PAPER • OPEN ACCESS

Demonstration of measurement-only blind quantum computing

To cite this article: Chiara Greganti *et al* 2016 *New J. Phys.* **18** 013020

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
23 March 2015

REVISED
11 October 2015

ACCEPTED FOR PUBLICATION
1 December 2015

PUBLISHED
8 January 2016

PAPER

Demonstration of measurement-only blind quantum computing

Chiara Greganti[1], **Marie-Christine Roehsner**[1], **Stefanie Barz**[1,2], **Tomoyuki Morimae**[3] **and Philip Walther**[1]

[1] University of Vienna, Faculty of Physics, Austria
[2] Present address: University of Oxford, Clarendon Laboratory, UK
[3] ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan

Keywords: quantum computing, security, photons

Supplementary material for this article is available online

Abstract

Blind quantum computing allows for secure cloud networks of quasi-classical clients and a fully fledged quantum server. Recently, a new protocol has been proposed, which requires a client to perform only measurements. We demonstrate a proof-of-principle implementation of this measurement-only blind quantum computing, exploiting a photonic setup to generate four-qubit cluster states for computation and verification. Feasible technological requirements for the client and the device-independent blindness make this scheme very applicable for future secure quantum networks.

Introduction

Quantum physics enables one to enhance security for processing data over a distributed network. In particular, quantum cloud computing allows quasi-classical clients (i.e. clients with a limited amount of quantum resources, such as qubit preparation or detection) to do calculations beyond their computational power, namely perform quantum algorithms. The first proposed and demonstrated two-party secure quantum cloud computation protocol is known as blind quantum computing (BQC) [1]: a client, Alice, who can generate only single-qubit states, delegates her quantum computing to a remote server, Bob, who has a fully fledged quantum computer, without leaking any of her privacy. Many theoretical studies based on this have been performed recently [2–11], and also experimental demonstrations have been reported [12–14]. A simplified and novel version for secure quantum computing consists of a two-party protocol [2, 15], where Alice only makes measurements and Bob's blindness is proven by the no-signaling principle [16]. Here blindness indicates that whatever Bob does; he cannot learn any of Alice's privacy.

In order to underline the feasibility of the measurement-only BQC we demonstrate the computation protocol in a photonic experiment. Bob generates four-qubit resource states that are used by Alice to implement generic two-qubit entangling gates and verification protocols.

Theory

The idea of measurement-only BQC is shown in figure 1. Bob generates a resource state for measurement-based quantum computing (MBQC) [17, 18], and he sends the corresponding qubits, one by one, through a one-way quantum channel to Alice. She measures each qubit according to her program. For any kind of a malicious Bob, he cannot learn anything about Alice's quantum computation, because information is sent only in one direction. The no-signaling principle then ensures that if Alice and Bob share a system (classical, quantum, or superquantum) and she measures her part, this does not transmit any information to Bob. This principle is more fundamental than quantum physics [16] and consequently provides security even against superquantum attacks.

We remark that the original BQC examines a different approach. A quasi-classical Alice must be able to generate randomly rotated single-qubit states, send these via a quantum channel to Bob, and interact via classical channels in order to control and receive the computation results. Recently, the single-qubit generation

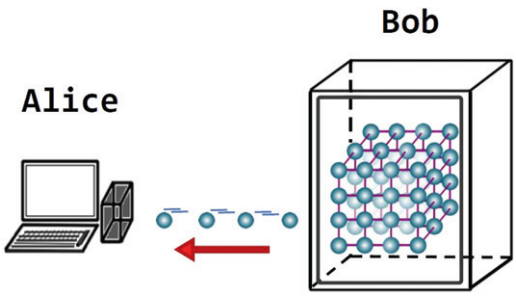

Figure 1. Measurement-only blind quantum computing. Alice, a client with a classical device (laptop) and a quantum detector device (grey box), receives quantum information via a one-way channel from Bob, a quantum server capable of generating entangled quantum states as universal resources. Here Bob's resource corresponds to a fault-tolerant 3D-cluster state, but it can be any other measurement-based quantum computation resource.

requirement is extended to the coherent state generation Vedran or single-qubit measurement [19]. The measurement-only BQC scheme centers on a quasi-classical Alice, who now only receives qubits that she then measures. This alternative concept produces a practical computing protocol. In particular, in optical systems, the technological demand for a client is readily available. An additional feature of measurement-only BQC is the device-independent blindness: even if Alice owns a malicious device (probably bought from another company), no information is transmitted to Bob because of the no-signaling principle. In our case, we obtain device independence regarding blindness; recently, the concept of device independence has also been generalized to verifiability [19, 20]. Furthermore the full-fledged quantum computer can be based on any model of MBQC (see [2] for more detailed discussion).

The concept of secure quantum computing opened up feasible verification methods [3, 13, 15] where Alice can test whether Bob is performing the computation correctly. It was shown that the verification is possible for the original protocol [3, 13] as well as for the measurement-only protocol [15]. The central idea in these protocols is that Alice secretly hides some 'trap' qubits in the resource state. This fundamentally reduces to the situation where Alice tries to verify Bob's quantum resource with a minimal set of measurements [21–23]. If Bob deviates from the correct protocol, he changes the states of the traps, and if Alice detects the change of any trap, she can detect Bob's malicious behaviour and abort the computation. The security corresponds to the probability that Alice does not accept the results received by a cheating Bob.

In measurement-only BQC, the trap qubits are randomly prepared and placed via measurements by Alice within the computation resource and are associated to qubit states in Z and X basis (corresponding to Pauli operators σ_z and σ_x respectively). When Alice receives the traps, she measures the qubits in the respective basis.

For the special case of a four-qubit linear cluster state, a verification protocol with only two different trap measurements exists. This protocol runs as follows:

1. Bob prepares the four-qubit linear cluster state and sends each qubit one by one to Alice.
2. Alice chooses one of the two tests randomly below:
   a. Alice measures qubits 1 and 3 in the Z basis and qubits 2 and 4 in the X basis.
   b. Alice measures qubits 2 and 4 in the Z basis and qubits 1 and 3 in the X basis.

If she chooses option (a), qubits 2 and 4 become trap qubits. If any trap qubit is changed (i.e. she does not get the expected result), then she detects Bob's malicious behavior. We call this the option (1, 3) test. On the other hand, if she chooses option (b), qubits 1 and 3 become trap qubits, and she can check those. We call this the option (2, 4) test. We show now that Bob has to prepare the exact four-qubit linear cluster state in order to pass all Alice's trap tests in the limit of n repetitions, where n tends toward infinity. In the original verification protocols [3, 15], it is shown that the probability that Alice is fooled by Bob can be exponentially small, by using quantum error-correcting codes.

Here, let us show the case without a quantum error-correcting code, which leads to a probability of accepting a wrong outcome to be polynomially small. We want to point out that this probability can be minimized to become exponentially small by exploiting standard error amplification techniques [24] via repeating the computation a number of times proportional to n. Bob can generate any state, but in order to pass the (1, 3) test, Bob has to prepare the state:

$$|\Psi\rangle \equiv \frac{1}{2}\Big(\big|0+0+\big\rangle\big|a_1\big\rangle + e^{i\theta_2}\big|0-1-\big\rangle\big|a_2\big\rangle + e^{i\theta_3}\big|1-0+\big\rangle\big|a_3\big\rangle + e^{i\theta 4}\big|1+1-\big\rangle\big|a_4\big\rangle\Big) \quad (1)$$

where $\{|a_j\rangle\}$ are certain states of Bob's ancilla, which are normalized $|\langle a_j|a_j\rangle|^2 = 1$, but not necesarily mutually orthogonal. We consider ancilla states, since Bob could prepare a larger system and keep a subsystem. Since Bob does not know which option Alice takes, this state also has to pass Alice's other test, i.e. the (2, 4) test. Assume that Alice gets the result (0, 0) when she measures qubits 2 and 4. Then the state after the measurement becomes

$$\big|\Psi'\big\rangle \equiv \frac{1}{2}\Big(|0\rangle_1|0\rangle_3|a_1\rangle + e^{i\theta_2}|0\rangle_1|1\rangle_3|a_2\rangle + e^{i\theta_3}|1\rangle_1|0\rangle_3|a_3\rangle + e^{i\theta 4}|1\rangle_1|1\rangle_3|a_4\rangle\Big). \quad (2)$$

In order to pass the (2, 4) test (again in the limit of n repetitions), this state must be $|+\rangle_1|+\rangle_3|b\rangle$ for a certain state $|b\rangle$. This means that, first, the reduced density operator of $|\Psi'\rangle$ for Bob's ancilla

$$\rho = \frac{1}{4}\sum_{j=1}^{4}\big|a_j\big\rangle\big\langle a_j\big|$$

must have rank 1, which leads to $|a_j\rangle = |a_k\rangle$ (up to a phase factor). Now the state is

$$\frac{1}{2}\Big(|0\rangle_1|0\rangle_3 + e^{i\theta_2'}|0\rangle_1|1\rangle_3 + e^{i\theta_3'}|1\rangle_1|0\rangle_3 + e^{i\theta 4'}|1\rangle_1|1\rangle_3\Big)|a_1\rangle.$$

Next, in order for this state to be $|+\rangle_1|+\rangle_3|b\rangle$, $\theta_j' = 0$ for all $j = 2, 3, 4$. Therefore, repeating both tests Alice verifies that Bob has the exact four-qubit cluster state, except for a small probability of undetected cheating.

In a general case, Alice can choose to use the resource state for either verification or computation. Increasing the number of verifications per computation provides a higher level of security at the cost of efficiency. The probability of undetected errors, i. e. Bob cheats in the computation and not in the verification, is linearly bounded as in [13]. In [13] Alice is assumed to send qubits, whereas here Alice measures the received qubits. Remarkably the same technique of verification can be applied in both schemes: Alice generates trap qubits via either choosing Bob's measurement settings or by directly performing the measurements at her side. This allows for the same analysis, discussed already in [13]. In our case, Alice can randomly choose between the two verification options and a regular computation on a four-qubit linear cluster. Reference[25] describes the asymptotic behavior of the scaling for linear cluster states of increasing length.

It is worth to note that in [1], a random-number generator is necessary for the blindness, whereas in measurement-only BQC [2], no random-number generator is required for Alice to guarantee the blindness. If we add the option of the verification, both protocols require random-number generators, since Alice has to randomly place trap qubits. Nevertheless the use of quantum random numbers is nowadays accessible at the consumer grade [26].

Experiment and results

We practically realize a proof-of-principle implementation of the protocol using photons, computing two-qubit entangling gates and verifying two single-trap qubits. In contrast to the proposed theoretical scheme [15], where traps are hidden within the computation resource, our experiment exploits a four-qubit cluster state either for a computation or for a verification run, due to the number of available qubits.

The four-qubit resource for measurement-only BQC (figures 3(a) and (b)) is produced in Bob's laboratory via a photonic setup in a so-called railway-crossing configuration (see figure 2). A double spontaneous parametric downconversion process allows us to generate two pairs of polarization entangled photons. Interferometers with polarizing beam splitters (PBSs) entangle the four photons. Additional half-wave plates (HWPs) on both pairs directions enable the generation of different graph states. The scheme has already been exploited in several other works to create four-qubit linear cluster states and states that can be obtained from them via local complementations (see e.g. [12, 27]). Here we focus on the generation of a four-qubit star cluster state and a four-qubit linear cluster state, respectively (figure 3(a) and (b)):

$$\big|C_{\text{star}}\big\rangle = \frac{1}{\sqrt{2}}(|++0+\rangle + |--1-\rangle)_{1234}, \quad (3)$$

$$|C_{\text{lin}}\rangle = \frac{1}{2}(|0+0+\rangle + |0-1-\rangle + |1-0+\rangle + |1+1-\rangle)_{1234}, \quad (4)$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ are the eigenstates of the Pauli operator $\sigma_x = X$. Remarkably these cluster states belong to different classes of entanglement.

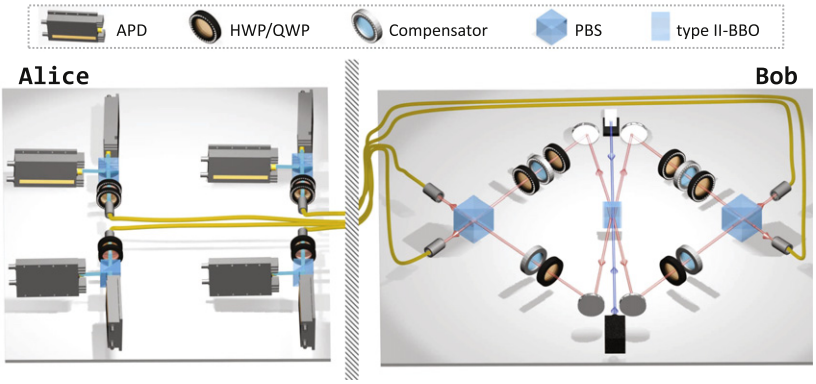

Figure 2. Schematic of Alice's (left) and Bob's (right) optical setups. Right: The four-qubit entangled states are generated via a fs-pulsed laser pumping a type-II BBO crystal in a double-passage scheme. The compensator, HWPs and PBSs allow Bob to select the desired four-qubit resource. Left: The detection requires HWP, QWP and PBS for measuring in different polarization basis and single-photon APD per qubit. The laboratories are connected by single-mode fibers as quantum channels. See main text for acronyms.

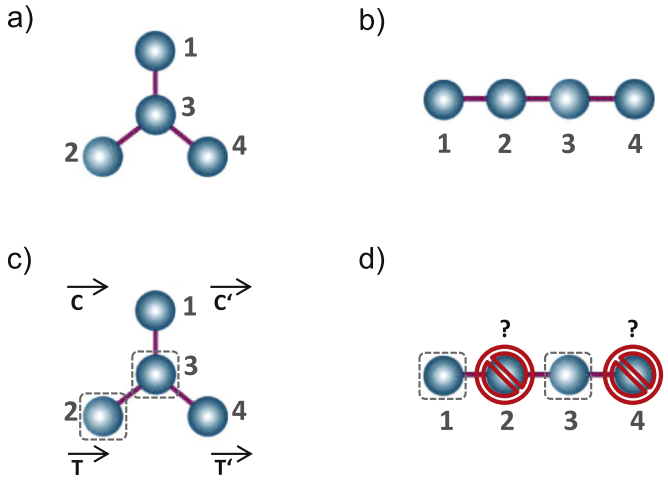

Figure 3. Bob's quantum resources: four-qubit (a) star and (b) linear cluster states. (c) Implementation of an entangling gate on a four-qubit star cluster. C (C') and T (T') are the control and target input (output) logical qubits. (d) Verification $(1,\ 3)$ test on a linear cluster state. The dashed frame corresponds to a single-qubit measurement, whereas the red frame represents a trap. Verification $(2,\ 4)$ test is equivalent under exchange of trap and measured qubits.

The four-qubit star cluster was generated within this setup only recently (see [22] for details) and now exploited for quantum information computing. Switching between the two entangled classes involves preparing specific Bell states at each SPDC process, different photonic interferences between the two pairs of photons, precise wavelength-scale alignment, and, therefore, high stability.

Alice's laboratory consists of four HWPs, four quarter-wave plates (QWPs), four PBSs and eight single photon counting detectors (APDs) in order to speed up the data acquisition (four APDs are sufficient to measure all possible polarization-basis of four-qubit state) and proceed to a complete analysis using quantum state tomography (QST) [28]. The connecting quantum channel from Bob to Alice is achieved by four single-mode fibers, which carry the photonic qubits. We reconstructed through overcomplete QST the density matrix of the two four-qubit resources, obtaining fidelities of the state with respect to the ideal star cluster and linear cluster of $F = 0.731 \pm 0.008$ and $F = 0.676 \pm 0.007$ (under local unitary operations), respectively (see SI for the density matrix histograms).

Computation

The four-qubit star and linear cluster states are the minimal resources for one-way computation, since the full universal set of gates can be reproduced [17]. This has been already demonstrated in few works [29–34]. In this work we reproduce different two-qubit entangling gates using the star cluster in order to validate the

Table 1. Results from measuring qubit 2 and qubit 3 of the star cluster onto Y_2X_3, which corresponds to a CNOT gate on states $|+ +_i\rangle$ and $|+ -_i\rangle$ up to a $(Z_1Z_4)^{s_3+1}$, where s_2 and s_3 are the measurement outcomes. The fidelities of the tomographic reconstructed two-qubit state with respect of the ideal state are reported.

s_2s_3	Ideal Output State	Fidelity
00	$(\|0 +_i\rangle + \mathrm{i}\,\|1 -_i\rangle)_{14}/\sqrt{2}$	$F = 0.87 \pm 0.03$
01	$(\|0 +_i\rangle + \mathrm{i}\,\|1 -_i\rangle)_{14}/\sqrt{2}$	$F = 0.74 \pm 0.04$
10	$(\|0 -_i\rangle - \mathrm{i}\,\|1 +_i\rangle)_{14}/\sqrt{2}$	$F = 0.77 \pm 0.03$
11	$(\|0 -_i\rangle - \mathrm{i}\,\|1 +_i\rangle)_{14}/\sqrt{2}$	$F = 0.77 \pm 0.04$

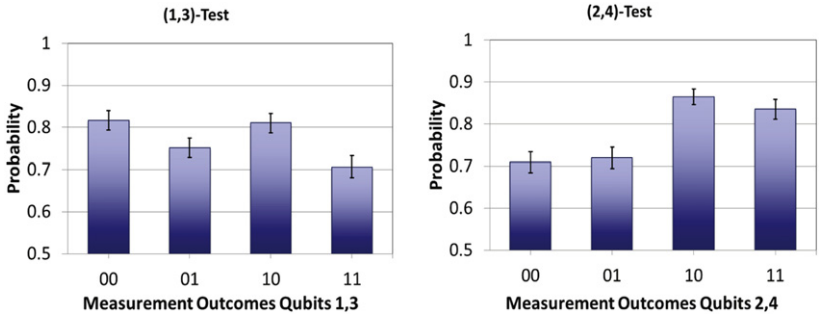

Figure 4. Probability that Alice receives the expected outcomes for the (1, 3) test and (2, 4) test on a linear cluster state. According to the measurement outcomes of the nontrap qubits (shown on the abscissa), we report the probability that measurements on each of Alice's trap qubits return the expected result (i.e. Alice trusts the state Bob sent).

computation from Alice's device. An entangling gate is performed using a star cluster, where qubits 1 and 2 are acting as input control (C) and target (T) qubits, respectively, whereas qubits 1 and 4 present the output control (C') and target (T') qubits, respectively, as shown in figure 3(c). Different combinations of measurement bases for qubit 2 and 3 enable to create entanglement between the output qubits. Detailed analysis for some entangling gates are reported in the SI. In table 1 we present, as an example, the results related to measuring qubits 2 and 3 in the Y_2X_3 basis (where Y is the Pauli σ_y), which corresponds to implementing a Controlled NOT (CNOT) gate for input state $|+ +_i\rangle$ and $|+ -_i\rangle$ (where $|+_i\rangle = (|0\rangle + \mathrm{i}\,|1\rangle)/\sqrt{2}$ and $|-_i\rangle = (|0\rangle - \mathrm{i}\,|1\rangle)/\sqrt{2}$ are the eigenstates of Y) up to local unitary operations. The two-qubit output states are analysed through two-qubit QST with acquisition time of 600 s per measurement setting. The corresponding uncertanties are due to Poissonian counting statistics and represent only a lower bound for the errors.

Verification

The four-qubit linear cluster allows verifying computation with only two different trap measurements and is especially suited for the verification protocol as described in the theory section. We present the results for this state along with the results for a four-qubit star cluster state. As has been shown in [13], the probability that Alice is fooled by Bob is bounded in such a setting.

For the case of the four-qubit linear cluster state, we implement the (1, 3) and (2, 4) tests by having Alice choosing the respective basis. Per trap we analyze the measurement outcomes in order to quantify the probabilities that Alice obtains the correct state (see figure 4). For a single trap, the results are within the values $[0.74 \pm 0.03, 0.98 \pm 0.01]$, where the range is due to unbalanced phase noises in the setup. Each of Alice's measures has an acquisition time of 1 h to decrease the uncertainty. Alice verified the resource with nonideal probability, due to experimental imperfections of the setup, which are present during the generation of the four-qubit resource as already seen from the full QST fidelity of the state.

Additionally, we performed the verification protocol on a four-qubit star cluster state, which we used before to implement entangling gates. We report the two trap tests performed on the star cluster state, equivalently to the linear cluster case) see figure 5). In this case, in order to get two trap qubits each time Alice measures Z_1Z_3 (expecting trap qubits in X basis) for the (1, 3) test, and Z_2X_4 (expecting one trap qubit in X basis and one in Z) for the (2, 4) test. The single probabilities of individual trap qubits, corresponding to Alice's expected results,

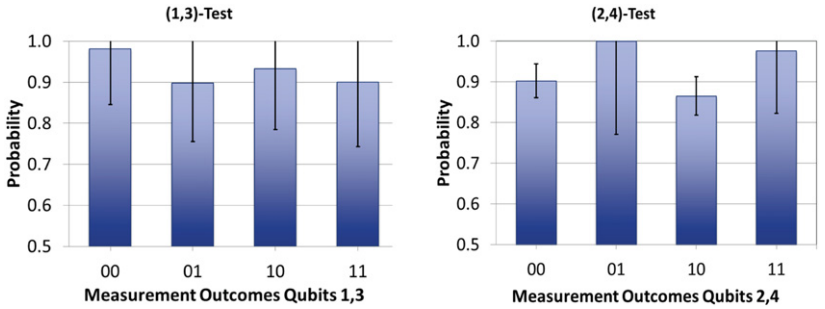

Figure 5. Probability that Alice receives the expected outcomes for the two verification tests on a star cluster. According to the measurement outcomes of the nontrap qubits (shown on the abscissa), we report the probability that measurements on each of Alice's trap qubits return an expected result (i.e. Alice trusts the state Bob sent).

and according to respective measurement outcomes of the nontrap qubits are in the range $[0.90 \pm 0.04, 1.00 - 0.16]$ with an acquisition time of 600 s per single measurement (see SI for details). The imbalance of the obtained probabilities with respect to the quantum state fidelity is due to asymmetric noise.

Here we want to point out that the small increased value of fidelity of the star cluster, with respect to the linear cluster, leads to significant improvements for the verification results.

Discussion

The use of four-qubit photonic cluster states allows us to prove the feasibility of two-party measurement-only BQC in current quantum optics laboratories. Nevertheless the demonstration can be expanded to several quantum systems and other MBQC models. In the photonic case, we want to emphasize that just one HWP, one QWP, one PBS, and one APD would be sufficient for Alice to measure every qubit received from Bob and consequently to implement computation and verification. The only additional requirement in Bob's laboratory would be a time-delay multiplexer (such as the one used in [35]) or a delay line in each photon's path (such as in [36]). The tomographic reconstruction of Bob's resource state, as we did in our experiment, is in fact superfluous for Alice's computation, since already from the single-qubit measurement she can verify Bob's state. The quantum power required for Alice is then restricted to measuring the state of the qubits. It is important to note the high losses, either due to low detection efficiencies or imperfect quantum channels, would break Alice's computation. However, the threshold for losses can be increased by using fault-tolerant MBQC models, which are robust against errors and losses [37], and besides, detection devices with almost unit efficiencies are now available [38, 39].

In conclusion the demonstrated protocol constitutes a step further to more realistic secure quantum computing models.

Acknowledgments

This work was supported by the European Commission, Initial Training Network PICQUE (No. 608062), QUILMI (No. 295293), EQUAM (No. 323714), GRASP (No. 613024); the Vienna Center for Quantum Science and Technology (VCQ), the Austrian Science Fund (FWF) through START (No. Y585-N20); the doctoral programme CoQuS, the Vienna Science and Technology Fund (WWTF) under grant ICT12-041; the Air Force Office of Scientific Research, Air Force Material Command, United States Air Force, under grant number FA8655-11-1-Science, and Technology3004; and the Tenure Track System by MEXT Japan and KAKENHI 26730003 and 15H00850 by JSPS.

References

[1] Broadbent A, Fitzsimons J and Kashefi E 2009 *Proc. of the 50th Annual Symp. on Foundations of Computer Science* 517–26
[2] Morimae T and Fujii K 2013 *Phys. Rev.* A **87** 050301
[3] Fitzsimons J and Kashefi E 2012 in preparation (arXiv:1203.5217)
[4] Dunjko V, Kashefi E and Leverrier A 2012 *Phys. Rev. Lett.* **108** 200502
[5] Morimae T, Dunjko V and Kashefi E 2015 *Quantum Inf. Comput.* **15** 0200
[6] Morimae T and Fujii K 2012 *Nat. Commun.* **3** 1036
[7] Morimae T 2012 *Phys. Rev. Lett.* **109** 230502
[8] Giovannetti V, Maccone L, Morimae T and Rudolph T 2013 *Phys. Rev. Lett.* **111** 230501

[9] Mantri A, Pérez-Delgado C and Fitzsimons J 2013 *Phys. Rev. Lett.* **111** 230502
[10] Sueki T, Koshiba T and Morimae T 2013 *Phys. Rev.* A **87** 060301
[11] Li Q, Chan W H, Wu C and Wen Z 2014 *Phys. Rev.* A **89** 040302
[12] Barz S, Kashefi E, Broadbent A, Fitzsimons J, Zeilinger A and Walther P 2012 *Science* **335** 303
[13] Barz S, Fitzsimons J F, Kashefi E and Walther P 2013 *Nat. Phys.* **9** 727
[14] Fisher K, Broadbent A, Shalm L, Yan Z, Lavoie J, Prevedel R, Jennewein T and Resch K 2014 *Nat. Commun.* **5** 3074
[15] Morimae T 2014 *Phys. Rev.* A **89** 060302
[16] Popescu S and Rohrlich D 1994 *Found. Phys.* **24** 379
[17] Raussendorf R and Briegel H 2001 *Phys. Rev. Lett.* **86** 5188
[18] Briegel H, Browne D E, Dür W, Raussendorf R and Van den Nest M 2009 *Nat. Phys.* **5** 19
[19] Hajdusek M, Pérez-Delgado C and Fitzsimons J 2015 in preparation (arXiv:1502.02563v1)
[20] Gheorghiu A, Kashefi E and Wallden P 2015 in preparation (arXiv:1502.02571v2)
[21] Tóth G and Gühne O 2005 *Phys. Rev.* A **72** 022340
[22] Greganti C, Roehsner M C, Barz S, Waegell M and Walther P 2015 *Phys. Rev.* A **91** 022325
[23] Knips L, Schwemmer C, Klein N, Wieśniak M and Weinfurter H 2014 in preparation (arXiv:1412.5881)
[24] Kitaev A Y, Shen A H and Vyalyi M N 2002 *Classical and Quantum Computation* (Boston, MA: American Mathematical Society)
[25] Hayashi M and Morimae T 2015 in preparation (arXiv:1505.07535)
[26] Sanguinetti B, Martin A, Zbinden H and Gisin N 2014 *Phys. Rev.* X **4** 031056
[27] Barz S, Vasconcelos R, Greganti C, Zwerger M, Duer W, Briegel H and Walther P 2014 in preparation (arXiv. 1308.5209)
[28] James D, Kwiat P, Munro W and White A 2001 *Phys. Rev.* A **64** 52312
[29] Walther P, Resch K, Rudolph T, Schenck E, Weinfurter H, Vedral V, Aspelmeyer M and Zeilinger A 2005 *Nature* **434** 169
[30] Prevedel R, Walther P, Tiefenbacher F, Böhi P, Kaltenbaek R, Jennewein T and Zeilinger A 2007 *Nature* **445** 65
[31] Chen K, Li C-M, Zhang Q, Chen Y-A, Goebel A, Chen S, Mair A and Pan J-W 2007 *Phys. Rev. Lett.* **99** 120503
[32] Vallone G, Pomarico E, Martini F D and Mataloni P 2008 *Phys. Rev.* A **78** 042335
[33] Tokunaga Y, Kuwashiro S, Yamamoto T, Koashi M and Imoto N 2008 *Phys. Rev. Lett.* **100** 210501
[34] Bell B, Tame M, Clark A, Nock R, Wadsworth W and Rarity J 2013 *New J. Phys.* **15** 053030
[35] Collins M, Xiong C, Rey I, Vo T, He J, Shahnia S, Reardon T K C, Steel M, Clark A and Eggleton B 2013 *Nat. Commun.* **4** 2582
[36] Megidish E, Halevy A, Shacham T, Dvir T, Dovrat L and Eisenberg H S 2013 *Phys. Rev. Lett.* **110** 210403
[37] Barrett S and Stace T M 2010 *Phys. Rev. Lett.* **105** 200502
[38] Lita A E, Miller A J and Nam S W 2008 *Opt. Express* **16** 3032
[39] Marsili F, Verma V B, Stern J A, Harrington S, Lita T G A E, Vayshenker I, Baek B, Shaw M D, Mirin R P and Nam S W 2013 *Nat. Phot.* **7** 210