PHYSICAL REVIEW A **72**, 050305(R) (2005)

Experimental quantum communication complexity

Pavel Trojek,[1,2] Christian Schmid,[1,2] Mohamed Bourennane,[3] Časlav Brukner,[4] Marek Żukowski,[5] and Harald Weinfurter[1,2]
[1]*Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany*
[2]*Sektion Physik, Ludwig-Maximilians-Universität, D-80799 München, Germany*
[3]*Department of Physics, Stockholm University, SE-10691 Stockholm, Sweden*
[4]*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090, Wien, Austria*
[5]*Instytut Fizyki Teoretycznej i Astrofizyki Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*
(Received 8 June 2004; published 28 November 2005)

We prove that by communicating $N-1$ times a single qubit, instead of $N-1$ classical bits, the success probability for solving some N partner communication complexity tasks is strongly enhanced. The superiority, as measured by the quantum-to-classical fidelity ratio, of the quantum scheme grows exponentially with N. We report an experimental implementation of these tasks for $N=5$. Even without correcting for any inefficiencies of the state-of-the-art setup, our multiparty quantum protocol still outperforms the best classical protocols.

DOI: 10.1103/PhysRevA.72.050305 PACS number(s): 03.67.Hk, 42.65.Lm

Quantum information science breaks limitations of conventional information transfer, cryptography, and computation. For example, communication complexity problems (CCPs) [1] were shown to have quantum protocols, which outperform any classical ones. In a CCP, separated parties performing *local* computations exchange information in order to accomplish a *globally* defined task, which is impossible to solve singlehandedly. Two types of CCPs can be distinguished: the first one minimizes the amount of information exchange necessary to solve a task with certainty [2–4]; the second maximizes the probability of successfully solving a task with a restricted amount of communication [4–6]. Such studies aim, e.g., at a speedup of a distributed computation by increasing the communication efficiency, or at an optimization of very large scale integrated (VLSI) circuits and data structures [7].

Quantum protocols involving multiparty entangled states were shown to be superior to classical protocols for a number of CCPs [2–6]. However, current methods of production of such states do not work for more than four particles, and suffer from high noise. Fortunately, single-qubit multipartner CCP protocols are possible and can outperform the classical ones [8–10]. This breakthrough makes multiparty communication tasks feasible. They become technologically comparable to quantum key distribution, so far the only commercial application of quantum information.

Here we prove that, for CCPs with restricted communication, the superiority of the single qubit-assisted protocols over the corresponding classical ones may increase even exponentially with the number of partners. Furthermore, using parametric down conversion as a source of heralded single qubits, we experimentally show that quantum protocols solve two examples of CCPs more efficiently, even with the limited detection efficiency inherent in any real experiments. By solving these CCPs with a sequential transfer of a single qubit only, we demonstrate a generic way of bringing multiparty quantum communication schemes much closer to realistic applications.

Let us introduce the two CCPs analyzed and implemented here. The first one, problem A, is the so-called *modulo-4 sum* problem [3,4,10]. Imagine N separated partners $\mathcal{P}_1,\ldots,\mathcal{P}_N$. Each of them receives a two-bit input string X_k, $(X_k=0,1,2,3;\ k=1,\ldots,N)$. The X_ks are distributed such that their sum is even, i.e., $(\Sigma_{k=1}^{N}X_k)\mathrm{mod}\,2=0$. No partner has any information whatsoever on the values received by the others. Next, the partners communicate with the goal that one of them, say $\mathcal{P}_N$, can tell whether the sum modulo-4 of all inputs is equal 0 or 2. That is, $\mathcal{P}_N$ should announce the value of a dichotomic, i.e., of values ±1, function $T(X_1,\ldots,X_N)$ given by $T_A=1-(\Sigma_{k=1}^{N}X_k \bmod 4)$ (for an alternative formulation see [11]). The total amount of communication is restricted to only $N-1$ bits (classical scenario). The partners can freely choose a communication protocol as long as it does not depend on input data. Such a dependence would imply a violation of the communication restriction. (For example, they can choose between sequential communication from one to the other, or any arbitrary treelike structure ending at the last party $\mathcal{P}_N$).

Problem B has a similar structure, but now N *real* numbers $X_1,\ldots,X_N\in[0,2\pi)$ with probability density

$$p_B(X_1,\ldots,X_N)=\frac{1}{4(2\pi)^{N-1}}\left|\cos(X_1+\cdots+X_N)\right| \qquad (1)$$

are distributed to the partners. Their task is to compute whether $\cos(X_1+\cdots+X_N)$ is positive or negative, i.e., to give the value of the dichotomic function $T_B=S[\cos(\Sigma_{k=1}^{N}X_k)]$, where $S(x)=x/|x|$. The communication restriction is the same as for problem A.

For further convenience, one can introduce a different more handy notation. For the task A we put $X_k=(1-y_k)+x_k$, where $y_k\in\{-1,1\}$, $x_k\in\{0,1\}$. For the task B we write $X_k=\pi(1-y_k)/2+x_k$, with $y_k\in\{-1,1\}$, $x_k\in[0,\pi)$. Note that the dichotomic variables y_k are not restricted by the probability distributions, p, for the X_ks. They are completely random. The task function T can now be put as $T=f(x_1,\ldots,x_N)\Pi_{k=1}^{N}y_k$, where $f:x_k^N\rightarrow\{1,-1\}$, and $p(X_1,\ldots,X_N)=2^{-N}p'(x_1,\ldots,x_N)$ (see Ref. [12]).

Since T is proportional to the product of *all* y_ks, the answer $e_N=\pm1$ of $\mathcal{P}_N$ is completely random with respect to T, if it does not depend on every y_k. Thus, an unbroken com-

munication structure is necessary: the information from all $N-1$ partners must directly or indirectly reach $\mathcal{P}_N$. Due to the restriction to $N-1$ bits of communication each of the partners, $\mathcal{P}_k$, where $k=1,\ldots,N-1$, sends only a one-bit message, which for convenience will be denoted as $e_k=\pm 1$ [13].

For a correct answer $Te_N=1$, otherwise, $Te_N=-1$, and the average success can be quantified with fidelity $F=\Sigma_{X_1,\ldots,X_N} pTe_N$, or equivalently

$$F=\frac{1}{2^N}\sum_{x_1,\ldots,x_N=0,1} p'(x_1,\ldots,x_N)f(x_1,\ldots,x_N) \times \sum_{y_1,\ldots,y_N=\pm 1}\prod_{k=1}^{N} y_k e_N(x_1,\ldots,x_N;y_1,\ldots,y_N) \quad (2)$$

[for the problem B integrations replace summations; the probability of success reads $P=(1+F)/2$].

In any classical protocol the answer e_N by $\mathcal{P}_N$ can depend on y_N, x_N, and messages, $e_{i_1},\ldots,e_{i_\ell}$, received *directly* from partners $\mathcal{P}_{i_1},\ldots,\mathcal{P}_{i_\ell}$. That is, $e_N=e(x_N,y_N,e_{i_1},\ldots,e_{i_\ell})$. Let us fix x_N, and treat e as a function e_{x_N} of the remaining $\ell+1$ dichotomic variables, $y_N,e_{i_1},\ldots,e_{i_\ell}$. In the $2^{\ell+1}$-dimensional space of such functions one has *an orthogonal basis* given by $V_{jj_1,\ldots,j_\ell}(y_N,e_{i_1},\ldots,e_{i_\ell})=y_N^j\Pi_{k=1}^{\ell}e_{i_k}^{j_k}$, where $j,j_1,\ldots,j_\ell=0,1$. Thus, one can expand e_{x_N}

$$e_{x_N}=\sum_{j,j_1,\ldots,j_\ell=0,1} c_{jj_1,\ldots,j_\ell}(x_N)y_N^j\prod_{k=1}^{\ell} e_{i_k}^{j_k}, \quad (3)$$

where

$$c_{jj_1,\ldots,j_\ell}(x_N)=\frac{1}{2^{\ell+1}}\sum_{y_N,e_{i_1},\ldots,e_{i_\ell}=\pm 1} e_{x_N}V_{jj_1,\ldots,j_\ell}.$$

Since $|e_{x_N}|=|V_{jj_1,\ldots,j_\ell}|=1$, one has $|c_{jj_1,\ldots,j_\ell}(x_N)|\leqslant 1$. We put the expansion to Eq. (2). As, $\Sigma_{y_N=\pm 1}y_Ny_N^0=0$, and $\Sigma_{y_k=\pm 1}y_ke_k^0=0$, only the term with $j,j_1,\ldots,j_\ell=1$ in expansion (3) can give a nonzero contribution to F_c. Thus, without changing the result of Eq. (2), e_N in (2) can be replaced by a function $e'_N=y_Nc_N(x_N)\Pi_{k=1}^{\ell}e_{i_k}$, where $c_N(x_N)$ stands for $c_{11,\ldots,1}(x_N)$. Next, notice that, e.g., e_{i_1}, which is in the formula for e'_N, can depend only on x_{i_1},y_{i_1} and the messages obtained by $\mathcal{P}_{i_1}$ from a subset of partners: $e_{p_1},\ldots,e_{p_m}$ (this set does not contain any e_{i_k}). In analogy with (3), e_{i_1}, for a fixed x_{i_1}, can be expanded in terms of orthogonal basis functions

$$e_{i_1}=\sum_{j,j_1,\ldots,j_m=0,1} c'_{jj_1,\ldots,j_m}(x_{i_1})y_{i_1}^j\prod_{k=1}^{m} e_{p_k}^{j_k}. \quad (4)$$

Again, $|c'_{jj_1,\ldots,j_m}(x_{i_1})|\leqslant 1$. If one puts this into e'_N one obtains for the fidelity

$$F_c=\frac{1}{2^{N-2}}\sum_{x_1,\ldots,x_N} g(x_1,\ldots,x_N)c_N(x_N)c_{i_1}(x_{i_1}) \times \sum_{y'}\prod_{k\neq N,i_1} y_k\prod_{r=1}^{m} e_{p_r}\prod_{k=2}^{\ell} e_{i_k}, \quad (5)$$

where $g=p'f$, $c_{i_1}(x_{i_1})=c'_{11,\ldots,1}(x_{i_1})$, and $\Sigma_{y'}$ represents summation over $y_1,\ldots,y_{i_1-1},y_{i_1+1},\ldots,y_{N-1}=\pm 1$. Note that each message appears in the product only once. We continue this procedure of expanding the messages, until it halts (i.e., until we reach the level of those partners who do not receive any messages). The end result is

$$F_c=\sum_{x_1,\ldots,x_N} g(x_1,\ldots,x_N)\prod_{n=1}^{N} c_n(x_n), \quad (6)$$

with $|c_n(x_n)|\leqslant 1$. Since F_c in Eq. (6) is linear in every $c_n(x_n)$, its extrema are at the limiting values $c_n(x_n)=\pm 1$. In other words, a Bell-like inequality $|F_c|\leqslant \max(F_c)\equiv\mathcal{B}(N)$ gives the classical fidelity bound [14].

For our problems A and B the classical fidelity bounds decrease exponentially with N. For task A one gets as a result of the summation in Eq. (2) $F_{c,A}\leqslant 2^{-K+1}$, where $K=N/2$ and $K=(N+1)/2$ for even and odd number of parties, respectively. This *analytic* result confirms the numerical simulations of [10] for small N. For task B one has $F_{c,B}\leqslant(2/\pi)^{N-1}$. The derivation is equivalent to the proof of the inequality of Ref. [15].

For the quantum protocols, we note that the Holevo bound [16] limits the information storage capacity of a qubit to no more than one bit. Thus, we must now restrict the communication to $N-1$ qubits, or alternatively, to $(N-1)$-fold exchange of a *single* qubit. The solution of task A starts with a qubit in the state $|\psi_0\rangle=2^{-1/2}(|0\rangle+|1\rangle)$. Parties sequentially act on it with the phase-shift transformation $|0\rangle\langle 0|+e^{i\pi X_k/2}|1\rangle\langle 1|$, in accordance with their local data. After all N phase shifts one has

$$|\psi_N\rangle=\frac{1}{\sqrt{2}}(|0\rangle+e^{i\pi(\Sigma_{k=1}^{N}X_k)/2}|1\rangle). \quad (7)$$

Since the sum over X_k is even, the phase factor $e^{i\pi(\Sigma_{k=1}^{N}X_k)/2}$ is equal to the dichotomic function T_A to be computed. Thus, a measurement of the qubit in the basis $(|0\rangle\pm|1\rangle)/\sqrt{2}$ reveals the value of T_A with fidelity $F_{q,A}=1$, that is, *always* correctly.

Task B starts also with a qubit in the state $|\psi_0\rangle$. Each party performs according to his local data a unitary transformation $|0\rangle\langle 0|+e^{iX_k}|1\rangle\langle 1|$, leading to

$$|\psi_N\rangle=\frac{1}{\sqrt{2}}(|0\rangle+e^{i\Sigma_{k=1}^{N}X_k}|1\rangle). \quad (8)$$

The last party makes the same measurement as in task A. The probability for the detection of state $2^{-1/2}(|0\rangle\pm|1\rangle)$, which we associate with the result $r=\pm 1$, is given by $P(\pm)=[1\pm\cos(\Sigma_{k=1}^{N}X_k)]/2$. The expectation value for the final answer $e_N=r$ is $E=P(+)-P(-)$, and reads $\cos(\Sigma_{k=1}^{N}X_k)$. The fidelity of e_N, with respect to T_B is

$$F_{q,B}=\int_0^{2\pi}dX_1\cdots\int_0^{2\pi}dX_N p_B(X_1,\ldots,X_N) \times T_B(X_1,\ldots,X_N)E(X_1,\ldots,X_N). \quad (9)$$

With the actual forms of p_B, T_B, and E, one gets $F_{q,B}=\pi/4$, i.e., the protocol gives the correct value of T_B with probability $P_{q,B}=(1+\pi/4)/2\approx 0.892$.

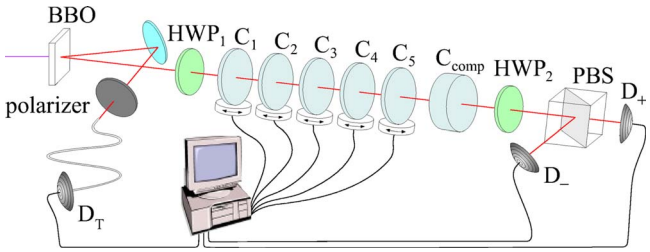

FIG. 1. (Color online) Setup for qubit-assisted CCPs. Pairs of orthogonally polarized photons are emitted from a BBO crystal via the type-II SPDC process. The detection of one trigger photon at D_T indicates the existence of the protocol photon. The polarization state is prepared with a half-wave plate (HWP_1) and a polarizer, placed in the trigger arm. Each of the parties introduces a phase-shift by the rotation of a birefringent YVO_4 crystal (C_1 to C_5). The last party performs the state analysis using a half-wave plate (HWP_2) followed by a polarizing beam splitter (PBS).

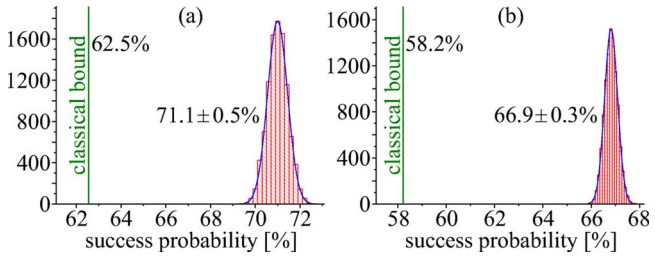

FIG. 2. (Color online) Histograms of measured quantum success probabilities (a) for the task A and (b) for B. The bounds for optimum classical protocols are displayed as well.

For both problems the classical fidelity F_c or the probability of success P_c decreases exponentially with growing N to the value corresponding to a random guess by $\mathcal{P}_N$. That is, communication becomes useless. In contrast, P_q does not change with N. For task A it equals 1, and for B it is approximately 0.892. The simple, one qubit assisted quantum protocol, without any shared multiparticle entanglement, clearly outperforms the best classical protocols.

We implemented the quantum protocols for $N=5$ parties, using a heralded single photon as the carrier of the qubit communicated sequentially by the partners [17]. The qubit was encoded in polarization. The computational basis, "0" and "1," corresponds to horizontal H and vertical V linear polarization, respectively. The data X_k of each party was encoded on the qubit via a phase shift, using birefringent materials. The last party performed a measurement in the $2^{-1/2}(|H\rangle \pm |V\rangle)$ basis to obtain the answer e_N.

In the experiment (Fig. 1) photon pairs are produced via spontaneous parametric down conversion (SPDC). The detection of one photon by the trigger detector D_T heralds the existence of the other one used in the protocol. The narrow gate window of 4 ns for coincidence detection between these two photons, along with the single-count rates of $\sim 140\,000\ s^{-1}$ at the detectors D_+ and D_-, warrant that the recorded data are due to single photons only. Type-II SPDC in 2-mm-thick β-barium borate (BBO) crystal, pumped by a single-mode laser diode (402.5 nm, 10 mW) is used, emitting pairs of orthogonally polarized photons at $\lambda = 805$ nm ($\Delta\lambda \approx 6$ nm). Filtering of the vertical polarization of trigger photons by a polarizer, ensures that the protocol photon has horizontal polarization initially. A half-wave plate (HWP_1) transforms the qubit to the initial state $2^{-1/2}(|H\rangle + |V\rangle)$.

For a fair comparison of the quantum protocols with the classical ones, no heralded events are discarded, even if the detection of the protocol photon failed. In such a case one can still guess the value of T, but with success rate of only 1/2. Therefore high detection efficiency of the heralded photons, i.e., high coincidence-to-single ratio for our setup, is essential for an unambiguous demonstration of the superiority of qubit-assisted protocol [10].

To minimize the cases with no detection of photons, the yield of heralded photons was maximized by adopting an unbalanced SPDC scheme. We select a restricted spatial mode with well-defined polarization of the trigger photons by coupling them into single-mode fiber behind a polarizer, whereas no spatial filtering is performed on the protocol photons. As a result, we observed $\approx$5000 trigger events per second with $\approx$2400 coincident events per second of protocol detections, i.e., an overall detection efficiency of $\approx$0.48, close to the limit given by the detector efficiency of our photodiodes (about 55%, for our operating wavelength).

The individual phase shifts of parties are implemented by rotating 200-μm-thick yttrium-vanadate (YVO_4) birefringent crystals (C_i) along their optic axis, oriented perpendicularly to the beam. An additional YVO_4 crystal (C_{comp}) compensates dispersion effects. To analyze the polarization state of photons in the desired basis, a half-wave plate (HWP_2) followed by polarizing beam splitter (PBS) is used.

The protocols were run many times, to obtain sufficient statistics. Each run took about one second. It consisted of generating a set of pseudorandom numbers obeying the specific distribution, subsequent setting of the corresponding phase shifts, and opening detectors for a collection time window τ. The limitation of communicating one qubit per run requires that only these runs, in which exactly one trigger photon is detected during τ, are selected for the evaluation of the probability of success P_{expt}. To maximize the number of such runs, n, the length of τ was optimized to 200 μs, assuming a Poissonian photon-number distribution of SPDC photons.

In order to determine the probability of success from the data acquired during the runs we have to distinguish the following two cases. First, the heralded photon is detected, which happens with probability η, given by the coincidence-to-single ratio. Then the answer e_N can be based on the measurement result. However, due to experimental imperfections in the preparation of the initial state, the setting of the desired phase shifts, and the polarization analysis, the answer is correct only with a probability γ, which must be compared with the theoretical limits given by $P_{q,A}$ and $P_{q,B}$ for the tasks A and B, respectively. Second, with the probability $1-\eta$ the detection of the heralded photon fails. Forced to make a random guess, the answer is correct in half of the cases. This leads to an overall success probability $P_{expt} = \eta\gamma + (1-\eta)0.5$, or a fidelity of $F_{expt} = \eta(2\gamma - 1)$.

Due to a finite measurement sample, our experimental results for the success probability are distributed around the

value P_{expt} as shown in Fig. 2 for both tasks. The width of the distribution is interpreted as the error in the experimental success probability. For task A we obtain a quantum success probability of $P_{expt,A}=0.711\pm0.005$. The bound $P_{c,A}=5/8$ for the optimal classical protocol is violated by 17 standard deviations. For the task B we reached $P_{expt,B}=0.669\pm0.003$, whereas the classical bound is $P_{c,B}\approx0.582$. The violation is by 29 standard deviations [18]. Table I summarizes the relevant experimental parameters n, η, and γ for both tasks.

In conclusion, we have proved and experimentally demonstrated the superiority of quantum communication over its classical counterpart for distributed computational tasks by solving two examples of CCPs. For CCPs, where the input from all the partners is required in order to obtain a nonrandom final result, the best classical fidelity goes exponentially to 0 with increasing number of partners, N. In contrast, for our single qubit protocols, fidelity is higher for all N, and does not change with N. In our experiment we have reached higher-than-classical performance in spite of all imperfections of state-of-the-art technologies. Thus, by successfully performing a fair and real comparison with the best classical scenario, we clearly illustrate the potential of the implemented scheme in real applications of multiparty quantum communication. Most importantly, our method gives a generic prescription to simplify many multiparty quantum communication protocols. For example, many-party secret-sharing protocols, employing multiqubit GHZ states and local operations only, can now be transformed to single-qubit schemes, thereby significantly enhancing their applicability [19].

TABLE I. Experimental parameters

	n	η	γ
Task A	6692	0.452 ± 0.010	0.966 ± 0.003
Task B	18169	0.471 ± 0.006	0.858 ± 0.004

M.Ż. was supported by Professorial Subsidy of FNP, and by MNiI Grant No. PBZ-MIN-008/P03/2003. This work was supported by the DFG, EU-FET (RamboQ, IST-2001-38864), the Marie Curie program, and the DAAD/KBN exchange program.

[1] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (ACM Press, NewYork, 1979), p. 209.
[2] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
[3] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp, Phys. Rev. A **60**, 2737 (1999).
[4] H. Buhrman, R. Cleve, and W. van Dam, SIAM J. Comput. **30**, 1829 (2001).
[5] L. Hardy and W. van Dam, Phys. Rev. A **59**, 2635 (1999).
[6] Č. Brukner, M. Żukowski, and A. Zeilinger, Phys. Rev. Lett. **89**, 197901 (2002); Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, *ibid.* **92**, 127901 (2004).
[7] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, New York, 1997).
[8] H. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 1998), p. 63.
[9] R. Raz, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 1999), p. 358.
[10] E. F. Galvão, Phys. Rev. A **65**, 012318 (2002).
[11] The connection with task B is more visible if one reexpresses the data probability distribution as $p_A(X_1,\ldots,X_N)=2^{-2N+1}|\cos[(\pi/2)\Sigma_{k=1}^{N}X_k]|$ and the task function as $T_A(X_1,\ldots,X_N)=\cos[(\pi/2)\Sigma_{k=1}^{N}X_k]$.
[12] Consequently, $f=f_A=\cos[(\pi/2)\Sigma_{k=1}^{N}x_k]$ with $p'=p'_A=2^{-N+1}|\cos[(\pi2)\Sigma_{k=1}^{N}x_k]|$, and $f=f_B=S[\cos(\Sigma_{k=1}^{N}x_k)]$ with $p'=p'_B=2^{-1}\pi^{-N+1}|\cos(\Sigma_{k=1}^{N}x_k)|$.
[13] Broadcasting of bits, i.e., communicating them publicly, does not improve the success rate of the classical protocol.
[14] Thus, the class of protocols, in which the partners $\mathcal{P}_1$ to $\mathcal{P}_{N-1}$ calculate $e_k=y_kc_k(x_k)$, with $c_k(x_k)=\pm1$, and send the result, encoded in e_k, to $\mathcal{P}_N$, who puts $e_N=\Pi_{k=1}^{N}[y_kc_k(x_k)]$, contains an optimal protocol of fidelity $\mathcal{B}(N)$.
[15] M. Żukowski, Phys. Lett. A **177**, 290 (1993).
[16] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973) [Probl. Inf. Transm. **9**, 177 (1973)].
[17] Bright polarized pulses of light cannot replace the heralded single photons. In such a case, a suitable polarization measurement reveals all the encoded input data of any party: two bits for task A, and arbitrarily many for task B. Thus, the communication restriction to $N-1$ bits is violated. Attenuation of the pulses to the single-photon level does not help either. The efficiency of the protocol is significantly lowered, due to many nondetection events, forcing one to guess the answer most of the time (see the description of the experiment in the text).
[18] Expressing the final results in terms of fidelities, we obtain $F_{\mathrm{expt},A}=0.421\pm0.010$ for task A, and $F_{\mathrm{expt},B}=0.337\pm0.006$ for task B. The best classical protocol reaches $F_{c,A}=0.25$ for A and $F_{c,B}\approx0.164$ for B.
[19] C. Schmid *et al.*, Phys. Rev. Lett. (to be published).