

Experimental Realization of Deutsch's Algorithm in a One-Way Quantum Computer

M. S. Tame,¹ R. Prevedel,² M. Paternostro,¹ P. Böhi,^{2,*} M. S. Kim,¹ and A. Zeilinger^{2,3}

¹*School of Mathematics and Physics, Queen's University, Belfast BT7 1NN, United Kingdom*

²*Faculty of Physics, University of Vienna, Boltzmannngasse 5, A-1090 Vienna, Austria*

³*Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmannngasse 3, A-1090 Vienna, Austria*

(Received 21 November 2006; published 2 April 2007)

We report the first experimental demonstration of an all-optical one-way implementation of Deutsch's quantum algorithm on a four-qubit cluster state. All the possible configurations of a balanced or constant function acting on a two-qubit register are realized within the measurement-based model for quantum computation. The experimental results are in excellent agreement with the theoretical model, therefore demonstrating the successful performance of the algorithm.

DOI: [10.1103/PhysRevLett.98.140501](https://doi.org/10.1103/PhysRevLett.98.140501)

PACS numbers: 03.67.Lx, 02.50.Le, 03.67.Mn, 42.50.Dv

The increasing interest in topics of quantum information processing (QIP) and quantum computation has stimulated considerable efforts in the realization of *quantum hardware* based on various experimental settings. These efforts have resulted in the realization of one and two-qubit logical gates [1], even though the networking of these basic building blocks is still far from being practical. Nevertheless, investigations in this direction, both at the experimental and theoretical level are vital for the advancement of QIP. The ultimate aim is the realization of multiqubit quantum algorithms able to outperform their classical analogues [1,2]. In this context, the implementation of few-qubit quantum algorithms represents a step forward in the construction of working processors based on quantum technology [3,4].

Very recently, a radical change of perspective in the design of quantum computational protocols has been proposed and formalized in the "one-way" model [5]. Here, computation is not performed by inducing a sequence of logical gates involving the elements of a quantum register, as in the quantum circuit model [1]. In the one-way case, a multipartite entangled state, the *cluster state*, is used as a resource for running a "program" represented by single-qubit measurements, performed in order to simulate a given computational task [5]. This new paradigm for quantum computation, which limits the amount of control one needs over a register to the ability of performing single-qubit measurements, has raised an enormous interest in the physical community. It has triggered investigations directed toward a better understanding of the model [6] and also its practical applications [7,8]. The efforts produced so far have culminated in the experimental demonstration of the basic features of the model, the realization of a two-qubit quantum search algorithm [7] and the theoretical proposal for a measurement-based realization of a quantum game [9]. The one-way model is also helping us to understand the paramount role of measurements in the quantum dynamics of a system.

Here, we report the first experimental demonstration of a one-way based implementation of Deutsch's algorithm [3].

It represents a simple but yet interesting instance of the role that the inherent parallelism of quantum computation plays in the speed-up characterizing quantum versions of classical problems. We have used an all-optical setup, where the construction of cluster states has been successfully demonstrated [7,8]. Negligible decoherence affecting qubits embodied by photonic degrees of freedom ensure the performance of the protocol in a virtually noise-free setting. Although Deutsch's algorithm has been implemented in a linear optical setup before [10], our protocol represents its first realization in the context of one-way quantum computation. It is based on the use of an entangled resource locally equivalent to the cluster state used previously for performing a two-qubit search algorithm [7] and reinforces the idea of the high flexibility of cluster resources. We show that four qubits in a linear cluster configuration are sufficient to realize all the possible functions acting on a logical two-qubit register. Two of these result from the application of an entangling gate to the elements of the register. In principle, this gate can be realized by inducing an interaction between the photonic qubits. In our cluster-state approach, the required entangling operations are realized by using the entanglement in the cluster resource and the nonlinearity induced by detection. There is no need for *engineering* it in a case by case basis [10], which is a very important advantage. The density matrix of the logical output qubits for the functions show excellent performance of the algorithm in our setup.

Model.—The generalized version of Deutsch's algorithm, also known as the Deutsch-Josza algorithm [11], takes an N -bit binary input x and allows one to distinguish two different types of function $f(x)$ implemented by an oracle. A function is *constant* if it returns the same value (either 0 or 1) for all possible inputs of x and *balanced* if it returns 0 for half of the inputs and 1 for the other half. Classically one needs to query this oracle as many as $2^{N-1} + 1$ times in some cases. However the quantum version requires only one query in all cases [11]. In the two-qubit version [3], the algorithm implements the oracle as a function f on a single query bit x using an input ancilla

bit y . The applied unitary operation is given by $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$. Preparing the input state as $|+\rangle|-\rangle$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $\{|0\rangle, |1\rangle\}$ is the single-qubit computational basis, the oracle maps the state to $(1/\sqrt{2}) \times [(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle]|-\rangle$. By measuring the query qubit in the $\{|\pm\rangle\}$ basis, one can determine which type of function $f(x)$ corresponds to. If $f(x)$ is balanced (constant), the query qubit is always $|-\rangle$ ($|+\rangle$). Thus, only one query of the oracle is necessary, compared to two in the classical version.

The action of the above oracle is either preset or dictated by the outcome of another algorithm. In order to implement all possible configurations that it might take in the two-qubit version, we must be able to construct them using a combination of quantum gates. In Fig. 1 we show all possible oracles in terms of their quantum network. By describing each as a “black box”, one can see that all four black boxes [BB(i)–(iv)] implement their respective oracle operation. In order to carry out the algorithm using these quantum gates, we use a cluster state and carry out one-way quantum computation on it by performing a correct program of measurements. No adjustment to the experimental setup is necessary.

Given a cluster state, there are two types of single-qubit measurements that allow a one-way quantum computer to operate. First, by measuring a qubit j in the computational basis it can be disentangled and removed from the cluster, leaving a smaller cluster state of the remaining qubits. Second, in order to perform QIP, qubits must be measured in the basis $B_j(\alpha) = \{|\alpha_+\rangle, |\alpha_-\rangle\}$, where $|\alpha_\pm\rangle_j = (|0\rangle \pm e^{i\alpha}|1\rangle)_j/\sqrt{2}$ ($\alpha \in \mathbb{R}$). Choosing the measurement basis determines the rotation $R_z(\alpha) = \exp(-i\alpha\sigma_z/2)$, followed by a Hadamard operation $H = (\sigma_x + \sigma_z)/\sqrt{2}$ being simulated on an encoded logical qubit in the cluster residing on qubit j ($\sigma_{x,y,z}$ are the Pauli matrices). With a large enough

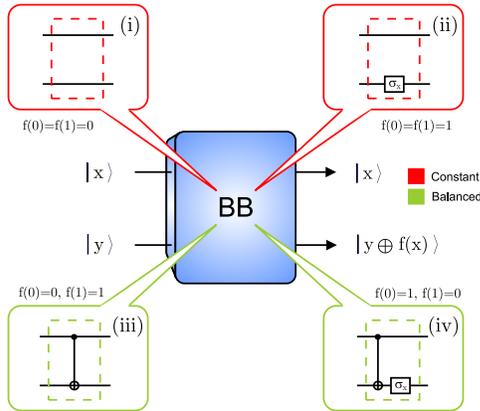


FIG. 1 (color online). Network diagrams for the black boxes in Deutsch’s algorithm. We have $\text{BB}(\text{i}) = \mathbb{1} \otimes \mathbb{1}$, $\text{BB}(\text{ii}) = \mathbb{1} \otimes \sigma_x$, $\text{BB}(\text{iii}) = \text{CNOT}$, and $\text{BB}(\text{iv}) = (\mathbb{1} \otimes \sigma_x)\text{CNOT}$ (CNOT denotes a Control-NOT gate).

cluster, any quantum logic operation can be performed with a proper choice for the $B_j(\alpha)$ ’s [12].

Experimental implementation.—For the entangled resource, in an ideal case, the following four-photon state is produced by means of the setup shown in Fig. 2(a) $|\Phi_c\rangle = (1/2)(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234}$ with $|0\rangle_j$ ($|1\rangle_j$) embodied by the horizontal (vertical) polarization state of one photon populating a spatial mode $j = 1, \dots, 4$. The preparation of the resource relies on postselection: a four-photon coincidence event at the detectors facing each spatial mode witnesses the preparation of the state. This state is locally equivalent to a four-qubit linear cluster state $|\Phi_{\text{lin}}\rangle$ (the local operation being $H_1 \otimes \mathbb{1}_2 \otimes \mathbb{1}_3 \otimes H_4$). The experimentally produced state ρ

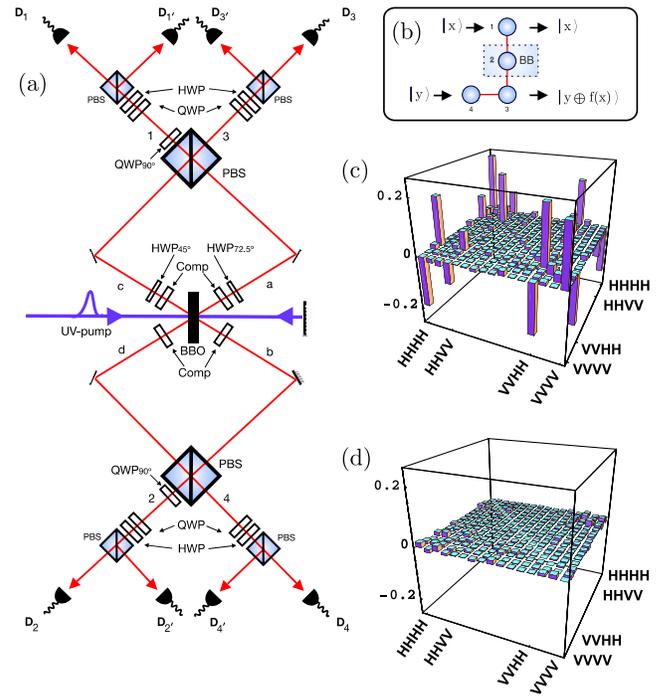


FIG. 2 (color online). (a) Experimental setup. An ultraviolet pump laser performs two passages through a nonlinear beta-barium-borate crystal (BBO) aligned to produce entangled photon pairs of the form $(|00\rangle - |11\rangle)_{ab}/\sqrt{2}$ and $(|00\rangle + |11\rangle)_{cd}/\sqrt{2}$. Compensators (Comp) are half-wave plates (HWP) and BBO crystals used in order to counteract walk-off effects at the BBO. By considering the possibility of obtaining a double-pair emission into the same pair of modes and the action of the polarizing-beam splitters (PBS’s), the four terms entering $|\Phi_c\rangle$ are obtained and their amplitudes and respective signs adjusted [7] with an additional HWP in mode (a). The algorithm is executed by using quarter-wave plates (QWPs), HWP’s, PBS’s, and photcounter pairs $\{D_j, D_j\}$ for the performance of polarization measurements in arbitrary bases of the photons in mode j . (b) Sketch of the cluster-state configuration. Qubit 1 embodies the logical input for $|x\rangle$ and its output. Qubit 4 (3) is the logical input (output) for $|y\rangle$, which is always found to be $|-\rangle_3$. (c) and (d): Real and imaginary plots, respectively, of the reconstructed experimental density matrix ρ .

verified by means of a maximum-likelihood technique for tomographic reconstruction [13] performed over a set of 1296 local measurements [7], each acquired within a time window of 500 s. This provides information about the overall quality of the experimental state on which the algorithm is performed. We have used all the possible combinations of the elements of the mutually unbiased basis $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |R\rangle, |L\rangle\}_j$ with $|\pm\rangle_j$ embodied by the polarization state at $\pm 45^\circ$ and $|L/R\rangle_j = (|0\rangle \pm i|1\rangle)_j/\sqrt{2}$, corresponding to left- and right-circularly polarized photons. This over-complete state tomography has the advantage of providing a more precise state estimation and significantly smaller error bars [7]. The reconstructed density matrix of ρ is shown in Figs. 2(c) and 2(d) and has a fidelity with the ideal state $|\Phi_c\rangle$ of $F = \langle \Phi_c | \rho | \Phi_c \rangle = 0.62 \pm 0.01$. The error bar was estimated by performing a 100 run Monte Carlo simulation of the whole state tomography analysis, with Poissonian noise added to the count statistics in each run [13]. Obtaining a higher fidelity is limited by phase instability during the lengthy process of state tomography and nonideal optical elements. However, it is well above the limit $F = 0.5$ for any biseparable four-qubit state [14] and demonstrates the presence of genuine four particle entanglement.

In order to perform Deutsch's algorithm on the cluster resource $|\Phi_c\rangle$, we have used a specific set of measurement bases for the qubits in each black box case. In Table I we provide these basis sets (BB_c) and feed-forward (FF) operations used to carry out the black boxes on $|\Phi_c\rangle$ and also $|\Phi_{\text{in}}\rangle$ (BB basis sets). As BB(ii) and BB(iv) are obtained from BB(i) and BB(iii) by using alternative FF operations (corresponding to adaptive measurements on the output qubits [12]), in what follows we explicitly describe BB(i) and BB(iii). Figure 2(b) shows the in-out logical states of the algorithm, where the logical input state corresponding to $|x\rangle = |+\rangle$ is encoded on qubit 1. The state $|y\rangle = |-\rangle$ will be encoded on qubit 3 by measuring qubit 4 in the $B_4(\pi)$ basis during the implementation of the algorithm (described next). This gives $|x\rangle|y\rangle \equiv [1 \otimes R_z(\pi)]|+\rangle|+\rangle$.

Qubit 2 in $|\Phi_{\text{in}}\rangle$ plays the pivotal role of the oracle as it performs a two-qubit gate on the logical input states $|x\rangle$ and $|y\rangle$. For BB(i), measuring qubit 2 in the computational basis disentangles it from the cluster and $|\Phi_{\text{in}}\rangle$ is trans-

formed into $|\pm\rangle_1(1/\sqrt{2})(|0\rangle|+\rangle \pm |1\rangle|-\rangle)_{34} (+ (-)$ for outcome $|0\rangle_2 (|1\rangle_2)$). The effective operation performed by this choice of the oracle's measurement basis is $1 \otimes 1$. By including the H operation applied to the input state $|y\rangle$ from the measurement of qubit 4, the overall computation results in $(1 \otimes 1)[1 \otimes HR_z(\pi)]|+\rangle|+\rangle$ which is equivalent to $|x\rangle|y \oplus f(x)\rangle = (1 \otimes 1)|+\rangle|-\rangle$ up to a local rotation H on physical qubit 3, applied at the FF stage. Qubits 1 and 3 can now be taken as the output $|x\rangle|y \oplus f(x)\rangle$. For BB(iii), upon measuring qubit 2 in the $B_2(\pi/2)$ basis, the oracle applies the gate $[R_z(\pi/2) \otimes R_z(\pi/2)]\text{CPHASE}$ on $|x\rangle$ and $|y\rangle$ (see Tame *et al.* in [6]), where CPHASE shifts the relative phase of the state $|1\rangle|1\rangle$ by π . This gives the computation $|x\rangle|y \oplus f(x)\rangle = \text{CNOT}|+\rangle|-\rangle \equiv [R_z(\pi/2) \otimes R_z(\pi/2)]\text{CPHASE}[1 \otimes HR_z(\pi)]|+\rangle|+\rangle$ up to local rotations $R_z(-\pi/2) \otimes HR_z(-\pi/2)$ on qubits 1 and 3, applied at the FF stage. The measurements and outcomes of qubits 1, 3, and 4 constitute the algorithm. The additions to the FF stages described above, together with the measurement of qubit 2 should be viewed as being carried out entirely by the oracle.

The results of our experiment are shown in Fig. 3, where we fully characterize the output states of our quantum computer by repeating the algorithm a large number of times. A single run of the algorithm (measuring the output qubit 1 in a specific basis only once) is sufficient in our setup to carry out the quantum computation with success rates as large as 90% (78%) for BB(i) [BB(iii)].

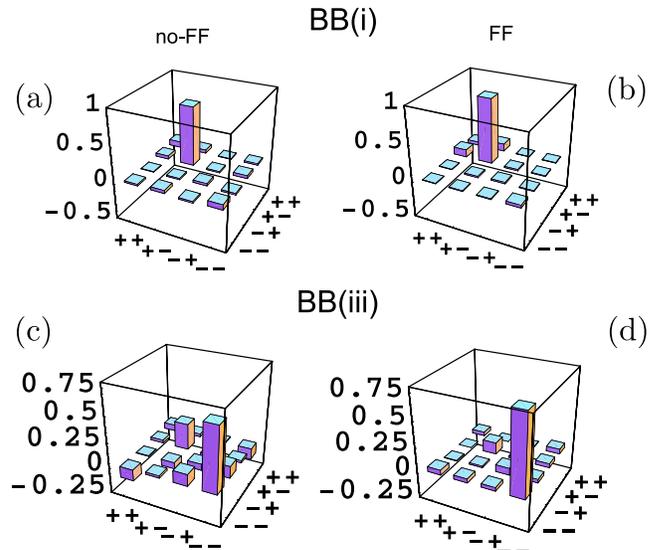


TABLE I. Measurement bases for the black boxes. The FF operations are $(\sigma_x^{s_2})_1(\sigma_x^{s_4})_3$ for BB_c (i) and $(\sigma_z^{s_2 \oplus s_4})_1(\sigma_x^{s_4})_3$ for BB_c (iii). Here, s_j is 0 (1) if the outcome is $|\alpha_+\rangle_j$ ($|\alpha_-\rangle_j$) on qubit j .

	Measurement basis
BB(i)	$\{B_1(0), \{ 0\rangle_2, 1\rangle_2\}, \{ 0\rangle_3, 1\rangle_3\}, B_4(\pi)\}$
BB_c (i)	$\{\{ 0\rangle_1, 1\rangle_1\}, \{ 0\rangle_2, 1\rangle_2\}, \{ 0\rangle_3, 1\rangle_3\}, \{ 1\rangle_4, 0\rangle_4\}\}$
BB (iii)	$\{B_1(\pi/2), B_2(\pi/2), \{ 0\rangle_3, 1\rangle_3\}, B_4(\pi)\}$
BB_c (iii)	$\{B_1(3\pi/2), B_2(\pi/2), \{ 0\rangle_3, 1\rangle_3\}, \{ 1\rangle_4, 0\rangle_4\}\}$

FIG. 3 (color online). The output density matrices for cluster qubits 1 and 3 when BB(i) and BB(iii) are implemented. Panels (a) and (c) show the real parts of the two-qubit density matrix elements as obtained from a maximum-likelihood reconstruction for the no-FF cases of BB(i) and BB(iii), respectively. Panels (b) and (d) show the corresponding plots for the FF case, due to the randomness of measurement outcomes for qubits 2 and 4. In all four cases the imaginary parts are zero in theory and negligible in the experiment (average values < 0.02).

However, repeating it several times allows us to verify the density matrix for the quantum state of qubits 1 and 3 reconstructed through a maximum-likelihood technique [13]. Although only the logical state residing on qubit 1 provides the outcome of the algorithm, it is useful for the characterization of the quantum computer's performance to also determine the state residing on qubit 3. Ideally, the joint state of qubits 1 and 3 should be the product state $|x\rangle|y \oplus f(x)\rangle$. By obtaining both correct logical output states, we can confirm that the algorithm will run correctly if included in a larger protocol. Figure 3 shows the output density matrices for BB(i) and BB(iii). Both the no-feed-forward (no-FF) and FF situations are shown. In the latter case, the state of the output qubits is corrected from the randomness of the measurements performed on the physical qubits 2 and 4. From the previous analysis, we know that the expected outcome from a single run, when a constant (balanced) function is applied is $|+, -\rangle_{13}$ ($|-, -\rangle_{13}$). Evidently, the reconstructed density matrices, both in the FF and no-FF cases, show a very good performance of the algorithm when compared with the theoretical expectations. The real parts are dominated by the correct matrix elements and no significant imaginary parts are found. Quantitatively, the fidelity with the desired state in the case of a constant (balanced) function is found to be as large as 0.90 ± 0.01 (0.78 ± 0.01) for the FF case and 0.82 ± 0.01 (0.63 ± 0.01) for the no-FF one. Moreover, no entanglement is found in any of the joint output states, as witnessed by the negativity of partial transposition criterion [15]. The small admixture of the undesired $|+, -\rangle_{13}$ to the expected $|-, -\rangle_{13}$ state when a balanced function is applied [Fig. 3(c)] is due to the non-ideal fidelity of the experimental cluster state with $|\Phi_c\rangle$. This is more pronounced for BB(iii) than for BB(i), where the measurement basis of qubit 2 breaks the channel between $|x\rangle$ and $|y\rangle$ resulting in a protocol-dependent *noise-inheritance* effect for imperfect cluster states (see Tame *et al.* in [6]).

Remarks.—We have designed, demonstrated, and characterized the performance of the first experimental realization of Deutsch's algorithm on a four-qubit cluster state. Our experiment is one of the few quantum algorithms entirely implemented utilizing the one-way model [7,9]. The agreement between the experimental data and theory is excellent and only limited by the overall quality of the entangled resource in the experiment.

We thank Č. Brukner, C. Di Franco, and A. Stefanov. We acknowledge support from DEL, the Leverhulme Trust

(No. ECF/40157), UK EPSRC, FWF, the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate and the U.S. Army Research Funded DTO Office.

*Present address: Max-Planck-Institut für Quantenoptik und Sektion Physik der Ludwig-Maximilians-Universität, Schellingstr. 4, 80799 München, Germany.

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computing and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
- [2] P. Shor, SIAM J. Comput. **26**, 1484 (1997); L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997); E. Bernstein and U. Vazirani, *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing, San Diego, CA, May 1993* (ACM, New York, 1993).
- [3] D. Deutsch, Proc. R. Soc. A **400**, 97 (1985).
- [4] N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997); D. G. Cory *et al.*, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997); I. L. Chuang *et al.*, Nature (London) **393**, 143 (1998); J. Jones, M. Mosca, and R. H. Hansen, Nature (London) **393**, 344 (1998).
- [5] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001); R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
- [6] M. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004); P. Walther *et al.*, *ibid.* **95**, 020403 (2005); M. S. Tame *et al.*, Phys. Rev. A **72**, 012319 (2005); D. Gross, K. Kieling, and J. Eisert, *ibid.* **74**, 042343 (2006).
- [7] P. Walther *et al.*, Nature (London) **434**, 169 (2005); R. Prevedel *et al.*, Nature (London) **445**, 65 (2007).
- [8] N. Kiesel *et al.*, Phys. Rev. Lett. **95**, 210502 (2005); A. N. Zhang *et al.*, Phys. Rev. A **73**, 022330 (2006); C.-Y. Lu *et al.*, Nature Phys. **3**, 91 (2007).
- [9] M. Paternostro, M. S. Tame, and M. S. Kim, New J. Phys. **7**, 226 (2005).
- [10] M. Mohseni *et al.*, Phys. Rev. Lett. **91**, 187903 (2003).
- [11] D. Deutsch and R. Jozsa, Proc. R. Soc. A **439**, 553 (1992).
- [12] A detailed introduction to experimental one-way quantum computing can be found in [7].
- [13] A. G. White *et al.*, Phys. Rev. Lett. **83**, 3103 (1999); D. James *et al.*, Phys. Rev. A **64**, 052312 (2001).
- [14] For a formal proof of this statement and the definition of biseparable states in multipartite systems, see: G. Toth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005).
- [15] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996); J. Lee *et al.*, J. Mod. Opt. **47**, 2151 (2000).