

PAPER • OPEN ACCESS

## Exchange-free computation on an unknown qubit at a distance

To cite this article: Hatim Salih *et al* 2021 *New J. Phys.* **23** 013004

View the [article online](#) for updates and enhancements.





You may also like

- [Preparation of optimal entropy squeezing state of atomic qubit inside the cavity via two-photon process and manipulation of atomic qubit outside the cavity](#)  
Bing-Ju Zhou, , Zhao-Hui Peng et al.
- [Entanglement Preserving in Quantum Copying of Three-Qubit Entangled State](#)  
Tong Zhao-Yang and Kuang Le-Man
- [NMR imaging analogue of the individual qubit operations in superconducting flux-qubit chains](#)  
Toshiyuki Fujii, Shigemasa Matsuo and Noriyuki Hatakenaka



## PAPER

## Exchange-free computation on an unknown qubit at a distance

Hatim Salih<sup>1,2,\*</sup> , Jonte R Hance<sup>1</sup> , Will McCutcheon<sup>1,3</sup> , Terry Rudolph<sup>4</sup> and John Rarity<sup>1</sup> <sup>1</sup> Quantum Engineering Technology Laboratory, Department of Electrical and Electronic Engineering, University of Bristol, Woodland Road, Bristol BS8 1UB, United Kingdom<sup>2</sup> Quantum Technology Enterprise Centre, HH Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom<sup>3</sup> Institute of Photonics and Quantum Science, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom<sup>4</sup> Department of Physics, Imperial College London, Prince Consort Road, London SW7 2AZ, United Kingdom

\* Author to whom any correspondence should be addressed.

E-mail: [salih.hatim@gmail.com](mailto:salih.hatim@gmail.com)**Keywords:** counterfactual communication, quantum computation, quantum information, quantum algorithmsRECEIVED  
4 October 2020REVISED  
5 December 2020ACCEPTED FOR PUBLICATION  
15 December 2020PUBLISHED  
19 January 2021Original content from  
this work may be used  
under the terms of the  
[Creative Commons  
Attribution 4.0 licence](https://creativecommons.org/licenses/by/4.0/).Any further distribution  
of this work must  
maintain attribution to  
the author(s) and the  
title of the work, journal  
citation and DOI.

### Abstract

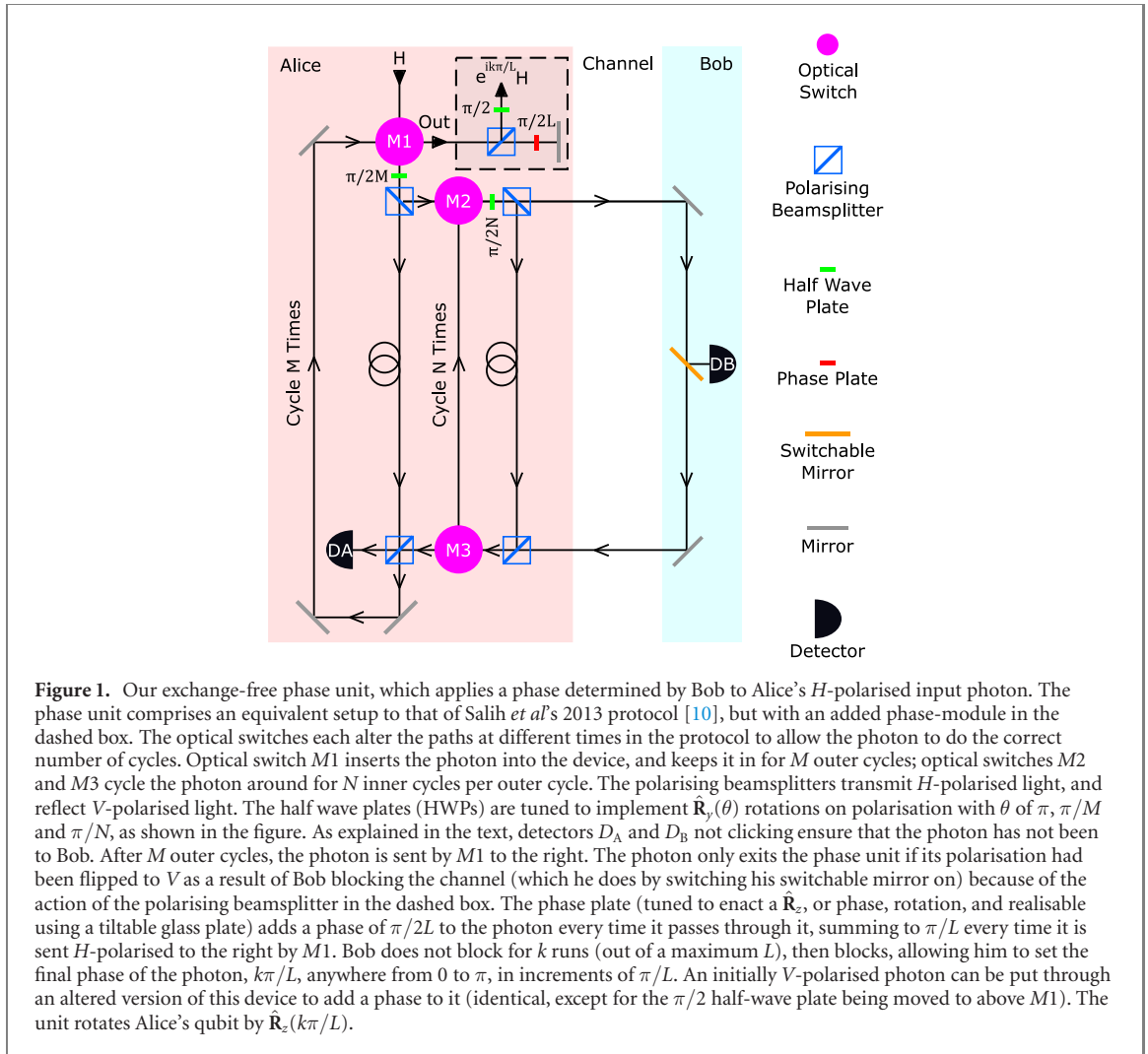
We present a way of directly manipulating an arbitrary qubit, without the exchange of any particles. This includes as an application the exchange-free preparation of an arbitrary quantum state at Alice by a remote classical Bob. As a result, we are able to propose a protocol that allows one party to directly enact, by means of a suitable program, any computation exchange-free on a remote second party's unknown qubit. Further, we show how to use this for the exchange-free control of a universal two-qubit gate, thus opening the possibility of directly enacting any desired algorithm remotely on a programmable quantum circuit.

Quantum physics opens up the surprising possibility of obtaining knowledge from, or through, places where no information-carrying particles have been. This was first proposed and subsequently demonstrated experimentally in the context of computing [1, 2], where the result of a computation is learnt based on the phenomena of interaction-free measurement and the Zeno effect [3–7]. More specifically, without any photons entering or leaving an optical circuit, the result of a computation is obtained without the computer ever ‘running’.

Just as intriguing was the proposal and subsequent experimental demonstration of a simple quantum scheme for allowing two remote parties to share a cryptographic random bit-string, without exchanging any information-carrying particles [8, 9]. The fact that the protocol had limited maximum-efficiency was not a serious drawback for its purpose since the shared information was random, meaning failed attempts could simply be discarded in the end. This, however, begged the question whether efficient, deterministic communication was possible exchange-free, that is without particles crossing the communication channel.

In 2013, building on the ideas above, Salih *et al* devised a scheme allowing two remote parties to efficiently and deterministically share a message exchange-free, in the limit of a large number of protocol cycles and ideal practical implementation [10]. The protocol was recently demonstrated experimentally by Pan and colleagues [11]. Importantly, the previously-heated debate over whether the laws of physics even allow such communication (for both bit values) seems to be settling; nature does allow exchange-free communication (and therefore computation) [12–18].

We present in what follows a protocol allowing a remote Bob to prepare any qubit he wishes at Alice without any particles passing between them, thus exchange-free. This is different from counterfactually sending a quantum state from Bob to Alice by means of counterportation [19, 20], in that Bob does not need to prepare a quantum object at his end (a quantum superposition of blocking and not blocking the optical communication channel) thus making the scheme much easier to implement. More generally, Bob can directly apply any arbitrary Bloch-sphere rotation to an unknown qubit at Alice—in other words, any single-qubit quantum computation. Note that we use ‘exchange-free’ and ‘counterfactual’ interchangeably.



While we describe an optical realisation using photon polarisation, the scheme is in principle applicable to other physical implementations—and helps advance quantum information science.

Our protocol consists of a number of nested outer interferometers, each containing a number of inner interferometers, as in Salih *et al*'s 2013 protocol [10]. We combine these interferometers into a device that we call a phase unit, allowing Bob to apply a relative phase to Alice's photonic qubit (figure 1). We pair two phase units such that one applies some phase to Alice's  $H$ -polarised component, while the other applies an equal but opposite-sign phase to her  $V$ -polarised component, resulting in a  $\hat{R}_z(\theta)$  rotator. By chaining three such  $\hat{R}_z(\theta)$  rotators, interspersed with appropriate wave-plates, Bob can apply any arbitrary unitary to Alice's qubit, exchange-free (figure 2).

Note, we define the Bloch sphere for polarisation such that the poles are  $|H\rangle$  and  $|V\rangle$ , and the rotations are

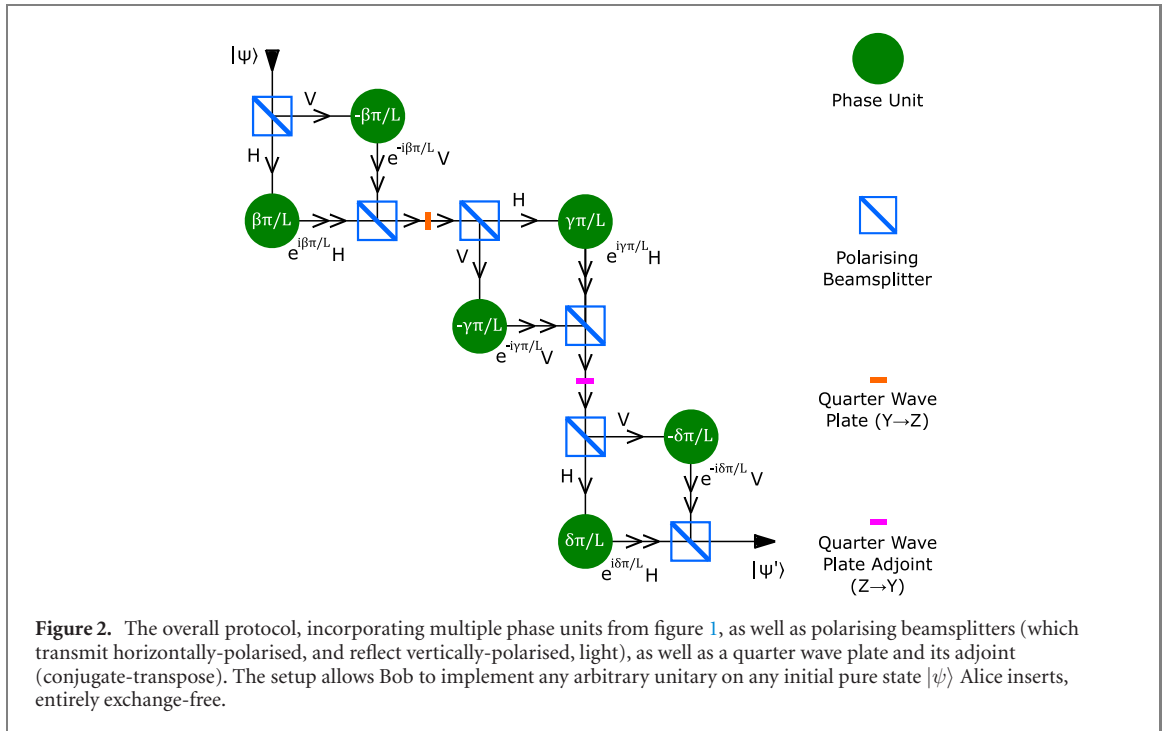
$$\hat{R}_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i \sin\left(\frac{\theta}{2}\right) \\ i \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} = e^{-i\theta\hat{\sigma}_x/2} \quad (1)$$

$$\hat{R}_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} = e^{-i\theta\hat{\sigma}_y/2} \quad (2)$$

$$\hat{R}_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = e^{-i\theta\hat{\sigma}_z/2} \quad (3)$$

for dummy variable  $\theta$ , and Pauli matrices  $\hat{\sigma}_{x,y,z}$ .

We first go through Salih *et al*'s 2013 protocol. However, we describe the protocol, following [20], without any reference to either interaction-free measurement or the Zeno effect of [3, 6]. In order to do



this, we think of our detectors as being placed far enough, such that they perform no measurement before the photon had had time to exit the protocol. Any photonic component travelling towards either detector can thus be thought of as entering a loss mode, meaning that if the photon exits the protocol successfully then it cannot have taken the path towards that detector, and the detector will subsequently not register a click.

To start with, a photon of state  $a|H\rangle + b|V\rangle$  enters the outer interferometer through a HWP tuned to apply a  $\hat{R}_y(\pi/M)$  rotation. The photon then enters a polarising beam splitter (PBS), which transmits horizontal polarisation, but reflects vertical polarisation.

The  $V$ -polarised component circles through a series of  $N$  inner interferometers, where, in each, it goes through a HWP tuned to apply a  $\hat{R}_y(\pi/N)$  rotation, then through another PBS. The  $H$ -polarised component from this PBS passes across the channel, from Alice to Bob, who can choose to block or not block, by switching on or off his switchable mirror. If he blocks, this  $H$ -polarised component goes into a loss mode towards detector  $D_B$ ; if not, it returns to Alice's side, recombines at another PBS with the  $V$ -polarised component, then enters the next inner interferometer. After the chain of  $N$  inner interferometers, the resulting components are then passed through one final PBS, sending any  $H$ -polarised component that has been to Bob into a loss mode towards detector  $D_A$ , before being recombined at another PBS with the  $H$ -polarised component from the arm of the outer interferometer. Importantly, neither detector clicking, ensures that the photon has not been to Bob.

As each inner interferometer applies  $\hat{R}_y(\pi/N)$ , if Bob does not block, the rotations sum to

$$\hat{U}_{NB}^N = (e^{-i\pi\hat{\sigma}_y/2N})^N = e^{-i\pi\hat{\sigma}_y/2} = \hat{R}_y(\pi). \quad (4)$$

Therefore, the state after the inner interferometer chain is

$$|V\rangle_I \rightarrow \hat{U}_{NB}^N |V\rangle_I = |H\rangle_I \rightarrow \text{Loss}. \quad (5)$$

This means the  $V$ -polarised component becomes  $H$ -polarised, entering the loss mode towards detector  $D_A$  after the final PBS, meaning the only component of the wavefunction exiting the outer interferometer is the  $H$ -polarised one that went via the outer arm.

Similarly, if Bob blocks for all inner interferometers,

$$\begin{aligned} \hat{A}_B^N &= \left[ e^{-i\pi\hat{\sigma}_y/2N} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right]^N \\ &= \begin{pmatrix} \cos\left(\frac{\pi}{2N}\right)^N & 0 \\ \cos\left(\frac{\pi}{2N}\right)^{N-1} \sin\left(\frac{\pi}{2N}\right) & 0 \end{pmatrix}. \end{aligned} \quad (6)$$

Therefore, the state after an outer interferometer is

$$\begin{aligned} |V\rangle_I &\rightarrow \hat{\mathbf{A}}_B^N |V\rangle_I \\ &= \cos\left(\frac{\pi}{2N}\right)^N |V\rangle_I + \cos\left(\frac{\pi}{2N}\right)^{N-1} \sin\left(\frac{\pi}{2N}\right) |H\rangle_I \\ &\rightarrow \cos\left(\frac{\pi}{2N}\right)^N |V\rangle + \text{Loss} \end{aligned} \quad (7)$$

meaning some  $V$ -polarised component exits the outer interferometer.

If Bob, does not block, the outer cycle applies

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} e^{-i\pi\hat{\sigma}_y/2M} \quad (8)$$

If he does block, the outer cycle applies

$$\begin{pmatrix} 1 & 0 \\ 0 & \cos\left(\frac{\pi}{2N}\right)^N \end{pmatrix} e^{-i\pi\hat{\sigma}_y/2M}. \quad (9)$$

We repeat this  $M$  times, starting with a  $H$ -polarised photon, and using a final PBS to split it into  $H$ - and  $V$ -polarised components.

As Alice applies a  $\hat{\mathbf{R}}_y(\pi/M)$  rotation at the start of each outer interferometer, if Bob does not block, the state of the photon after  $M$  outer cycles is

$$\cos\left(\frac{\pi}{2M}\right)^M |H\rangle. \quad (10)$$

Therefore, if the photon is not lost, it remains  $H$ -polarised. However, if Bob blocks, the photon after  $M$  outer cycles (as  $N \rightarrow \infty$ ) becomes  $V$ -polarised.

To prepare any qubit at Alice, Bob needs to apply a relative phase between Alice's two component, which can be represented as a  $\hat{\mathbf{R}}_z(\theta)$  rotation. Bob can implement this exchange-free using the device in figure 1, for an  $H$ -polarised component, relative to some other  $V$ -polarised component (e.g. one separated beforehand using a polarising beamsplitter).

We put this  $H$ -polarised component through one run of Salih *et al*'s 2013 protocol, with Bob either always blocking or not blocking his channel. If he blocks, and the component exits  $V$ -polarised, the PBS sends it through a HWP that flips it to  $H$ -polarised, and it is kicked out of the device; however, if it is  $H$ -polarised, it goes through a phase plate (gaining a phase increase of  $\pi/2L$ ), hits a mirror, goes back through the phase plate (gaining another phase increase of  $\pi/2L$ , for a total increase of  $\pi/L$ ), and re-enters the device for another run.

This is repeated  $L$  times, with Bob blocking or not blocking for all outer cycles in a given run. After each run, the component goes into a PBS: if it is  $H$ -polarised, it gains a phase of  $\pi/L$ ; if  $V$ -polarised, it is flipped to  $H$ -polarised and sent out from the unit. Bob first does not block for  $k$  runs, applying a phase of  $k\pi/L$ , then blocks, applying the transformation

$$|H\rangle \rightarrow e^{ik\pi/L} |H\rangle. \quad (11)$$

When  $N$  is finite, the rotations applied by each outer cycle when Bob blocks are not complete, meaning one run ( $M$  outer cycles) does not fully rotate the state from  $H$  to  $V$ . However, given Bob only blocks after the component has had a phase applied to it, to kick the component out of the device, any erroneous  $H$ -polarised component can be kept in the device by Bob not blocking for the remaining  $L - k$  full runs afterwards, letting us treat the erroneous  $H$ -component as loss.

While coarse-grained for finite  $L$ , as  $L$  goes to infinity (with  $0 \leq k/L \leq 1$ ), Bob can generate any relative phase for Alice's qubit, from 0 to  $\pi$ . Further, by moving the  $\pi/2$  half-wave plate from its location in figure 1 to the input, a similar phase can be added to a  $V$ -polarised component, relative to a  $H$ -polarised component.

Moreover, the phase unit can be constructed to include Aharonov and Vaidman's clever modification of Salih *et al*'s 2013 protocol [17], satisfying their weak-measurement criterion for exchange-free communication. We do this by running the inner cycles for  $2N$  cycles rather than  $N$ , except that for the case of Bob not blocking, he instead blocks for one of the  $2N$  inner cycles, namely the  $N$ th inner cycle. This has

the effect of helping to remove any lingering  $V$  component exiting the inner interferometer of figure 1 due to imperfections in practical implementation.

We now use our phase unit as the building block for a protocol where Bob can implement any arbitrary unitary onto Alice's qubit, exchange-free.

Any arbitrary  $2 \times 2$  unitary matrix can be written as

$$\begin{aligned}\hat{U} &= e^{i(2\alpha' - \beta'\hat{\sigma}_z - \gamma'\hat{\sigma}_y - \delta'\hat{\sigma}_x)/2} \\ &= e^{i\alpha'} \hat{\mathbf{R}}_z(\beta') \hat{\mathbf{R}}_y(\gamma') \hat{\mathbf{R}}_x(\delta').\end{aligned}\quad (12)$$

Note, the factor of  $e^{i\alpha'}$  can be ignored, as it provides global rather than relative phase, which is unphysical for a quantum state [21].

We can apply the  $\hat{\mathbf{R}}_z(\theta)$  rotations using the phase unit, and make a  $\hat{\mathbf{R}}_y(\theta)$  rotation by sandwiching a  $\hat{\mathbf{R}}_z(\theta)$  rotation between a  $-\pi/4$ -aligned quarter wave plate,  $\hat{U}_{\text{QWP}}$ , and its adjoint,  $\hat{U}_{\text{QWP}}^\dagger$ , where

$$\begin{aligned}\hat{U}_{\text{QWP}} &= \hat{\mathbf{R}}_x(-\pi/2) = e^{i\pi\hat{\sigma}_x/4} \\ \hat{U}_{\text{QWP}}^\dagger &= \hat{\mathbf{R}}_x(\pi/2) = e^{-i\pi\hat{\sigma}_x/4}.\end{aligned}\quad (13)$$

We set

$$\beta' = 2\pi\beta/L, \quad \gamma' = 2\pi\gamma/L, \quad \delta' = 2\pi\delta/L, \quad (14)$$

where, for the three phase unit runs,  $k$  is  $\beta$ ,  $\gamma$  and  $\delta$ .

The phase units form components of the overall protocol, as shown in figure 2. Here, Alice first splits her input state  $|\psi\rangle$  into  $H$ - and  $V$ -polarised components with a PBS, before putting each component through a phase unit, to generate equal and opposite phases on each. She recombines these at another PBS. Afterwards, she puts the components through a quarter wave plate, then through another run of PBS, phase unit, and PBS, then through the conjugate-transpose of the quarter-wave plate, tuned to convert the partial  $\hat{\mathbf{R}}_z$  rotation (phase rotation) into a partial  $\hat{\mathbf{R}}_y$  rotation. Finally, she applies another run of PBS, phase unit, and PBS to implement a second  $\hat{\mathbf{R}}_z$  rotation.

Using these  $\hat{\mathbf{R}}_z$  and  $\hat{\mathbf{R}}_y$  rotations, Bob can implement any arbitrary rotation on the surface of the Bloch sphere on Alice's state. This can be used either to allow Bob to prepare an arbitrary pure state at Alice (if she inserts a known state, such as  $|H\rangle$ ), or to perform any arbitrary unitary transformation on Alice's qubit, without Bob necessarily knowing that input state.

Because the phase units output their respective photon components after Bob blocks for a run, the timing of which depends on the phase Bob wants to apply, there is a time-binning (a grouping of exit times into discrete bins) of the components from each phase unit correlated with the phase Bob applies in that unit. Bob can, on his side, compensate for the time-binning (given he knows the phase he is applying). Further, in order to locate the photon in time, Alice can detect the time of exit using a non-demolition single photon detector (NDSPD).

Alternatively, we could add a final pair of phase units with the value of  $k$  set to  $3L' - \beta - \gamma - \delta$  (where  $L'$  is the value of  $L$  for each of the first three phase unit pairs, and  $\beta$ ,  $\gamma$  and  $\delta$  are their respective  $k$ -values), but without phase plates (see figure 1). This means that while no phase is applied, a time delay is still added to the components, meaning the photon always exits the overall device at a time proportional to  $3L$ , rather than  $\beta$ ,  $\gamma$  and/or  $\delta$  as before. This makes the time of exit uncorrelated to Bob's unitary, which means Alice can know in advance the expected exit time of her photon from the protocol (without needing to perform a non-demolition measurement to find it).

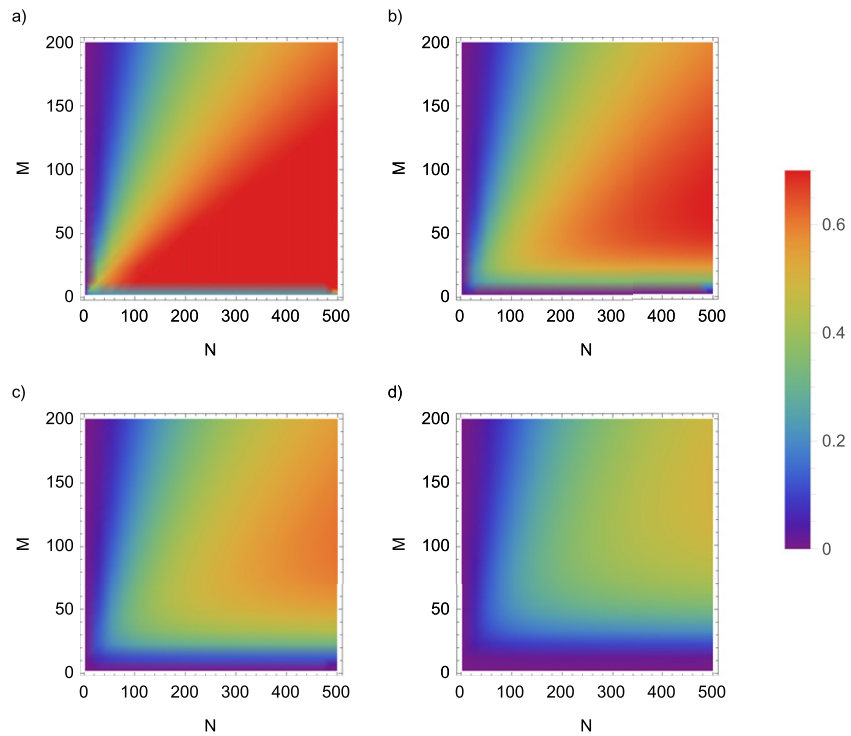
When considering a finite number of outer and inner cycles, there is a nonzero probability of the photon not returning to Alice, which reduces the protocol's efficiency. The survival probability of a photon going through a phase unit is plotted in figure 3. The survival probability for the overall protocol is the product of the survival probability for the three phase units:

$$P(\text{Tot})_{\text{sv}} = P(\beta)_{\text{sv}} \cdot P(\gamma)_{\text{sv}} \cdot P(\delta)_{\text{sv}}. \quad (15)$$

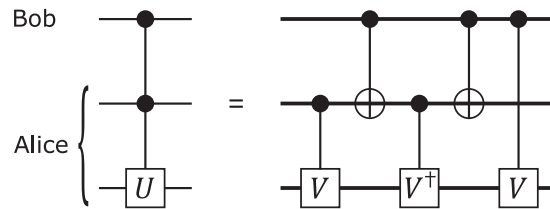
As expected, as  $\{M, N\} \rightarrow \infty$ , the survival probability goes to one.

Regardless, postselection renormalises Alice's output state such that if Alice receives an output photon, it will be in a pure state. Thus, for our set-up, given ideal optical components, the rotation enacted on Alice's qubit is always the rotation Bob has applied, not just for any  $L$ , but also for any  $N$ ,  $M$ , and  $k$ .

Interestingly, a phase unit, which outputs a photon into one of  $L$  different time bins depending on the number of runs Bob blocks, could be adapted to sending, exchange-free, a classical logical state of dimension  $d$  greater than two—a 'dit', rather than a bit. We do this by removing the phase plate in the phase unit (see figure 1). Bob first does not block for  $k$  runs, then blocks for the remaining  $L - k$ , meaning



**Figure 3.** The survival probability of a photon going through a phase unit (figure 1) of given  $M$  (number of outer cycles) and  $N$  (number of inner cycles). This is shown for the unit imparting phase  $ik\pi/L$ , where  $k$ , the number of runs of the protocol before the photon is emitted from the unit, is 1 for (a), 5 for (b), 10 for (c) and 20 for (d). Note there is no dependence on  $L$ , the maximum number of runs.



**Figure 4.** Quantum circuit diagram, showing how a 3-qubit gate applying a controlled-controlled unitary  $U$  can be constructed from two-qubit gates along with single-qubit gates, where  $U$  is some unitary transformation, and  $V^2 = U$  [22]. Using our exchange-free single-qubit gate, a classical Bob can directly simulate the control action on Alice's photonic qubits. Since any quantum circuit can be constructed using 2-qubit gates along with single-qubit ones, our exchange-free single-qubit gate allows Bob in principle to directly program any quantum algorithm at Alice, without exchanging any photons.

the photon's output occurs in the  $k$ th time-bin of  $L$  possible time-bins. This encodes a dit of dimension  $L$  into the photon, which Alice can read via NDSPD.

We now show how our exchange-free protocol enabling arbitrary single-qubit operations, can in principle allow a classical Bob to directly enact any quantum algorithm he wishes on Alice's qubits, without exchanging any particles with her. This is based on the fact any quantum algorithm can be efficiently constructed from 2-qubit operations (such as CNOT) and single-qubit ones. Our protocol already enables exchange-free single-qubit operations, i.e. gates. Thus, if Bob can directly activate or not, a 2-qubit gate at Alice, exchange-free, then directly programming an entire quantum algorithm at Alice using these two building blocks becomes possible. The quantum network of figure 4 shows how a 3-qubit controlled-controlled gate, applying some unitary  $U$  to the target qubit at Alice, can be constructed from 2-qubit controlled gates [22]. (Some controlled-controlled gates can have more implementable circuits than the general one given here [21].) A classical Bob, at the top end of figure 4, uses our exchange-free single-qubit gate to simulate the control action on Alice's photonic qubits. For simulating the CNOT gate, he can choose to either apply the identity transformation, representing control-bit  $|0\rangle$ , or apply an  $X$  transformation, representing control-bit  $|1\rangle$ . For the controlled- $V$  gate, he can choose to either apply the identity transformation, again representing control-bit  $|0\rangle$ , or apply a  $V$  transformation, representing control-bit  $|1\rangle$ . In this scenario, we envisage an optical programmable circuit, with exchange-free



single-qubit gates acting on Alice's qubits that Bob can directly program, and 2-qubit gates acting on Alice's qubits that he can directly choose to activate, exchange-free.

In summary, we have presented a protocol allowing Bob to directly perform any computation on a remote Alice's qubit, without exchanging any photons between them. We use this to show how, in principle, Bob can directly enact any quantum algorithm at Alice, exchange-free.

## Acknowledgments

We thank Claudio Marinelli for helping to bring this collaboration together. This work was supported by the Engineering and Physical Sciences Research Council (Grants EP/P510269/1, EP/T001011/1, EP/R513386/1, EP/M013472/1 and EP/L024020/1).

## Appendix A. A simpler protocol for applying an $\hat{\mathbf{R}}_y$ rotation

While considering how Bob could prepare an arbitrary qubit at Alice exchange-free, we have stumbled upon a much simpler protocol for Bob to prepare exchange-free a qubit with real, positive probability amplitudes.

Consider figure 1, without the phase module. Starting with Alice's  $H$ -polarised photon, instead of Bob blocking or not blocking every cycle, he instead does not block for the first  $M - k$  outer cycles, then blocks for the rest. In order to eliminate the error resulting from a finite number of blocked inner cycles, Alice introduces loss, attenuating the outer arm of the interferometer on her side by a factor of  $\cos(\pi/2N)^N$  for each outer cycle. This means, before the final PBS, the state is

$$|\Psi\rangle = \cos\left(\frac{\pi}{2N}\right)^{MN} \cos\left(\frac{\pi}{2M}\right)^{M-k} \times \left( \cos\left(\frac{k\pi}{2M}\right) |H\rangle + \sin\left(\frac{k\pi}{2M}\right) |V\rangle \right). \quad (16)$$

By postselecting on Alice's photon successfully exiting the protocol, she receives the state

$$|\Psi\rangle_{\text{PS}} = \cos\left(\frac{k\pi}{2M}\right) |H\rangle + \sin\left(\frac{k\pi}{2M}\right) |V\rangle. \quad (17)$$

By choosing  $k$ , Bob directly applies a  $\hat{\mathbf{R}}_y$  rotation to Alice's  $|H\rangle$  input state. Now, in order to allow Bob to apply such a rotation to an arbitrary input polarisation state, Alice's photon is initially split into  $H$  and  $V$ -components using a PBS. The desired rotation is applied separately. In the case of the  $V$ -component, its polarisation is first flipped to  $H$  before the rotation is applied, followed by a phase flip and a polarisation flip upon exit. The separate components can then be combined using a 50:50 beamsplitter, with the correct state obtained 50% of the time. The advantage, however, is that, assuming perfect optical components and a large number of cycles, only two runs of the protocol are needed on average.

## Appendix B. Kraus operator notation

Viewing exchange-free communication more abstractly, we consider the communication channel in Kraus operator notation.

Here, we associate a channel  $\mathcal{X}$  to the set of Kraus operators  $\{X_i\}_i$  which describe its action on a given density operator such that

$$\begin{aligned} \mathcal{X} &\sim \{X_i\}_i \\ \rho &\rightarrow \mathcal{X}(\rho) = \sum_i X_i \rho X_i^\dagger \\ \sum_i X_i^\dagger X_i &= \mathbb{1}. \end{aligned} \quad (18)$$

In general, for channels  $\mathcal{X}$  and  $\mathcal{Y}$ , their composition can be written,

$$\mathcal{X} \circ \mathcal{Y}(\rho) := \mathcal{X}(\mathcal{Y}(\rho)) = \sum_i X_i \left( \sum_j Y_j \rho Y_j^\dagger \right) X_i^\dagger \quad (19)$$

and we denote the  $N$ -fold composition of a channel  $\mathcal{X}^N(\rho) := \mathcal{X} \circ \mathcal{X} \circ \dots \circ \mathcal{X}(\rho)$ .



In this manner we can define three channels in this protocol: first that constituting Bob's action on the channel,  $b$ , that goes via him, when he blocks/does not block

$$\begin{aligned}\mathcal{B}^B &\sim \{|0_b\rangle\langle 1_b|, |0_b\rangle\langle 0_b|\}, \\ \mathcal{B}^{NB} &\sim \{|1_b\rangle\langle 1_b|, |0_b\rangle\langle 0_b|\};\end{aligned}\quad (20)$$

Each cycle of Alice's inner-interferometer is given by  $\mathcal{B}^{NB} \circ \hat{\mathbf{R}}_{y,(a1,b)}^{(\pi/N)}$ , and imposing that the initial state in Bob's mode is vacuum, and omitting it from the output state by tracing it out, we have that over the  $N$  inner cycles one finds channels on Alice's mode  $a1$  given by,

$$\begin{aligned}\mathcal{A}_1^B(\rho) &:= \text{tr}_b \left[ (\mathcal{B}^B \circ \hat{\mathbf{R}}_{y,(a1,b)}^{(\pi/N)})^N (\rho \otimes |0_b\rangle\langle 0_b|) \right], \\ \mathcal{A}_1^{NB}(\rho) &:= \text{tr}_b \left[ (\mathcal{B}^{NB} \circ \hat{\mathbf{R}}_{y,(a1,b)}^{(\pi/N)})^N (\rho \otimes |0_b\rangle\langle 0_b|) \right],\end{aligned}\quad (21)$$

where any channel acting on a larger Hilbert space than that on which it is defined acts as identity channel, i.e.  $\mathcal{B}^{NB} \sim \mathcal{B}^{NB} \otimes \mathbb{1}$ . We find when Bob blocks/does not block:

$$\begin{aligned}\mathcal{A}_1^B &\sim \left\{ \cos\left(\frac{\pi}{2N}\right)^N |1_{a1}\rangle\langle 1_{a1}|, \cos\left(\frac{\pi}{2N}\right)^{N-1} \sin\left(\frac{\pi}{2N}\right) |0_{a1}\rangle\langle 1_{a1}| \right\}, \mathcal{A}_1^{NB} \\ &\sim \{|0_{a1}\rangle\langle 1_{a1}|, |0_{a1}\rangle\langle 0_{a1}|\};\end{aligned}\quad (22)$$

then finally the effect this has overall as the channel created by a chain of  $M$  outer interferometers on Alice's inner and outer interferometer ( $V$  and  $H$ ) modes, when Bob blocks/does not block:

$$\begin{aligned}\mathcal{A}_{12}^B(\rho) &:= (\mathcal{A}_1^B \circ \hat{\mathbf{R}}_{y,(a2,a1)}^{(\pi/M)})^M(\rho), \\ \mathcal{A}_{12}^{NB}(\rho) &:= (\mathcal{A}_1^{NB} \circ \hat{\mathbf{R}}_{y,(a2,a1)}^{(\pi/M)})^M(\rho).\end{aligned}\quad (23)$$

Therefore, we find

$$\begin{aligned}\mathcal{A}_{12}^B &\sim \left\{ c_1 |1_{a2}0_{a1}\rangle\langle 1_{a2}0_{a1}|, c_2 |0_{a2}1_{a1}\rangle\langle 0_{a2}1_{a1}|, c_3 |0_{a2}1_{a1}\rangle\langle 1_{a2}0_{a1}|, \right. \\ &c_4 |1_{a2}0_{a1}\rangle\langle 0_{a2}1_{a1}|, |0_{a2}0_{a1}\rangle\langle 0_{a2}0_{a1}| \sqrt{(1-c_1^2-c_3^2)} |0_{a2}0_{a1}\rangle\langle 1_{a2}0_{a1}|, \\ &\left. \sqrt{(1-c_2^2-c_4^2)} |0_{a2}0_{a1}\rangle\langle 0_{a2}1_{a1}| \right\} \\ \mathcal{A}_{12}^{NB} &\sim \left\{ \cos\left(\frac{\pi}{2M}\right)^M |1_{a2}0_{a1}\rangle\langle 1_{a2}0_{a1}|, \sqrt{\left(1-\cos\left(\frac{\pi}{2M}\right)^{2M}\right)} |0_{a2}0_{a1}\rangle\langle 1_{a2}0_{a1}|, \right. \\ &\left. |0_{a2}0_{a1}\rangle\langle 0_{a2}1_{a1}|, |0_{a2}0_{a1}\rangle\langle 0_{a2}0_{a1}| \right\},\end{aligned}\quad (24)$$

where coefficients  $c_1, c_2, c_3$  and  $c_4$  are functions of  $M$  and  $N$ , with  $c_2$  and  $c_3$  going to 1, and  $c_1$  and  $c_4$  going to zero, as  $N$  and  $M$  go to infinity. This means one run (of  $M$  outer cycles of  $N$  inner cycles each) acts as a perfect optical switch in this limit, turning  $H$  to  $V$  (and vice versa) if Bob blocks, and implementing identity if he does not.

## ORCID iDs

Hatim Salih  <https://orcid.org/0000-0003-3854-7813>

Jonte R Hance  <https://orcid.org/0000-0001-8587-7618>

Will McCutcheon  <https://orcid.org/0000-0003-0344-6385>

John Rarity  <https://orcid.org/0000-0002-8601-5558>

## References

- [1] Mitchison G and Jozsa R 2001 Counterfactual computation *Proc. R. Soc. A* **457** 1175

- [2] Hosten O, Rakher M T, Barreiro J T, Peters N A and Kwiat P G 2006 Counterfactual quantum computation through quantum interrogation *Nature* **439** 949
- [3] Elitzur A C and Vaidman L 1993 Quantum mechanical interaction-free measurements *Found. Phys.* **23** 987
- [4] Kwiat P, Weinfurter H, Herzog T, Zeilinger A and Kasevich M A 1995 Interaction-free measurement *Phys. Rev. Lett.* **74** 4763
- [5] Kwiat P G, White A G, Mitchell J R, Nairz O, Weihs G, Weinfurter H and Zeilinger A 1999 High-efficiency quantum interrogation measurements via the quantum zeno effect *Phys. Rev. Lett.* **83** 4725
- [6] Misra B and Sudarshan E C G 1977 The Zeno's paradox in quantum theory *J. Math. Phys.* **18** 756
- [7] Rudolph T 2000 Better schemes for quantum interrogation in lossy experiments *Phys. Rev. Lett.* **85** 2925
- [8] Noh T-G 2009 Counterfactual quantum cryptography *Phys. Rev. Lett.* **103** 230501
- [9] Liu Y *et al* 2012 Experimental demonstration of counterfactual quantum communication *Phys. Rev. Lett.* **109** 030501
- [10] Salih H, Li Z-H, Al-Amri M and Zubairy M S 2013 Protocol for direct counterfactual quantum communication *Phys. Rev. Lett.* **110** 170502
- [11] Cao Y *et al* 2017 Direct counterfactual communication via quantum zeno effect *Proc. Natl Acad. Sci. USA* **114** 4920
- [12] Vaidman L 2014 Comment on 'protocol for direct counterfactual quantum communication' *Phys. Rev. Lett.* **112** 208901
- [13] Salih H, Li Z-H, Al-Amri M and Zubairy M S 2014 Salih *et al* reply *Phys. Rev. Lett.* **112** 208902
- [14] Griffiths R B 2016 Particle path through a nested Mach–Zehnder interferometer *Phys. Rev. A* **94** 032115
- [15] Salih H 2018 Comment on 'particle path through a nested Mach–Zehnder interferometer' *Phys. Rev. A* **97** 026101
- [16] Griffiths R B 2018 Reply to 'comment on 'particle path through a nested Mach–Zehnder interferometer'' *Phys. Rev. A* **97** 026102
- [17] Aharonov Y and Vaidman L 2019 Modification of counterfactual communication protocols that eliminates weak particle traces *Phys. Rev. A* **99** 010103
- [18] Salih H, McCutcheon W, Hance J R and Rarity J 2018 Do the laws of physics prohibit counterfactual communication? (arXiv:1806.01257)
- [19] Salih H 2016 Protocol for counterfactually transporting an unknown qubit *Front. Phys.* **3** 94
- [20] Salih H 2018 From a quantum paradox to counterportation (arXiv:1807.06586)
- [21] Nielsen M A and Chuang I 2002 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
- [22] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 Elementary gates for quantum computation *Phys. Rev. A* **52** 3457