# Deliverable Report

## Deliverable No: D7.1

## Deliverable Title: Development and classification of HQC based on non-adaptive linear optics

**Grant Agreement number: 899544**

**Project acronym: PHOQUSING**

**Project title: PHOtonic Quantum SamplING machine**

**Project website address: www.phoqusing.eu**

**Name, title and organisation of the scientific representative of deliverable's lead beneficiary (task leader):**
Prof. Ernesto F. Galvão, LIN INL

**Deliverable table**

| | |
|---|---|
| **Deliverable no.** | D7.1 |
| **Deliverable name** | Development and classification of HQC based on non-adaptive linear optics |
| **WP no.** | 7 |
| **Lead beneficiary** | LIN INL |
| **Type** | Report |
| **Dissemination level** | Public |
| **Delivery date from Annex I** | M12 |
| **Actual delivery date** | 31 August 2021 |

***What was planned*** *(from Annex I:)*
**D7.1: Development and classification of HQC based on non-adaptive linear optics [M12]**
Description: Report mapping the requirements for initial, proof of principle demonstrations of hybrid quantum computation (HPC) applications suitable for non-adaptive, photonic quantum sampling machines: Monte Carlo integration, Max-Haf approximate optimization, identification of dense subgraphs. Classification of tasks with the resources necessary for proof-of-principle demonstrations: amount and accuracy of squeezing parameter in inputs, complexity of the linear interferometer design, postselection overhead, number of different devices required (alternatively, the desired level of parameter tunability).

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION
HORIZON 2020

**What was done.**

## 1 Introduction

In this report we investigate the feasibility of some hybrid quantum computation (HQC) tasks that are suitable for implementation using non-adaptive linear optics, in particular programmable interferometers with inputs consisting of either Fock states or Gaussian states. These HQC tasks are candidates for implementation using the devices in development as part of the PHOQUSING project. In section 2 we describe applications using Fock-state inputs, with Gaussian state inputs in section 3. In section 4 we point out some promising alternatives to investigate in the future and offer some concluding remarks.

## 2 HQC using Fock-state inputs

With Fock-state inputs comprising a total of $n$ photons, the probability amplitudes of output events are a function of the permanents of $n$ $x$ $n$ submatrices associated with the interferometer design, as described in [Aaro11]. Calculating the permanent, even approximately, is a problem known to be in the #P-hard computational complexity class, and this fact is the basis for the hardness of simulation of these processes. Using random interferometer designs and particular choices for the scaling between number of photons $n$ and number of modes $m$, this motivated quantum computational advantage experiments generically called Boson Sampling, after the original proposal by Aaronson and Arkhipov [Aaro11]. In this section, we will focus on the first applications we have identified as promising for hybrid quantum computation using this set-up: quantum Bernoulli factories, variational quantum cloning machines, and verification of solutions of NP problems.

### 2.1 Quantum Bernoulli factories

In a classical framework, Bernoulli factories are a set of protocols associated to a function $f$ that take as input a sample obtained from a Bernoulli process with arbitrary (unknown) parameter $p$, and provide as output a sample obtained from a Bernoulli process with parameter $f(p)$. Such a problem has been completely theoretically characterized in [Kean94], by identifying the exact set of functions that can be constructed from a classical coin. In particular, it has been shown that there are set of functions which cannot be classically implemented, a prominent example being provided by the wedge function $f_W(p) = \min\{2p, 2(1-p)\}$ that has a relevant application for Markov processes.

Recently, it has been proposed to extend such a framework to the quantum domain. A first proposal relies on what is called "quantum-to-classical" Bernoulli factories, where the input coin is replaced by a quantum system, while the output is still represented by a classical Bernoulli process. More specifically, quantum-coins are provided by pure states, which after measurement in the computational basis provide a classical output associated to a Bernoulli process. Quantum-to-classical Bernoulli factories are constructed to perform appropriate operations on the quantum coins before the measurement, which yields a classical output that can be processed by a classical Bernoulli factory. Quantum coins enable access to a larger set of transformations, allowing transformations to functions $f$ not accessible to classical Bernoulli factories. In particular, in [Dale15] the complete set of functions that are enabled by such a quantum extension was characterized, showing also that the only required quantum operation in such framework is the capability of performing measurements in different bases, while no entangled measurements are strictly necessary. Recent experiments have reported the implementation of such a paradigm. In particular, in Ref. [Yuan16] a quantum-to-classical Bernoulli factory has been implemented by using superconducting qubits in the single-qubit regime, allowing for the implementation of the wedge function $f_W$ defined above. Similar results have been also obtained with photonic systems in [Pate19] by using polarization-encoded qubits, with an added analysis of the method's robustness.

The second extension, called a "quantum-to-quantum" Bernoulli factory, provides a further generalization by considering that both input and outputs are quantum coins (or qubits). In this way, the output state can be further used in quantum computation, allowing this randomness-processsing protocol to be a sub-routine in a larger computation. Theoretically, the class of functions associated to these processes have been characterized [Jian18]. However, proposals for experimental schemes as well as experimental demonstrations in the full quantum-to-quantum domain are currently very restricted. In particular, in the literature there is no experimental scheme available that can implement a general Bernoulli factory [Zhan20, Liu20]. Indeed, while schemes performing single operations (sum, product, inverse) are available, no approach reported up to now permits concatenations of sequences of operations. The latter is a crucial requirement to fulfil the full set of functionalities theoretically identified in [Jian18].

Under the PHOQUSING project the nodes UNIROMA1, CNR, and LIN INL plan to develop and implement an experimental scheme for quantum-to-quantum Bernoulli factories based on the hardware developed within the project. The main aspect will represent the demonstration of the possibility of concatenating a sequence of operations. The first implementation will foresee the concatenation of two operations, while the scheme will be shown to be applicable for an arbitrary number of layers. Furthermore, we will provide a detailed investigation of the success probability of the scheme, to verify scalability for larger number of qubits.

## 2.2 Variational quantum cloning machines

A variational algorithm for quantum cloning was proposed recently in [Coyl20]. The basic idea is to use variational machine learning techniques to find near-optimal parameterized circuits for various quantum cloning tasks, with applications to attacks on quantum coin-flipping and key distribution protocols. The cloning tasks considered included universal and covariant quantum cloning, as well as cloning from a set of known quantum states. Besides the theoretical analysis and numerical results, the original paper [Coyl20] also implemented versions of these algorithms run on the superconducting quantum processing unit (QPU) Aspen-8 by Rigetti Computing. We identified this as an interesting application to consider for PHOQUSING's projected photonic devices. In this section we report some preliminary results, obtained by a collaboration between the INL and Sorbonne nodes of PHOQUSING. These were part of the Bachelor's thesis of student Sebastià Nicolau Orell, co-supervised in 2021 by project partners Elham Kashefi (Sorbonne) and Ernesto Galvão (INL).

The first possibilities that were investigated involved parameterizing general 4- and 6-mode linear-optical interferometers, for experiments using two or three single photons (in dual-rail encoding). Appropriate cost functions were defined, using the fidelity of the clones as the key metric to optimize. We obtained 1-to-2 qubit universal quantum cloning machines, and 1-to-2, 1-to-3 phase-covariant cloning machines with near-optimal fidelities.

In Fig. 1 (left panel) we report the clone fidelities as a function of the number of training steps, for 1-to-2 cloning and 6 modes. On the right we show the fraction of events discarded by post-selection, due to the photons having left the dual-rail encoding, something we detect at the output.

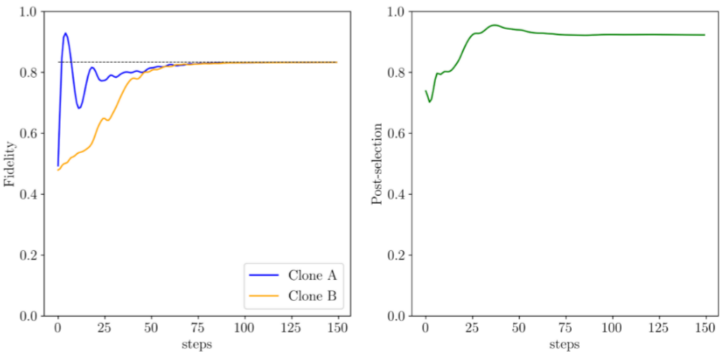

*Figure 1 1-to-2 qubit universal cloning using dual-rail encoding in 6 modes. Clone fidelity (left) and fraction of events discarded at post-selection (right), as a function of the number of training steps.*

It is worth noting some characteristics of these first implementations that are specific to the photonic platform. The photonic optimization/learning was done directly using the physical platform’s parameters, i.e. phase shifters and beam-splitters. We introduced a more efficient learning procedure that uses Pauli eigenstates only, as opposed to uniformly drawn pure states – this resulted in faster learning due to the 2-design properties of Pauli eigenstates [Amba07]. Finally, the postselection cost can be included in the cost function, which is appropriate for photonic implementations of dual-rail qubits. We have experimented with that, as well as with using smaller photonic circuits, obtaining good results for 1-to-2 universal cloning machines with only two dual-rail qubits (it is known that 3 qubits are necessary for optimal cloning fidelities). These lessons could be useful for other hybrid quantum computation schemes based on photonic devices.

The preliminary investigations briefly described in this section were done using classically-simulated photonic circuits of the type under development in PHOQUSING, and the open-source package Strawberry Fields, developed by Canadian company Xanadu. We aim to extend this approach by experimenting with cryptographic applications, and other variational quantum algorithms, as they are suited to small-depth circuits with limited photon numbers.

### 2.3 Verification of solutions of NP-hard problems under communication restrictions

Computational problems in the complexity class NP have solutions that can be efficiently verified, even if finding them may be computationally hard. NP-hard problems are important for a multitude of applications, from graph theory and bio-informatics to optimization. If not enough information about the solution of an NP problem is revealed, the verification can instead take exponential time on a classical computer. In [Aaro08], this result on the limitation of the information about the solution to NP problems was shown to result in a setting where quantum computers can have a computational advantage. More precisely, for a problem of size *N*, if an encoding of a solution uses *O(sqrt(N)log(N))* bits, the classical verification will take exponential time. Interestingly, quantum encodings of a solution of that same size allows for an efficient (polynomial-time) verification by a quantum computer. This means verifying the solution to NP-hard problems, under a constraint in the amount of information that is made available about the solution is a natural setting where quantum computers can have an exponential advantage over classical computers. It was argued in [Arra18b] that the restriction on the information made available about the solution may be justified in some situations due to privacy concerns in a cryptographic setting.

In [Arra18b], it was shown that a linear-optical setup would be sufficient for implementing the quantum version of this verification test, without the need for measurement feed-forward or non-linear optics. The simplest problem to be considered is the 2-out-of-4 satisfiability (SAT) problem, to which the famous 3-SAT problem can be reduced. The simplest linear-optical implementation suggested in [Arra18b] involves a problem of size *N=4*, but with solutions encoded using only *log(3)* bits. It requires 3 single-photon inputs, and a completely programmable 12-mode interferometer, with photodetectors at all output modes.

Recently, a linear-optical implementation of this protocol was demonstrated that uses a different linear-optical setup: attenuated coherent inputs encoded using a phase modulator, a single balanced beam-splitter, and photo-detection [Cent21]. Information on the solution was encoded in the phases of a train of weak coherent pulses with up to N=14000 time-bins. This shows that this task allows for interesting resource trade-offs between different ingredients of this linear-optical set-up, in this case decreasing the number of linear-optical elements from $O(N^2)$ to a constant, at the cost of increasing the complexity of the preparation of input states. Implementation of a variation of these linear-optical implementations of the protocol for testing solutions of NP-hard problems remains in consideration as a possible goal within the PHOQUSING project.

## 3 HQC using Gaussian-state inputs

Gaussian state inputs, together with linear-optical dynamics and photodetection at the output comprise the so-called Gaussian Boson Sampling (GBS) paradigm [Hami17]. In 2020/21 there were two ground-breaking demonstrations of quantum computational advantage using photonic Gaussian Boson Sampling devices [Zhon20, Zhon21], as well as impressive proof-of-principle demonstrations of applications thereof using programmable, integrated photonic hardware of Canadian company Xanadu [Arra21]. Other research has described the use of GBS as a basic building block of a scalable architecture for photonic quantum computation [Bour21].

In this report we review the experimental requirements of the recent photonic HQC demonstrations, and outline the experimental requirements for other applications of Gaussian Boson Sampling.

Gaussian Boson Sampling (GBS) [Hami17] devices use squeezed vacuum (and sometimes, also displaced/squeezed vacuum) to sample from a probability distribution that is proportional to the square of the hafnian of a matrix describing the setup (interferometer and squeezing parameters). The hafnian is related to the permanent, and its computation is also #P-hard (i.e., intractable). It is possible to encode any symmetric matrix into the interferometer, making this a natural way of encoding the adjacency matrix *A* of a graph. Since the probability distribution is proportional to the hafnian of a matrix built from the one describing the interferometer, GBS samples will be biased towards submatrices having high hafnians. Hafnians are functions that count the number of perfect matchings of a graph. Since this correlates with the graph's density [Arra18], as a result the GBS distribution naturally samples from high-density subgraphs of *A*. This realization was formalized in [Arra18c], which defined the Max-Haf problem, proving it is NP-hard by reducing it to the maximal clique problem.

This suggests that GBS samples may be computationally helpful as a source of high-density subgraphs, which can be explored in hybrid quantum/classical algorithms. Finding high-density subgraphs can be crucial in many applications, for example by identifying communities in social networks; interacting proteins in biology; or congestion in communication networks. For a review of graph-theoretical applications of GBS, see [Brom20].

For practical usefulness of GBS in applications, its complexity must scale favourably against the best known classical algorithms for the same tasks. For the case of graph-theoretical applications we describe in more detail below, a recent classical simulation algorithm was proposed that generates approximate samples of GBS-encoded undirected, unweighted graphs in time that is polynomial in the number of graph vertices [Ques20]. This means an asymptotic quantum computational advantage of GBS for problems involving undirected, unweighted graphs, if it exists, can only be polynomial. As we will briefly mention below, this is also the case for a proposal of using GBS for quantum chemistry calculations, for the estimation of Franck-Condon profiles of molecular vibronic spectra [Huh15].

Next we analyse the use of GBS in HQC for different applications, highlighting the experimental requirements of first demonstrations.

### 3.1 Graph similarity

As mentioned above, the adjacency matrix can be encoded in the interferometer of a GBS set-up. It has been shown that two graphs are isomorphic if and only if the GBS probability distributions arising from them is the same, up to a permutation [Brad21]. The GBS probabilities of single events, however, is typically not accessible experimentally, as the possible number of outcomes increases exponentially with the number of modes and average number of photons. To make a GBS-based graph similarity test practical, coarse-grainings of test results were proposed, lumping many different outcomes in single-bins for comparison [Brad21]. Under a particular coarse-graining, each graph will be represented by a feature vector of many components, all of which must have the same values for isomorphic graphs. Comparison of these feature vectors allows to identify not just graph isomorphism but to cluster graphs according to similarity, which may be useful for applications based on graph theory.

Very recently there appeared the first experimental demonstration of a GBS-based graph similarity HQC [Arra21]. It used an 8-mode programmable photonic processor, and Gaussian states with up to 5 detected photons composing a 3-dimensional feature vector. This enabled the characterization of 16, 8-vertex graphs into four clearly separate groups of isomorphic graphs. Note that this task could be easily done visually, and some doubt was expressed with respect to the feasibility of getting a computational speed-up for this problem using GBS. In particular, it was observed that the effect of losses was not studied, and moreover that very good classical heuristics exist to characterize graph similarity, and which are therefore hard to outperform. Despite this negative outlook expressed in the experimental paper, some numerical simulations reported in [Schu20] used simulated GBS data to analyse similarity of graphs with between 6 and 25 nodes from different common datasets, showing GBS has comparable performance to classical approaches in the success rate for classifying graphs, at least using simulated, noiseless GBS devices (at great simulation computational cost).

### 3.2 Dense subgraphs

GBS can also be used to identify dense subgraphs of a given graph, in particular to find maximally-connected subgraphs (cliques). Both primitives are useful for graph-based applications, and as mentioned before, exact solutions for some classes of problems are known to be NP-hard (e.g. finding the highest-density subgraph, or the maximal clique problem). The encoding of the adjacency matrix $A$ of the graph into GBS device is as described before, using both the programmable interferometer and the choice of single-mode squeezing parameters. One experimental limitation is that we need as many modes as there are vertices in the full graph (or twice that number, for the simplest encoding); moreover, the squeezing parameters must be tuned according to the number of vertices of the dense subgraph sought, within limits set by the largest eigenvalue of $A$ (as described in [Brad18]). These limitations make an experimental implementation harder.

A preliminary investigation of this GBS application was done as part of the Master's degree project of student Ana Filipa Carvalho, supervised at University of Minho by Ernesto Galvão. An ensemble *E* of 1000 random 16-vertex graphs was used. Each graph in the ensemble is created from a 12-vertex sub-graph with random edge density 0.2, joined to a 4-vertex complete graph by two randomly picked edges. Each 16-vertex graph was encoded in a GBS device with 16 modes, using Autonne-Takagi decomposition described in [Arra18], which results in the distributions of required single-mode squeezing parameters on the left of Fig. 2. On the right of Fig. 2, we see numerical evidence that GBS samples from a distribution peaked at high-density subgraphs, in comparison with a uniform, classical sampling of 4-vertex subgraphs.

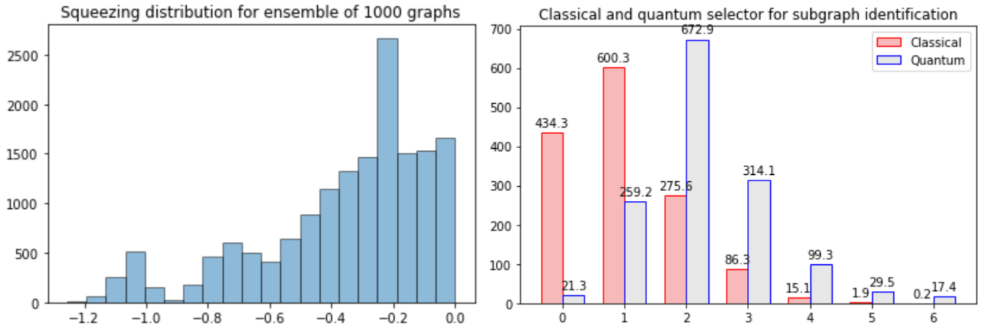

*Figure 2 Left: Distribution of single-mode squeezing parameters in Autonne-Takagi encoding of the ensemble E of graphs into linear-optical interferometers with squeezed-state inputs. Right: Classical versus quantum performance at identifying dense 4-vertex subgraphs of ensemble E. The classical approach consists of picking 4-vertex subgraphs randomly (and uniformly), whereas the quantum approach uses samples from a GBS machine. The x-axis shows number of edges of the 4-vertex subgraphs sampled, showing evidence that GBS has a distribution peaked at high-density subgraphs.*

For these preliminary simulations, we see that the range of squeezing parameters necessary are within experimental reach for GBS experiments with a 16-mode programmable device. A more realistic comparison could include limited accuracy in the squeezing parameters, losses in the interferometer, and comparison against more sophisticated classical algorithms for dense sub-graph sampling.

### 3.3 Simulation of molecular vibronic spectra

In the previous sub-section we reviewed some graph-theoretic applications of GBS, all fundamentally based on the fact that GBS devices sample from a distribution that is proportional to the hafnian of submatrices that describe the device, which correlates with the subgraph's density. Here we briefly describe another type of application of GBS devices, to certain quantum chemistry computations.

The first proposed application of GBS to quantum chemistry was in the evaluation of vibronic molecular spectra [Huh15], more specifically the Franck/Condon profile of transition probabilities using Duschinsky's relation [Dusc37]. In [Arra21] a GBS-based implementation was described to simulate the vibronic spectra of two molecules: ethylene ($C_2H_4$) and (E)-phenylvinylacetylene ($C_{10}H_8$). Even though in general squeezing and displacement of all modes may be necessary for best results, in this implementation no displacement was used, and a single mode featured a squeezed vacuum input (for each block of fully programmable 4-mode interferometers used).

Very recently, it was realized that a polynomial-time algorithm for the same task can be devised, based on efficient simulation of Gaussian states and dynamics, as reported in a yet-unpublished, private communication by J. M. Arrazola [Arra21b], and in the blog post [Aaro20]. Together with the new, state-of-the-art classical simulation algorithm of GBS reported in [Ques20], this cast doubts on whether other HQC applications of GBS to quantum chemistry [Joha20] can offer significant speed-up over approaches that are purely classical, even if quantum-inspired.

## 4 Outlook and perspectives

Gaussian Boson Sampling (GBS) use non-adaptive linear optical interferometers associated with Gaussian state inputs for advantage in hybrid quantum computation (HQC) tasks in graph theory and quantum chemistry. We have mapped the experimental parameters used in the initial experimental demonstrations of such applications (graph similarity, simulation of molecular vibronic spectra), and the requirements for a proof-of-principle demonstration of an algorithm to find dense subgraphs. Recent theoretical developments about classical algorithms for vibrational molecular spectra simulation [Arra21, Aaro20] and graph-theoretical applications [Ques20] put into question whether GBS applications can decisively outperform a purely classical approach. Research into GBS may still reveal interesting applications for NISQ-era photonic computers, perhaps by exploring harder-to-simulate GBS settings corresponding e.g. to the encoding of weighted and/or directed graphs in GBS devices. Thinking in the longer-term, GBS devices are useful building blocks for Gottesman-Kitaev-Preskill (GKP) continuous-variable encodings for qubits [Gott01], as shown in e.g. [Bour21]. This means GBS devices may play an architectural role in the longer-term goal of developing error-corrected, scalable photonic quantum computers.

We have also described recently-proposed applications of non-adaptive linear-optical interferometers using Fock-state inputs. These are some of the initial applications we aim to explore experimentally using the devices developed under the PHOQUSING project:

- Randomness manipulation using quantum-to-quantum Bernoulli factories
- Verification of solutions of NP problems under constraints on the information available
- Quantum learning of photonic cloning machines for cryptographic applications

We expect to refine the understanding of these applications as the project develops, proposing new variations in a back-and-forth interaction between theory and experiment.

## 5. Bibliography

[Aaro08] S. Aaronson et al., in 23rd Annual IEEE Conference on Computational Complexity, 2008. (IEEE, 2008), pp. 223–236.
[Aaro11] S. Aaronson and A. Arkhipov, Proceeding STOC '11 - Proceedings of the forty-third annual ACM symposium on Theory of computing, p. 333-342 (San Jose, California, USA).
[Aaro20] Post in Scott Aaronson’s blog Shtetl-Optimized https://www.scottaaronson.com/blog/?p=5159
[Amba07] A. Ambainis and J. Emerson, in *22nd Annual IEEE Conference on Computational Complexity (CCC'07)*, p. 129 (2007).
[Arra18] J. M. Arrazola and T. R. Bromley, Phys. Rev. Lett. 121, 030503 (2018).
[Arra18b] J. M. Arrazola, E. Diamanti, and I. Kerenidis, npj Quantum Information volume 4, Article number: 56 (2018).
[Arra18c] J. M. Arrazola et al., Phys. Rev. A 98, 012322 (2018).
[Arra21] J. M. Arrazola et al., Nature 591, 54 (2021).
[Arra21b] J. M. Arrazola, private communication (2021).
[Bour21] J. E. Bourassa et al., Quantum 5, 392 (2021).
[Brad18] K. Bradler et al., Phys. Rev. A 98, 032310 (2018).
[Brad21] K. Bradler et al., Special Matrices 9 (1), 166 (2021).

[Brom20] T. R. Bromley et al., Quantum Sci. Technol. 5, 034010 (2020).  
[Cent21] F. Centrone et al., Nature Communications 12, 850 (2021).  
[Coyl20] B. Coyle, M. Doosti, E. Kashefi, N. Kumar. Preprint ArXiv:2012.11424 [quant-ph].  
[Dale15] H. Dale, D. Jennings, T. Rudolph, Nature Commun. 6, 8203 (2015).  
[Dusc37] F. Duschinsky, Acta Physicochim. URSS 7, 551 (1937).  
[Gott01] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A 64, 012310 (2001).  
[Hami17] C. S. Hamilton et al., Phys. Rev. Lett. 119, 170501 (2017).  
[Huh15] J. Huh et al., Nature Photonics 9 (9), 615 (2015).  
[Jian18] J. Jiang, J. Zhang, X. Sun, Phys. Rev. A 97, 032303 (2018).  
[Joha20] S. Jahangiri et al., Phys. Chem. Chem. Phys.22, 25528 (2020).  
[Kean94] M. S. Keane, G. L. O’Brien, ACM Trans. Model. Comput. Simul., 4, p. 213–219 (1994).  
[Liu20] Y. Liu, et al., preprint arXiv:2002.03076 [quant-ph].  
[Pate19] R. B. Patel, T. Rudolph, G. J. Pryde, Sci. Adv. 5, eaau6668 (2019).  
[Ques20] N. Quesada and J. M. Arrazola, Phys. Rev. Research 2, 023005 (2020).  
[Schu20] M. Schuld, K. Brádler, R. Israel, D. Su, and B. Gupt, Phys. Rev. A 101, 032314 (2020).  
[Yuan16] X. Yuan, et al., Phys. Rev. Lett. 117, 010502 (2016).  
[Zhan20] X. Zhan, et al., Phys. Rev. A 102, 0126605 (2020).  
[Zhon20] H.-S. Zhong et al., Science 370 (6523), 1460 (2020).  
[Zhon21] H.-S. Zhong et al., preprint arXiv:2106.15534 [quant-ph].