits - a standard procedure in one-way QC where a local unitary operation before a measurement is equivalent to a basis change of the measurement itself [13]. The above combination of logic gates and FF corresponds to the required circuit for the BB of Fig. 2 (c). For measurement outcomes $s_2 = s_4 = 0$ the final state (with FF applied) is

$$\left|\psi'_\ell\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|-\rangle_3 + |1\rangle_1|+\rangle_3\right)|0\rangle_5|0\rangle_6\,, \qquad (2)$$

which gives the outcomes for the query qubits (when measured in the computational basis) of $y_i = s_1 s_5$ equal to 00 or 10, as expected. For the other measurement outcomes of qubits 2 and 4 one applies FF operations to qubits 1 and 5 given in Table 1 by incorporating them into the measurement basis. Full details of the evolution of the cluster state resource during these steps can be found in Ref. [27].

The same basic rules can be applied for all the BBs. Table I provides the measurement programs for each BB. Here, the final Hadamards for the query qubits after the BB's (before they are measured) are also added to the FF stage, allowing the algorithm for SP_{22} to be implemented. The measurements and outcomes of qubits 1, 3, 5 and 6 constitute the algorithm (only query qubits 1 and 5 need to be measured to obtain y_i). Additions to the FF stages, and measurements of qubits 2 and 4 are viewed as being carried out by the oracle [14].

$f(x)$	$s = 01$	$s = 10$	$s = 11$
$f(00)$	00	00	00
$f(01)$	00	10	10
$f(10)$	10	00	10
$f(11)$	10	10	00
$\mathcal{M}_2$	$B(\pi/2)$	$\|0/1\rangle$	$B(\pi/2)$
$\mathcal{M}_4$	$\|0/1\rangle$	$B(\pi/2)$	$B(\pi/2)$
FF_1	X^{20}	ζ^{20}	X^{20}
FF_3	X^{24}	X^{24}	$\tilde{X}^{24}$
FF_5	ζ^{04}	X^{04}	X^{04}
FF_6	H	H	H

TABLE I: BB function outputs $f(x)$ for SP_{22} (rows 1-4, the y_i outputs from the quantum algorithm are given later in the main text), measurement program $\mathcal{M}_i$ for qubit i of the cluster state $|\phi_C\rangle$ (rows 5,6) and FF operations (rows 7-10) for each period s. The notation $|0/1\rangle$ corresponds to a measurement in the computational basis with $X^{ij} = X^{s_i+s_j}HR_z(-\pi/2)$, $\tilde{X}^{ij} = X^{s_i+s_j}HR_z(-\pi)$ and $\zeta^{ij} = HX^{s_i+s_j}$. Here, s_k is the measurement outcome of qubit k (with $s_0 = 0$). For each period, s, there are an additional three function outputs, obtained by applying the combination $\mathbb{1}\otimes X$, $X\otimes\mathbb{1}$ and $X\otimes X$ to ancilla qubits z_1 and z_2 (see $\square$'s in Fig. 2).

The results of the experiment are shown in Fig. 2 (f)-(h), where we display the average success probability of obtaining the different logic outcomes of the query qubits for each BB function shown in (c)-(e). For the BB with $s = 01$, the success probabilty should be split equally between $y_i = 00$ and $y_i = 10$, as $s\cdot y_i = 0$ and $\cdot$ is the bitwise inner product. We find $p_{00} = 0.54 \pm 0.02$ and $p_{10} = 0.45 \pm 0.02$ as shown in Fig. 2 (f). For the BB with $s = 10$ ($s = 11$), the success probabilty should

be split equally between $y_i = 00$ and $y_i = 01$ ($y_i = 11$) as $s\cdot 00 = s\cdot 01 = 0$ ($s\cdot 00 = s\cdot 11 = 0$). We find $p_{00} = 0.54 \pm 0.02$ and $p_{01} = 0.45 \pm 0.01$ ($p_{00} = 0.49 \pm 0.02$ and $p_{11} = 0.37 \pm 0.01$) as shown in Fig. 2 (g) ((h)). In Fig. 2 (f)-(h) we include the no-FF ($s_i = 0\ \forall i$) and FF cases for the algorithm [30]. Note that we have repeated the algorithm a number of times to obtain the success probabilities. However, on average only ~ 2 runs are sufficient in order to obtain an outcome other than 00. This is in contrast to the classical scenario which requires on average 8/3 runs to determine the period [27]. While this gap between the quantum and classical runtime is small in the two-qubit version, it scales exponentially with the size of the input register. Our results provide the first experimental evidence of the existence of this gap. We have briefly analyzed the resources required for demonstrating n-qubit versions of the algorithm for SP and found that the minimal graph state for performing SP_{nn} contains n^2+n+1 qubits and $2n^2-2n+2$ edges. This resource scales polynomially with n [27]. The six-qubit resource used here for SP_{22} is a special case excluding $1-1$ functions.

Remarks.- We have reported the first experimental realization of a two-qubit version of the algorithm for Simon's Problem, a black box problem, showing the first hint of an exponential gap existing between the classical and quantum runtime. The agreement between the experimental data and theory is excellent and limited only by the overall quality of the resource. The experiment has been performed in a photonic system, which due to the strong potential of using photonics for advanced quantum information processing, makes our scheme ideal for future probing of the boundary between classical and quantum efficiency in computing algorithms. Subsequent work on applying the techniques described here to other quantum algorithms may further stimulate one-way QC with minimal resources and their expansion to full-scale quantum information processing.

Acknowledgments.- We thank M. Paternostro for helpful discussions, and support from EU project 600838 QWAD and ERC grant 247462 QUOWSS.

* Electronic address: markstame@gmail.com

[1] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (2000).
[3] T. D. Ladd *et al.*, Nature **464**, 45 (2010).
[4] D. Deutsch, Proc. Roy. Soc. Lond. **A 400**, 97 (1985); D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. **A 439**, 553 (1992); P. Shor, SIAM J. Comput. **26**, 1484 (1997); L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[5] D. R. Simon, Proc. 35th IEEE Symp. Found. Comp. Sci., Santa Fe, NM, 116-123 (1994); D. R. Simon, SIAM J. Comp. **26**, 1474 (1994).
[6] J. L. O'Brien, A. Furusawa and J. Vuckovic, Nat. Phot. **3**, 687 (2009).
[7] A. M. Childs and W. van Dam, Rev. Mod. Phys. **82**, 1 (2010).
[8] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[9] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[10] B. A Bell *et al.*, New J. Phys. **15**, 053030 (2013).
[11] R. Stock and D. F. V. James, Phys. Rev. Lett. **102**, 170501 (2009).
[12] B. P. Lanyon *et al.*, Phys. Rev. Lett. **111**, 210501 (2013).
[13] P. Walther, *et al.*, Nature **434**, 169 (2005); R. Prevedel, *et al.*, Nature **445**, 65 (2007).
[14] M. S. Tame *et al.*, Phys. Rev. Lett. **98**, 140501 (2007).
[15] G. Vallone *et al.*, Phys. Rev. A **81**, 050302(R) (2010).
[16] S. M. Lee *et al.*, Opt. Exp., **20**, 6915 (2012).
[17] W.-B. Gao *et al.*, Nature Physics **6**, 331 (2010).
[18] D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007); D. Gross *et al.*, Phys. Rev. A **76**, 052315 (2007).
[19] H. J. Briegel *et al.*, Nat. Phys. **5**, 19 (2009).
[20] J. Fulconis *et al.*, Phys. Rev. Lett. **99**, 120501 (2007).
[21] M. Halder *et al.*, Opt. Exp. **17**, 4670 (2009).
[22] B. Bell *et al.* Nature Comm. **5**, 3658 (2014).
[23] D. F. V. James, P. G. Kwiat, W. J. Munro and A. G. White, Phys. Rev. A **64**, 052312 (2001).
[24] Coincidence counter from http://www.qumetec.com.
[25] The witness $\mathcal{W}_2 = 9/4 - \frac{1}{4}(X\mathbb{1}X\mathbb{1}X + X\mathbb{1}XZ\mathbb{1} + XZXZX + XZ\mathbb{1}\mathbb{1}\mathbb{1} + \mathbb{1}ZX\mathbb{1}X + \mathbb{1}ZXZ\mathbb{1} + \mathbb{1}\mathbb{1}\mathbb{1}ZX) - \frac{1}{2}(ZXZXZ + ZXZ\mathbb{1}\mathbb{1} + \mathbb{1}\mathbb{1}ZXZ)$. See Ref. [26].
[26] G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005).
[27] See supplementary information.
[28] For a detailed introduction to one-way QC, see [9, 13].
[29] M. S. Tame and M. S. Kim, Phys. Rev. A **82**, 030305(R) (2010).
[30] In the case of FF, based on the measurement outcomes of the qubits, the query outcomes have bit flips applied (see Tab. I) in order to retrieve the correct values.