Classical multiparty computation using quantum resources

Citation for published version:
Clementi, M, Pappa, A, Eckstein, A, Walmsley, IA, Kashefi, E & Barz, S 2017, 'Classical multiparty computation using quantum resources', Physical Review A, vol. 96, 062317.
https://doi.org/10.1103/PhysRevA.96.062317

Digital Object Identifier (DOI):
10.1103/PhysRevA.96.062317

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Physical Review A

Classical multiparty computation using quantum resources

Marco Clementi,[1,2] Anna Pappa,[3,4] Andreas Eckstein,[1] Ian A. Walmsley,[1] Elham Kashefi,[3,5] and Stefanie Barz[1,6]
[1]*Clarendon Laboratory, Department of Physics, University of Oxford, Oxford OX1 3PU, United Kingdom*
[2]*Department of Physics, University of Pavia, Pavia 27100, Italy*
[3]*School of Informatics, University of Edinburgh, Edinburgh EH8 9AB, United Kingdom*
[4]*Department of Physics & Astronomy, University College London, London WC1E 6BT, United Kingdom*
[5]*LIP6 - CNRS, Université Pierre Et Marie Curie, Paris 75005, France*
[6]*Institute for Functional Matter and Quantum Technologies and Center for Integrated Quantum Science and Technology IQST, University of Stuttgart, Stuttgart 70174, Germany*

(Received 23 June 2017; published 18 December 2017)

In this work, we demonstrate a way to perform classical multiparty computing among parties with limited computational resources. Our method harnesses quantum resources to increase the computational power of the individual parties. We show how a set of clients restricted to linear classical processing are able to jointly compute a nonlinear multivariable function that lies beyond their individual capabilities. The clients are only allowed to perform classical XOR gates and single-qubit gates on quantum states. We also examine the type of security that can be achieved in this limited setting. Finally, we provide a proof-of-concept implementation using photonic qubits that allows four clients to compute a specific example of a multiparty function, the pairwise AND.

DOI: 10.1103/PhysRevA.96.062317

I. INTRODUCTION

The ability to communicate and perform computations between parties in a network has become the cornerstone of the modern information age. As more parties with limited resources become connected in wide-scale distributed systems, a critical need is to develop efficient protocols for multiparty computations (MPC), both in terms of communication load and computing capability [1–4].

One approach to efficiently performing MPC is by exploiting quantum resources. It has been shown that measurements on specific types of entangled states (GHZ states [5]), when controlled by a linear computer, are sufficient to compute nonlinear universal functions [6]. Based on that result, it has been demonstrated that MPC under specific assumptions (use of a trusted party, restricted adversaries) is secure, by virtue of the quantum correlations of a GHZ state [7]. Similar results have recently been shown in a client-server scenario, where a client restricted to linear (XOR) operations is enabled to securely delegate the computation of a universal Boolean function to a quantum server [8,9]. The idea behind all these protocols is to use quantum resources in order to compute classical functions more efficiently, without having to build a fully fledged quantum computer.

In this work, we propose a way of computing nonlinear multivariable functions using only linear classical computing and limited manipulation of quantum information. We examine the scenario where a number of clients want to jointly compute a Boolean function of their inputs. We consider that the clients have limited computing capabilities, namely access to linear (XOR) functionalities. We show how quantum resources can enable such limited clients to securely compute nonlinear functions, the complexity of which lies beyond their computing capability. Since access to XOR gates alone is not sufficient for universal classical computing, the clients' computational power is enhanced by means of manipulation of quantum resources provided by a server.

To demonstrate this boost of computational capabilities using quantum resources, we will focus on a particular example of classical nonlinear multiparty computation (the pairwise AND function) that requires as little as one single qubit of communication between the clients. Because of the low quantum communication cost required for the evaluation of this function, the proposed protocol can be used as a building block for more complex computations.

The basic idea of our approach is shown in Fig. 1. A quantum server generates a single qubit that is sent through a chain of clients. Each of the clients applies a rotation on the received quantum state according to their classical input. The quantum state is then sent back to the server, which performs a measurement to obtain the result of the computation. Our protocol is designed in such a way that the input of each client remains hidden from the other clients and from the server. Furthermore, the result of the computation remains hidden from the server and is sent back to the clients in an encrypted fashion, meaning that the server performs the computation without learning anything about the result.

II. THEORY

Our aim is to compute a nonlinear Boolean function $f(x_1,\dots,x_n)$ on input bits $x_i \in \{0,1\}$. We focus on a particular example of a basic multivariable Boolean function, the pairwise AND:

$$f(x_1,\dots,x_n) = \bigoplus_{j=1}^{n}\left[x_{j+1} \times \left(\bigoplus_{i=1}^{j} x_i\right)\right]. \tag{1}$$

The addition and multiplication are the XOR operation and the logical AND operation respectively over the field $\mathbb{F}_2$. If the function in Eq. (1) was linear, then a change in the assignment of one of the variables would either always change the value of the function or would never change it. However, it is easy to verify that the function at hand does not follow this rule, and as a nonlinear function, it cannot be computed using only

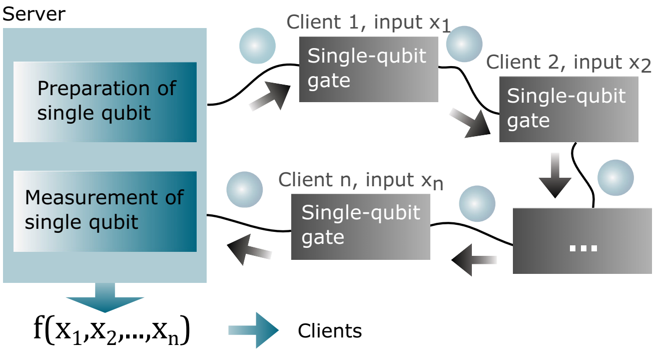

FIG. 1. A sketch of our scheme for multiparty computation, where a server computes a Boolean function $f(x_1,x_2,\dots,x_n)$ with inputs x_i from different clients. The server generates simple computational resources, such as single qubits, and sends them consecutively to a number of different clients. Each client manipulates the computational resources by performing single-qubit gates. At the end, the server measures the output state. The result of this measurement is sent to the clients, who can deduce the result of the computation.

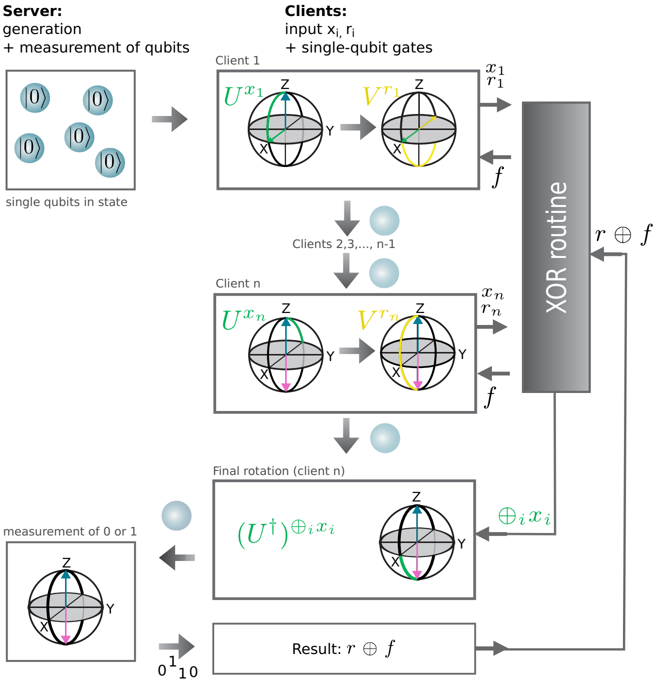

FIG. 2. Protocol for delegated multiparty computation. For a description of the protocol, see the main text.

linear operations in $\mathbb{F}_2$, such as XOR, but necessitates the use of nonlinear operations like NAND.

Now let us define by $U = R_y(\pi/2)$ the rotation around the y axis of the Bloch sphere (i.e., $R_y(\theta) = e^{-i\theta\sigma_y/2}$). Then the following equation can be used to compute the function $f = f(x_1,\dots,x_n)$ in Eq. (1):

$$(U^\dagger)^{\oplus_i x_i} U^{x_n} \dots U^{x_2} U^{x_1} |0\rangle = |f\rangle. \qquad (2)$$

The fact that Eq. (2) uses only linear processing and operations on a single qubit to compute a nonlinear function demonstrates the computational power that quantum resources can provide. Equation (2) can also be thought of in the clients-server setting described in Fig. 1, where each client C_i has an input bit x_i and performs an operation on the received qubit before forwarding it to the next client. By adding extra rotations $V = R_y(\pi)$ around the y axis, we can transform Eq. (2) in the following way:

$$(U^\dagger)^{\oplus_i x_i} \underbrace{V^{r_n}U^{x_n}}_{C_n} \dots \underbrace{V^{r_2}U^{x_2}}_{C_2} \underbrace{V^{r_1}U^{x_1}}_{C_1} |0\rangle = |r \oplus f\rangle, \qquad (3)$$

where $r_i \ \in \{0,1\}$ for $i = 1,\dots,n$ and $r = \bigoplus_i r_i$. As we will see in the following sections, this extra V operation will provide some layer of security on top of the computational boost of the clients' power, in the case where there are dishonest participants.

A. The protocol

The server generates a single qubit in the state $|0\rangle$ that is sent to client C_1. C_1 applies $V^{r_1}U^{x_1}$ on the received qubit, according to input bit x_1 and a randomly selected bit r_1 and sends the qubit on to the second client C_2, who applies $V^{r_2}U^{x_2}$; this procedure continues until all the clients have applied their gates to the qubit (see Fig. 2). The last operation $U^\dagger$ depends on the global XOR of the clients' inputs, computed using a classical routine described below, and can be applied by any client. The resulting state $|r \oplus f\rangle$ contains the value of the function up to a random bit flip r [due to Eq. (3)].

The qubit is then sent back to the server where a measurement is performed in the computational basis and announces the outcome $r \oplus f$. The clients then locally compute the XOR of the random bits of the other clients and perform the last XOR operation $f = r \oplus (r \oplus f)$ to retrieve the result of the computation.

For the computation of the global XOR of both the inputs and the random bits, we consider that the clients run a classical routine that involves using their local XOR boxes to share their classical information among them. During the XOR routine, we assume that the clients communicate between them via secure classical channels that have been established by classical or Quantum Key Distribution (QKD) algorithms.

B. The XOR routine

For $i,j = 1,\dots,n$, each client C_j uses his local XOR box to choose random bits $x_j^i, r_j^i \in \{0,1\}$, such that $x_j = \bigoplus_{i=1}^n x_j^i$ and $r_j = \bigoplus_{i=1}^n r_j^i$ and sends x_j^i and r_j^i to client C_i. Each client C_i then uses his local XOR box to compute $\tilde{x}_i = \bigoplus_{j=1}^n x_j^i$ and $\tilde{r}_i = \bigoplus_{j=1}^n r_j^i$. When the designated client needs to perform the operation $U^\dagger$, the rest of the clients send $\tilde{x}_i$ to that client, who uses his local box to compute the global XOR (since $\bigoplus_{i=1}^n x_i = \bigoplus_{i=1}^n \tilde{x}_i$).

At the end of the protocol, when the server announces the value of the measurement $r \oplus f$, all clients broadcast $\tilde{r}_i$, so that all clients can compute the value r. Of course, a sequential announcement of the clients will give the last client the ability to learn the output of the computation first and then abort the protocol. More complicated ways of secret-sharing values and broadcast channels using threshold schemes could be used instead, but that would defeat the purpose of this paper, which is to show how simple manipulation of quantum states can boost the computational power of limited clients.

C. Security

As mentioned, the goal of this work is to demonstrate how quantum information can increase the computational abilities of parties in a client-server setting; however, the introduction of V rotations in Eq. (3) allows for some level of security in a passive adversarial model. More explicitly, we assume that both the server and the clients are interested in completing the computation, and will therefore act according to the protocol; they might, however, leak some information to an attacker that gains access to their records. We therefore assume that the server sends $|0\rangle$ single-qubit states during the protocol, and no multiple copies of the same qubit or parts of entangled states, but might leak the classical result of the measurement to an eavesdropper. The need to use single copies of quantum states in our protocol is also what distinguishes this work from the previous single-client single-server protocol [9], where using *cobits* (i.e., systems capable of being in a coherent superposition of two states) was sufficient for secure classical computing.

The privacy of the secret input bits of the clients is maintained against someone who acquires a copy of the server's data, since all information that the latter can retrieve is equivalent to the sequence of gates applied, which is in turn equal to $V^{r\oplus f}$. Since the term in the exponent represents padded information, the server cannot retrieve more information than that contained in $r \oplus f$, which is indeed the expected outcome of measurement.

Furthermore, security against dishonest clients is also maintained, even if we allow them to prepare quantum states and perform measurements on the received states. This is again due to the V rotation that is chosen uniformly at random and performed by all honest clients on the qubit. To see this more clearly, we examine the case when the first honest client in the chain, C_i, applies his rotation on the received qubit. We can assume without loss of generality that the qubit is prepared by the dishonest clients in the XZ plane, since all rotations by the honest clients are done on that plane, and therefore any component outside the plane will not be affected. The honest operation on any pure state $|\psi\rangle$ on the XZ plane results in the totally mixed state

$$\frac{1}{2}\sum_{r_i} V^{r_i} U^{x_i} |\psi\rangle\langle\psi| (U^\dagger)^{x_i} (V^\dagger)^{r_i} = U^{x_i} \mathbb{I}_2 (U^\dagger)^{x_i},$$

which ensures that no information is leaked to the next clients. As in the case of the server, however, we need to restrict the clients' malicious behavior to sending single qubit states or equivalently that the honest rotation is done on one qubit. Finally, the client responsible for the last $U^\dagger$ rotation will unavoidably learn the parity of the inputs of the rest of the clients, but as long as at least two clients are honest, it is enough to guarantee the secrecy of the independent inputs.

D. Efficiency and comparison to previous protocols

A common way to perform multiparty computations is via expressing the desired circuits as a sequence of smaller gates, for example two-input universal gates. Previous work [8] can therefore be reinterpreted as a protocol that computes the NAND of the inputs of two clients. However, a straightforward extension of this to a multivariable function would prove very costly, requiring one qubit, up to two R_y rotations, and several rounds of classical communication to compute the necessary XORs, for each AND evaluation in the function. By just looking at the quantum communication needed in the new protocol (which requires a single qubit to compute the pairwise AND), we observe an immediate gain in efficiency. Furthermore, a straightforward implementation of a construction based on [8] guarantees no security for the inputs of the parties, since the XORs necessary for the application of $U^\dagger$ are on two bits; therefore, the client who performs the latter unavoidably learns the input of the other client.

Finally, previous studies of Boolean function evaluation in the measurement-based quantum computation model [10] required an $(n+1)$-extended GHZ state to compute the pairwise AND function of Eq. (1) while to compute other Boolean functions (i.e., n-tuple AND function), the resource state should have $2^n - 1$ qubits. In contrast, the presented protocol does not require any entanglement in the quantum state and uses only one qubit to compute the pairwise AND function, while for the n-tuple AND function, it requires at most $n-1$ qubits (one qubit for each AND operation), giving an exponential decrease on the number of qubits used.

III. EXPERIMENT AND RESULTS

We implement the protocol using polarization-encoded photonic qubits with $|0\rangle$ ($|1\rangle$) being the horizontal (vertical) polarization state. Single photons are generated by pumping a waveguided periodically poled potassium titanium oxide phosphate crystal with a mode-locked Ti:sapphire laser ($\tau =$ 200 fs, $\lambda =$ 775 nm, 250 kHz repetition rate). After spectral filtering, we obtain pairs of photons at 1547 nm (horizontal polarization) and 1553 nm (vertical polarization), each with 2-nm spectral bandwidth (FWHM). The photons are detected using InGaAs avalanche photodetectors (APD) [11,12].

Using this source, the server generates heralded single photons in state $|0\rangle$ which are sent to the clients' side via 15-m-long polarization-maintaining (PM) fibers. Each client $\mathcal{C}_i$ has access to a series of half-wave plates (HWPs) for implementing the quantum gates U^{x_i} and V^{r_i} (see Fig. 3):

$$C_i = U_{HWP}\Big(\frac{\pi}{4} r_i\Big) U_{HWP}\Big(-\frac{\pi}{8} x_i\Big), \tag{4}$$

where $U_{HWP}(\theta)$ is a HWP with optical axis rotated by θ. In order to demonstrate all the features of function f, we choose to implement a setup with four clients. This could be easily extended straightforwardly to a scheme with an arbitrary number of clients. The overall unitary evolution of the system is then described by the following sequence of operators:

$$\underbrace{U_{HWP}(0) U_{HWP}\Big(\frac{\pi}{8} \oplus_i x_i\Big)}_{\text{final rotation}} \underbrace{C_4 C_3 C_2 C_1}_{\text{client chain}} |0\rangle, \tag{5}$$

up to a global phase factor. For the purpose of our demonstration, $U_{HWP}(0)$ can be omitted as it has no effect on the correctness of the demonstration.

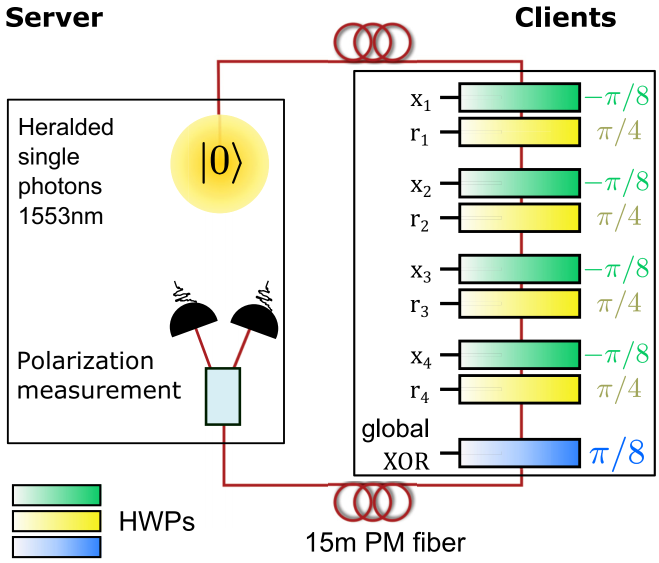

FIG. 3. Experimental scheme. The server generates heralded, horizontally polarized photons, which are sent to the clients' side. Each client uses a pair of half-wave plates for applying the gates V^{r_i} and U^{x_i}. If x_i or r_i are equal to zero, the setting of the respective half-wave plate is chosen to be zero. If x_i or r_i are equal to one, the corresponding half-wave plate is rotated by an angle θ with respect to the horizontal polarization state, where θ is given in the figure. Finally, one of the clients performs a final conditional rotation dependent on $\oplus_i x_i$. The photon is sent back to the server, where a measurement in the computational basis is performed; this has been implemented using a Wollaston prism and two single-photon Avalanche photodiodes (APDs).

Finally, single photons are coupled into another PM fiber and sent back to server. Here, they are measured in the computational basis using a polarization splitter (extinction ratio >60 dB) and two APDs connected to the output arms.

We performed measurements on all possible 32 sequences of the input bits x_i. For each sequence, all possible combinations of the padding bits r_i have been tested. Figure 4(a) shows statistics of the results for a subset of input configurations. The average probability of finding the correct result was measured (99.53 ± 0.03)%, where we assumed Poissonian statistics for the errors. Imperfections arise from state preparation, polarization manipulation and polarization measurements, and darks counts. Figure 4(b) shows results for the same input, but averaged over all combinations of random bits r_i, resulting in a flat distribution. The values we obtain for the average outcome of the computation lie between (49.95 ± 0.03)% and (50.06 ± 0.03)% with an average of (50.00 ± 0.03)%. These values are computed from the raw counts corrected by the coupling efficiencies. This shows that the server could not infer any information from the outcomes of its measurements. The main limiting factors in the correctness of the result are the uncertainty in wave-plate positioning and polarization crosstalk introduced by PM fiber connectors.

Figure 4(c) shows the long-time stability of our system: We repeated the same computation several times over a time interval of 13 h and studied drift in our experiment. The average correctness over this time was 99.43% with a standard deviation of 0.08%. The correctness decreases from (99.52 ±0.02)% to (99.27 ±0.06)%; the drop in probability is caused by drifts in the coupling to the fibers and polarization drifts.

Security of implementation

In addition to the theoretical security aspects discussed above, in our implementation we choose the wave-plate

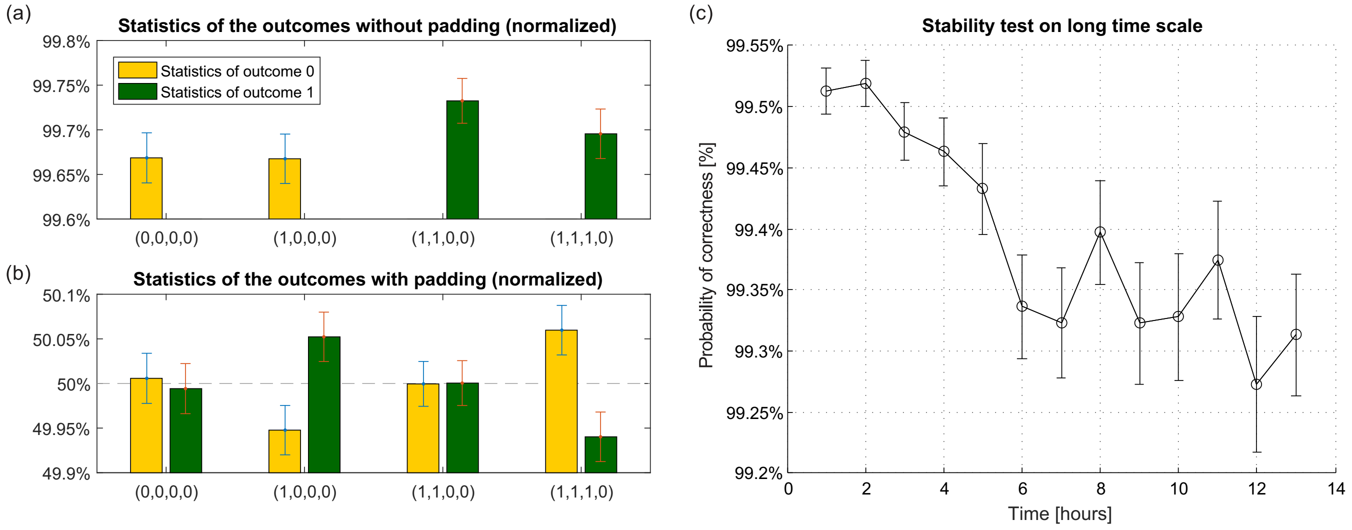

FIG. 4. (a) Measured outcomes of the computation after decoding $r \oplus (r \oplus f)$ for a sample subset (x_1,x_2,x_3,x_4) of the input bits tested (horizontal axis). (b) Measured outcomes of the computation before decoding $(r \oplus f)$, averaged over all possible combinations of r_i, $i = 1,\ldots,4$. For each data point, we integrated over 15 s, yielding an overall statistics of about 3000 counts for each computation performed. (c) Long-term stability of our experiment. The graph shows the probability of obtaining the correct outcome measured over 13 h of data acquirement. Every point of the plot corresponds to the average over 1 h of measurement time. The combination of the clients' input bits used here is $(x_1,x_2,x_3,x_4) = (1,1,1,1)$.

settings in such a way that there is no phase shift between the states $|0\rangle$ and $|1\rangle$ that could leak information about the inputs. As already discussed in Ref. [9], global phase shifts could leak information if the server, for example, sends part of an entangled state. However, this approach would require an interferometrically stable setup, which is an unlikely condition for a real-life implementation. Furthermore, the protocol requires the use of single qubits and a single-shot implementation in order to be secure. For the purpose of computing statistics for our proof-of-principle demonstration, we averaged over several runs of the experiment that used the same input settings. We note, however, that this would leak information about the inputs or the result to a malicious party; therefore in a realistic implementation, single-shot experiments would be required.

IV. CONCLUSION

In general, linear function evaluation is considered efficient and requires no prior shared randomness between the clients, while nonlinear function evaluation requires such resources, which increases the communication and computation cost. In this work, we demonstrate a way to perform nonlinear classical multiparty computation without any such requirements, by exploiting single qubits and access to restricted linear processes. This is done through studying a specific Boolean function that can be thought of as a building block for more complex computations.

Even though the main focus of this work is the boosting of the computational capabilities of limited clients manipulating single qubits, by introducing some extra rotations we can guarantee security under assumptions on the adversarial behavior of the participants. This holds even in a realistic setting where the noise in the system necessitates repetition of the protocol for a single computation, since the rotations are chosen uniformly at random in each repetition. In this setting, the classical data obtained during the protocol do not leak any information, given that the adversaries act in a restricted way. Since the goal was to keep the clients' quantum capabilities as limited as possible, it would defeat the purpose of this study to allow them to perform any check on the correct behavior of the server or the other clients. If we would consider a setting where the clients are enhanced with quantum measurement devices, security of the protocol could be increased by checking the mean photon number (however, see Ref. [13] for a discussion on attacks and countermeasures on commercial devices).

Our work also offers many avenues for further research. For example, are there more simple nonlinear functions like the one presented here that can be used as subroutines for larger computation protocols? And more generally, what is the most efficient way to perform complex computations when we have access to limited quantum and classical resources? Finally, surprisingly enough, this boosting of computational power is possible with the use of single qubits, and without the need of the type of contextuality mentioned in Ref. [14], opening a discussion on whether some other form of contextuality is relevant in this setting.

ACKNOWLEDGMENTS

The authors would like to thank Shane Mansfield for very useful suggestions during the development of the theory and Alex E. Jones for comments on the paper. M.C. acknowledges support from the Erasmus+ programme; A.P. acknowledges support from EPSRC Grant No. EP/M013243/1 and from the European Union's Horizon 2020 Research and Innovation program under Marie Sklodowska-Curie Grant Agreement No. 705194. I.A.W. acknowledges an ERC Advanced Grant (MOQUACINO) and the UK EPSRC Project No. EP/K034480/1. E.K. acknowledges funding through EPSRC Funds No. EP/N003829/1 and No. EP/M013243/1. S.B. acknowledges support from the Marie Curie Actions within the Seventh Framework Programme for Research of the European Commission, under the Initial Training Network PICQUE (Photonic Integrated Compound Quantum Encoding, Grant Agreement No. 608062), from the European Union's Horizon 2020 Research and Innovation program under Marie Sklodowska-Curie Grant Agreement No. 658073 and from the Carl Zeiss Foundation.

[1] A. C. Yao, in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, *SFCS '82* (IEEE Computer Society, Washington, DC, USA, 1982), pp. 160–164.

[2] I. Damgård, in *Proceedings of the 5th International Conference on Security and Cryptography for Networks, SCN '06* (Springer, Berlin, 2006), pp. 360–364.

[3] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft, in *Proceedings of the 13th International Conference on Financial Cryptography and Data Security*, *FC '09* (Springer, Berlin, 2009), pp. 325–343.

[4] J. Saia and M. Zamani, in *Proceedings of the 41st International Conference on Current Trends in Theory and Practice of Computer Science* (Springer, Berlin, 2015), pp. 24–44.

[5] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Going beyond Bell's theorem, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), pp. 73–76.

[6] J. Anders and D. E. Browne, Phys. Rev. Lett. **102**, 050502 (2009).

[7] K. Loukopoulos and D. E. Browne, Phys. Rev. A **81**, 062336 (2010).

[8] V. Dunjko, T. Kapourniotis, and E. Kashefi, J. Quantum. Inform. Comput. **16**, 0061 (2016).

[9] S. Barz, V. Dunjko, F. Schlederer, M. Moore, E. Kashefi, and I. A. Walmsley, Phys. Rev. A **93**, 032339 (2016).

[10] M. J. Hoban, E. T. Campbell, K. Loukopoulos, and D. E. Browne, New J. Phys. **13**, 023014 (2011).

[11] A. Eckstein, A. Christ, P. J. Mosley, and C. Silberhorn, Phys. Rev. Lett. **106**, 013603 (2011).

[12] G. Harder, V. Ansari, B. Brecht, T. Dirmeier, C. Marquardt, and C. Silberhorn, Opt. Express **21**, 13975 (2013).

[13] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015).

[14] R. Raussendorf, Phys. Rev. A **88**, 022322 (2013).