# Optical implementations, oracle equivalence, and the Bernstein-Vazirani algorithm

Arvind*
*Department of Physics, Indian Institute of Technology Madras, Chennai 600036*†

Gurpreet Kaur
*Department of Physics, IIT Madras, Chennai 600036*

Geetu Narang
*Department of Physics, Guru Nanak Dev University, Amritsar, 143 005*



We describe a new implementation of the Bernstein-Vazirani algorithm which relies on the fact that the polarization states of classical light beams can be cloned. We explore the possibility of computing with waves and discuss a classical optical model capable of implementing any algorithm (on $n$ qubits) that does not involve entanglement. The Bernstein-Vazirani algorithm (with a suitably modified oracle), wherein a hidden $n$ bit vector is discovered by one oracle query as against $n$ oracle queries required classically, belongs to this category. In our scheme, the modified oracle is also capable of computing $f(x)$ for a given $x$, which is not possible with earlier versions used in recent NMR and optics implementations of the algorithm.

PACS numbers: 03.67.Lx,42.25.Ja,42.25.Hz

## I. INTRODUCTION

Quantum mechanical systems have a large in-built information processing ability and can hence be used to perform computations [1, 2, 3]. The basic unit of quantum information is the quantum bit (qubit), which can be visualized as a quantum two-level system. The implementation of quantum logic gates is based on reversible logic and the fact that the two states of a qubit can be mapped onto logical 0 and 1 [4, 5, 6]. The quantum mechanical realization of logical operations can be used to achieve a computing power far beyond that of any classical computer [7, 8, 9, 10]. A few quantum algorithms have been designed and experimentally implemented, that perform certain computational tasks exponentially faster than their classical counterparts. While the Deutsch-Jozsa (DJ) algorithm [11] and Shor's quantum factoring algorithm [12, 13] lead to an exponential speedup, Grover's rapid search algorithm [14] and the Bernstein-Vazirani [15] algorithm are examples where a substantial (though non-exponential) computational advantage is achieved.

The exponential gain in computational speed achieved by quantum algorithms is intimately related to entanglement [16], and it turns out that when there is no entanglement (or the amount of entanglement is limited) in a pure state, the dynamics of a quantum algorithm can be simulated efficiently via classically deterministic or classical random means [17, 18, 19]. However in algorithms that do not lead to an exponential gain in speed or in those that use mixed states, the possibilities of achieving speedup without entanglement still exist [20].

Classical waves share certain properties of quantum systems. For example, the polarization states of a beam of light can act as qubits. It is to be noted that the superposition of classical waves does not lead to entanglement. For $n$ beams of light, with their polarization states providing us with $n$ qubits, we can only implement $U(2) \otimes U(2) \cdots \otimes U(2)$ transformations via optical elements [21] and cannot in general implement $U(2^n)$ transformations. Therefore, although superposition and interference are present and can be utilized, their scope is limited compared to what could be achieved with $n$ qubits which are actually quantum in character. However, it is interesting to explore the question if any useful computation could be performed with classical waves, that exploits their superposition and interference. It turns out that, if an algorithm based on qubits does not involve entanglement at any stage of its implementation, it can be realized using this classical model. The Deutsch-Jozsa algorithm for one and two qubits and the Bernstein-Vazirani algorithm for any number of qubits, can be re-cast in this form with a suitable modification of the oracle [15, 22, 23]. This modification of the algorithm has been central to the implementation of the Deutsch-Jozsa algorithm up to two qubits [24, 25, 26] and the Bernstein-Vazirani algorithm on any number of qubits using NMR [27] as well as optics [28] and superconducting nanocircuits [29].

In this paper, we propose a model based on classical light beams in which the $n$-qubit eigen states are mapped on to polarization states of these beams, and un-entangling unitary operators are implemented using passive optics. An added feature in this model is that cloning of states is possible as we are working entirely within the domain of classical optics. It turns out that this possibility of cloning along with interference leads to interesting results for certain algorithms.

*Electronic address: arvind@quantumphys.org
†Also at: Department of Physics, Guru Nanak Dev University, Amritsar 143005

We discuss an entirely new scheme for implementing the Bernstein-Vazirani algorithm. Instead of Hadamard transformations, we use cloning and re-interference to discover a hidden $n$-bit binary vector $a$, using only a single oracle call. The non-entangling nature of the modified oracle for the Bernstein-Vazirani algorithm is central to this implementation as it is for the earlier implementations [27, 28]. However this scheme differs from the earlier schemes in two ways: (a) instead of Hadamard transformation we use the cloning of classical beams via beam splitters, and (b) we are able to operate the modified oracle in the 'classical' mode as well, wherein we are able to obtain $f(x)$ for a given $x$.

The material in this paper is arranged as follows: the optical model based on polarization states is described in Section II. Section III begins with the description of the original Bernstein-Vazirani algorithm and later discusses the modified oracle and its implications. The new optical scheme is described in Section IV and Section V has some concluding remarks.

## II. OPTICAL IMPLEMENTATION BASED ON POLARIZATION

Consider a classical system consisting of a monochromatic light beam propagating in a given direction with a pure polarization. The polarization states of such a beam are in one-to-one correspondence with the states of a two-level quantum system and the beam can therefore be visualized as a qubit. The unitary transformations that transform one polarization state to another can be easily performed. Consider a birefringent plate with its thickness adjusted to introduce a phase difference of $\eta$ between the $x$ and $y$ components of the electric field, with its slow axis making an angle $\phi$ with the $x$ axis. The unitary operator corresponding to this plate is given by

$$U(\eta,\phi)=\begin{bmatrix}\cos\phi & -\sin\phi\\ \sin\phi & \cos\phi\end{bmatrix}\begin{bmatrix}e^{i\eta/2} & 0\\ 0 & e^{-i\eta/2}\end{bmatrix}\begin{bmatrix}\cos\phi & \sin\phi\\ -\sin\phi & \cos\phi\end{bmatrix} \tag{1}$$

For $\eta=\pi$, it becomes a half-wave plate (denoted by $H_\phi$), while for $\eta=\pi/2$ it becomes a quarter-wave plate (denoted by $Q_\phi$). It has been shown that all $U(2)$ transformations can be realized on the polarization states by taking two quarter-wave plates and one half-wave plate with suitable choices of angles of their slow axes with the $x$ axis. We will henceforth refer to this device, capable of implementing $SU(2)$ transformations, as "Q-H-Q" (a detailed discussion is found in [21]). Combining this with an overall trivial phase transformation, we can implement the complete set of $U(2)$ transformations.

Further, let us map the $x$ polarization state to logical 1 and the $y$ polarization state to logical 0. With this mapping, we proceed to work with this system as a qubit. Since this system comprises essentially of classical elements, we call it a "classical qubit". We will use a notation where we specify the polarization state as

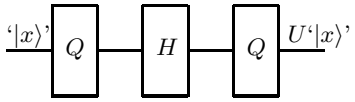


FIG. 1: The action of the Q-H-Q device on the polarization state '$|x\rangle$' of a single beam, taking it to a state '$|x\rangle$', where $U$ could be an arbitrary $SU(2)$ transformation

'$|x\rangle$' (i.e a ket vector within quotation marks) throughout this paper, where $x$ can take values 0 or 1. Multiple beams of this type can be considered and on each one of them arbitrary $U(2)$ transformations can be performed. All the computational basis states are mapped to appropriate polarization states using the above mapping. It is to be noted that we cannot obtain any entangled states here because the transformations available are $U(2)\otimes U(2)\cdots\otimes U(2)$.

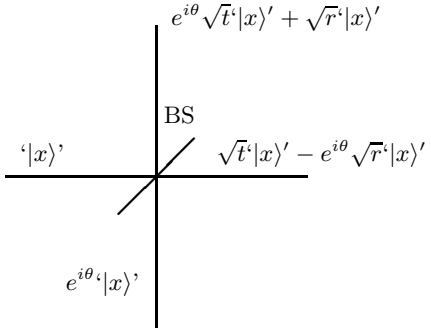


FIG. 2: The action of a beam splitter with transmission coefficient $t$ and reflection coefficient $r$ on a classical light beam with polarization state given by '$|x\rangle$'. The same polarization is being sent into both ports of the beam splitter and no polarization change occurs during the whole process. For instance, if the beam in one of the ports is missing and we use a 50-50 beam splitter, the beam splitter generates two identical beams which are clones of the original input beam and with their intensity reduced to half.

A beam splitter can be used to 'split' a beam and also to interfere beams with the same polarization. The transformation matrix of this operation on the amplitudes is given by

$$\mathrm{BS}=\begin{pmatrix}\sqrt{t} & -\sqrt{r}\\ \sqrt{r} & \sqrt{t}\end{pmatrix} \tag{2}$$

Where $t$ and $r$ are transmission and reflection coefficients respectively. This matrix acts on the amplitudes of the two beams entering the two ports of the beam splitter and not on the polarization states. Polarization states

do not undergo any transformation under the action of the beam splitter.

## III. THE BERNSTEIN-VAZIRANI ALGORITHM AND A MODIFIED ORACLE

Consider the binary function $f(x)$ defined from an $n$-bit domain space to a 1-bit range.

$$f : \{0,1\}^n \longrightarrow \{0,1\} \tag{3}$$

The function is considered to be of the form $f(x) = a \cdot x$, where $a$ is an $n$ bit string of zeros and ones and $a.x$ denotes bitwise XOR( or scalar product modulo 2):

$$f(x) = a_1x_1 \oplus a_2x_2 \oplus .....a_nx_n \tag{4}$$

The aim of the algorithm is to find the $n$-bit string $a$, given that we have access to an oracle which gives us the values of the function $f(x)$ when we supply it with an input $x$. Classically at least $n$ queries to the oracle are required in order to find the binary string $a$. The Bernstein-Vazirani algorithm solves this problem with a single query to a quantum oracle of the form

$$|x\rangle_{n-\text{qubit}}|y\rangle_{1-\text{qubit}} \xrightarrow{U_a} |x\rangle_{n-\text{qubit}}|f(x) \oplus y\rangle_{1-\text{qubit}} \tag{5}$$

where $x \in \{0, .....2^{n-1}\}$ is a data register and $|y\rangle$ acts as a target register. The algorithm works as follows: begin with an initial state with the first $n$-qubits in $|0\rangle$ state and the last qubit in the state $|1\rangle$. Apply a Hadamard transformation on all the $n+1$ qubits and then make a call to the oracle giving the following results:

$$\begin{aligned}
&|0\rangle^n|1\rangle \xrightarrow{H^{\otimes n+1}} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&\xrightarrow{U_a} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{(x.a)}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&\xrightarrow{H^{\otimes n+1}} \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{(x.a)}(-1)^{(x.z)}|z\rangle|1\rangle \\
&\equiv |a\rangle|1\rangle
\end{aligned} \tag{6}$$

where we have used the fact that

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{(a.x)}(-1)^{(x.z)} = \delta_{az}$$

A measurement in the computational basis immediately reveals the binary vector $a$. This algorithm therefore achieves the discovery of the vector $a$ in a single oracle call as opposed to $n$ oracle calls required classically. The oracle (5) has been queried on a superposition of states for this algorithm. However, if we query the oracle on a state $|x\rangle$ with the function register set to $|0\rangle$ we will recover the value $f(x)$ in the function register. This demonstrates that we can run the oracle in the classical mode when desired.

### A. Oracle modification and implementation without entanglement

This unitary oracle (5) requires $n+1$ qubits and can be operated in two different ways. If we use eigen states in the input and set $y = 0$, the algorithm outputs $f(x)$ for a given input $x$ in a reversible manner (which the original classical algorithm would do irreversibly). However, the algorithm can be performed on arbitrary quantum states (typically a uniform superposition of input states in the Deutsch-Jozsa and Bernstein-Vazirani algorithms).

A careful perusal of Equation (6) reveals two important facts about the Bernstein-Vazirani algorithm.

(a) The register qubit does not play any role in the algorithm. It is used only in the function evaluation step because the oracle (5) demands that we supply this extra qubit. However, if we modify the oracle to

$$|x\rangle_{\text{n-bit}} \xrightarrow{U_f} (-1)^{f(x)}|x\rangle_{\text{n-bit}} \tag{7}$$

we can implement everything on $n$ qubits. Since the state of the last qubit does not change, it can be considered redundant and we can remove the one-qubit target register altogether.

Although this oracle suffices to execute the Bernstein-Vazirani algorithm, it cannot give us the value of $f(x)$ for a given $x$. Therefore, one can argue that the connection with the original classical problem is lost and one is solving an altogether different problem. In this paper, we demonstrate that in the classical model based on polarization of light beams, this problem can be circumvented and we can obtain the value of $f(x)$ from $x$ via a suitable modification of the circuit. We will come back to these subtle points again in the next section.

(b) It turns out that this version of the oracle is implementable without requiring any entanglement for the case of the Bernstein-Vazirani algorithm. The modified oracle (7) can be implemented without introducing any entanglement because the unitary transformation $U_a$ can be decomposed as a direct product of single qubit operations.

$$\begin{aligned}
U_a &= U_a^{(1)} \otimes U_a^{(2)} \otimes \cdots U_a^{(n)} \\
&= (\sigma_z^1)^{a_1} \otimes (\sigma_z^2)^{a_2} \cdots (\sigma_z^n)^{a_n}
\end{aligned} \tag{8}$$

where $\sigma_z^j$ is the Pauli operator acting on the $j$ th qubit. On an $n$-qubit eigen state $|x\rangle = |x_1\rangle|x_2\rangle \cdots |x_n\rangle$ labeled by the binary string $x$ the action reduces to

$$U_a \equiv (-1)^{x_1.a_1} (-1)^{x_2.a_2} \cdots (-1)^{x_n.a_n} \tag{9}$$

This simplified version of the Bernstein-Vazirani algorithm where only $n$ qubits are used and we have separable states at all stages of the implementation has been depicted in figure (3). All the implementations till date have been along the lines of this circuit [27, 28].

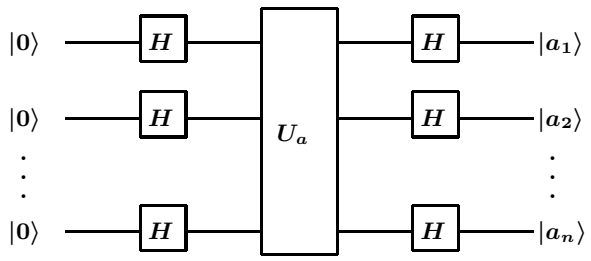


FIG. 3: Pictorial representation of the Bernstein-Vazirani algorithm using a modified oracle on $n$ un-entangled qubits. Initially the qubits are set to be all in the $|0\rangle$ state. Each box containing $H$ represents a Hadamard transformation and the box $U_a$ represents the oracle. By a single call to the oracle sandwiched between the hadamard gates we arrive at the final state $|a\rangle$ which on measurement reveals the binary vector $a$.

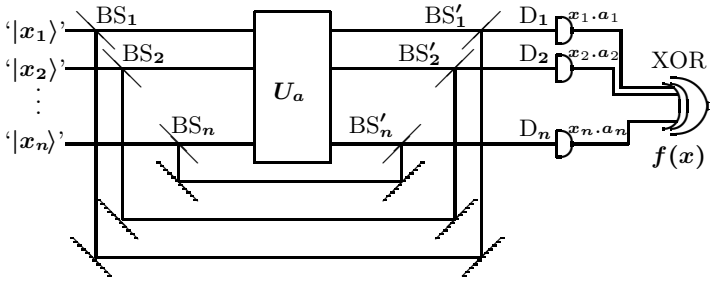


FIG. 4: Optical circuit to (a) implement the Bernstein-Vazirani algorithm in a new way and (b) to compute $f(x)$ from $x$. BS's represent 50/50 beam splitters, the corner elements are mirrors and D's are light detectors. The XOR gate is implemented on pairs of bits till we are left with only a one bit result.

## IV. NEW OPTICAL IMPLEMENTATION OF THE BERNSTEIN-VAZIRANI ALGORITHM

It was shown in Section (II) that $n$ classical beams of light can be visualized as an $n$ qubit system and the action of a non-entangling unitary transformation can be implemented via a suitable combination of two quarter wave plates and a half wave plate on each beam. Although the set of unitaries that can be implemented is limited, there is an added advantage that we can clone these beams by using beam splitters. The waves are classical and therefore there is no problem in dividing the amplitude of a given polarization to obtain two copies of the same polarization state. We will now use this property of the model to implement the Bernstein-Vazirani algorithm in a new way and also to make the modified oracle more powerful in terms of its capacity to compute $f(x)$ from $x$. A notation similar to quantum mechanics is used in which single quotations marks will be used around ket vectors for describing the polarization states of light beams, where '$|x_j\rangle$' represents $x$-polarization if $x_j = 0$ and $y$-polarization if $x_j = 1$. Each beam splitter in the circuit splits the beam into two, keeping the polarization state of both the beams identical to the original polarization. The intensity of the split beams is half that of the original beam.

We now follow the circuit described in Figure (IV) to arrive at our results. Consider the input state labeled by the binary vector $x$ with its bits given by $x_1, x_2 \cdots x_n$. We represent it by a polarization state '$|x_1\rangle$''$|x_2\rangle$'$\cdots$ '$|x_n\rangle$' where each beam has an $x$ or $y$ polarization depending upon the corresponding bit being 0 or 1.

Each beam goes through an identical set of operations. Consider the $j$th beam. The initial state of this beam is '$|x_j\rangle$' and after the beam splitter we have two copies of the same state (classical cloning of polarization states). The oracle acts on one of the copies and converts it via the unitary transformation $U_a^j = (-1)^{x_j.a_j}$; the other copy does not undergo any change. Both these copies are brought together and mixed at the beam splitter $BS'_j$ and the intensity is measured at the detector $D_j$.

$$'|x_j\rangle' \longrightarrow \begin{array}{ll} \frac{1}{\sqrt{2}}'|x_j\rangle' & \text{Transmitted} \\ -\frac{1}{\sqrt{2}}'|x_j\rangle' & \text{reflected} \end{array} \tag{10}$$

The transmitted component then undergoes the action of the oracle unitary (Equations (8) and (9)) which for the $j$th qubit acts via $U_a^j = \sigma_z^{a_J} = (-1)^{x_j.a_j}$. The state of the beam is

$$\frac{1}{\sqrt{2}}'|x_j\rangle' \xrightarrow{U_a^j} \frac{1}{\sqrt{2}}(-1)^{x_j.a_j}'|x_j\rangle' \tag{11}$$

As is clear from Equation (1), the implementation of $U_a^j$ on the $j$th beam is straightforward and is a polarization dependent phase shift corresponding to a single half wave plate with $\phi = 0$ and $\eta = \pi$ [30].

Finally, this beam meets the other beam (the one that did not undergo the oracle unitary) at the beam splitter $BS_j$, where they interfere to give the state of the beam moving towards detector $D_j$

$$\frac{1}{2}(-1)^{x_j.a_j}'|x_j\rangle' - \frac{1}{2}'|x_j\rangle' = \frac{1}{2}((-1)^{x_j.a_j} - 1)'|x_j\rangle' \tag{12}$$

The negative sign in Equation (12) implies that the beam which does not pass through the oracle acquires an extra phase factor of $\pi$, which can be easily arranged. After interference, the amplitude and hence the intensity at the detector $D_j$ is zero if $x_j.a_j$ is zero. On the other hand, if $x_j.a_j$ is one the intensity at the detector is

$\frac{1}{4}$ (assuming that we started with a beam of unit intensity). *This happens for all the beams and therefore each detector measures the corresponding $x_j.a_j$.*

### A. To find the $n$ bit string '$a$'

We can find $x_j.a_j$ separately for all $j$'s with this simple interferometric arrangement. The computation of the binary string $a$ is now straightforward. If we choose a special input state with $x_j = 1$ for all the $j \in \{1, 2, \cdots n\}$ then the detectors measure the corresponding $a_j$ and therefore we are able to compute the string $a$. This is quite different from the quantum version of the Bernstein-Vazirani algorithm where we use Hadamard gates to create superpositions. As a matter of fact, the scheme with Hadamard gates described in Figure (3) can also be implemented in our model with polarization qubits.

### B. Computing $f(x)$ for a given $x$

In order to compute $f(x)$ for a given $x$, the appropriate polarization state representing the $n$-bit input $x$ is chosen. The outputs from all the detectors are fed into a pair-wise XOR gate to compute addition modulo 2 (the XOR is applied to pairs of inputs until we are left with only one output). This process amounts to computing $f(x) = x_1.a_1 \oplus x_2.a_2 \cdots \oplus x_n.a_n$. We can thus compute $f(x)$ for any given $x$.

## V. CONCLUDING REMARKS

We have described a classical optical scheme to implement the Bernstein-Vazirani algorithm. This scheme is entirely classical as we have used only 'classical qubits' (based on the polarization states of light beams), and passive optical elements such as detectors, beam splitters, phase shifters and mirrors. The number of components needed to implement the algorithm increases linearly with the number of input beams. We have explicitly cloned the input and interfered it again with the part which undergoes the oracle unitary, in order to solve the Bernstein-Vazirani problem. This scheme does not require the implementation of any Hadamard gates. We have also shown through our interference arrangement that we can use the same oracle to compute $f(x)$ for a given $x$.

We believe that this analysis is a step in the direction where information processors based on interference of waves are analyzed in detail for their computation power. These systems seem to provide a model that is in-between the classical computation model based on bits and a fully quantum computer. The computational power is also likely to be in-between the two models (these issues will be discussed elsewhere).


[1] D. P. DiVincenzo, Science, **270**, 255 (1995).
[2] C. H. Bennett, Phys. Today, **273**, 44 (1995).
[3] C. H. Bennett and D. P. DiVincenzo, Nature, **404**, 247 (2000).
[4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[5] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[6] D. P. DiVincenzo, Proc. Roy. Soc. London A, **454**, 261 (1998).
[7] R. P. Feynmann, Int.J.Theor.Phys., **21**, 467 (1982).
[8] P. Benioff, Phys. Rev. Lett., **48**, 1581 (1982).
[9] D. Deutsch, Proc.Roy.Soc.London A, **400**, 97 (1985).
[10] D. Deutsch, Proc. Roy. Soc. London A, **425**, 73 (1989).
[11] D. Deutsch, and R. Jozsa, Proc. Roy. Soc. London A, **439**, 553 (1992).
[12] P. W. Shor, SIAM J. Comput., **26**, 1484 (1997).
[13] A. Ekert and R.Jozsa, Rev. Mod. Phy., **68**, 733 (1996).
[14] L. K. Grover, Phys.Rev.Lett. **79**, 325 (1997).
[15] E. Bernstein and U. Vazirani, "Quantum complexity theory†," *SIAM Journal on Computing* **26**(5), pp. 1411–1473, 1997.
[16] M. Horodecki, "Entanglement measures," *Quantum Information and Computation* **1**(1), pp. 3–26, 2001.
[17] R. Jozsa, *Entanglement and Quantum Computation*. Oxford University Press, January 1998.
[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[19] R. Jozsa and N. Linden, *Proceeding of the Royal Society of London series A* **459**, 2011, (2003).
[20] Dan Kenigsberg, Tal Mor, Gil Ratsaby, LANL preprint, quant-ph/0511272.
[21] R. Simon and N. Mukunda, Phys.Lett.A, **143**, 165 (1990).
[22] D. A. Meyer, Phys. Rev. Lett. **85**, (2000).
[23] B. Terhal and J. A. Smolin, Phys. Rev. A **58**, 1822 (1998).
[24] D. Collins, K. W. Kim, and W. C. Holton, Phys.Rev.A, **58**, R1633 (1998).
[25] Arvind, Pramana-J. Phys. **56**, 357 (2001).
[26] Arvind, Kavita Dorai and Anil Kumar, Pramana-J. Phys. **56**, 705 (2001).
[27] J. Du, M. Shi, X. Zhou, Y. Fan, B. Ye, R. Han, and J. Wu, Phys. Rev. A **64**, 042306 (2001).
[28] E. Brainis, L. -P. Lamoureux, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar Phys. Rev. Lett. **90**, 157902 (2003).
[29] J. Siewert and R. Fazio, Phys. Rev. Lett. **87**, 257905 (2001).
[30] We have to introduce an overall phase to bring the final output to the desired form. However, that can be done trivially and is hence not shown explicitly.