NATO Science for Peace and Security Series
D: Information and Communication Security - Vol. 11

Quantum Communication and Security

Edited by
Marek Żukowski
Sergei Kilin
Janusz Kowalik

IOS Press

NATO OTAN

This publication is supported by:

The NATO Science for Peace and Security Programme

Quantum Communication and Security
M. Żukowski et al. (Eds.)
IOS Press, 2007

Experimental Single Qubit Quantum Multiparty Communication

Mohamed BOURENNANE [a,1], Christian SCHMID [b], Pavel TROJEK [b], Christain KURTSIEFER [c], Časlav BRUKNER [d], Marek ŻUKOWSKI [e], and Harald WEINFURTER [b]

[a] *Physics Department, Stockholm University, Stockholm, Sweden*
[b] *Sektion Physik, Ludwig-Maximilians-Universität, D-80797 München, Germany and Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany*
[c] *Department of Physics, National University of Singapore, Singapore 117 542, Singapore*
[d] *Institut für Experimentalphysik, Universität Wien, A-1090, Wien, Austria*
[e] *Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*

Abstract. We present simple and practical quantum solution for secure multiparty communication protocols, the secret sharing and the communication complexity and their proof-of-principle experimental realizations. In the secret sharing protocol, a secret is split among several parties in a way that its reconstruction requires the collaboration of the participating parties. In the communication complexity problem, the goal is to maximize the success probability of the partners for solving for giving communication resources some N partner communication complexity tasks. Our quantum solution is based on sequential transformations on a single qubit. In contrast with recently proposed schemes involving multiparticle GHZ states.

Keywords. Quantum cryptography, communication complexity, quantum information

Introduction

Quantum information science breaks limitations of conventional information transfer, cryptography and computation. Here we will consider two multiparty protocols, secret sharing and communication complexity. The 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 [2,3,4]. The second one maximizes the probability of successfully solving a task with a restricted amount of communication

[1] Corresponding Author: E-mail: boure@physto.se

[3,5,6]. Such studies aim, e.g., at a speed-up of a distributed computation by increasing the communication efficiency, or at an optimization of VLSI circuits and data structures [7].

In the secret sharing protocol (SSP), the secret is splitted in way that a single person is not able to reconstruct it. Suppose for example that the launch sequence of a nuclear missile is protected by a secret code. Yet, it should be ensured that a single lunatic alone is not able to activate it, but at least two lunatics are required. Solutions for this problem, and its generalization and variations, are studied in classical cryptography [8]. In such problems the aim here is to split information, using some mathematical algorithms, and to distribute the resulting pieces to two or more legitimate parties. However classical communication is susceptible to eavesdropping attacks.

Quantum protocols for the CCPs [2,3,4,5,6] and the SSPs [9,10,11,12] involving multiparty entangled states were shown to be superior to classical protocols. However,current methods of production of such states do not work for more than four particles, and suffer from high noise.

Here we propose a quantum protocol for the CCPs and SSPs for N parties, in which a sequential single qubit communication between them is used with no need for GHZ-states. As our protocol requires only single qubits it is realizable with the current state-of-the-art technologies, they become technologically comparable to quantum key distribution, so far the only commercial application of quantum information.

1. Single qubit secret sharing protocol

Here we present An N party SSP [13], where only the sequential communication of a single qubit is used, runs as follows (see Figure 1). The qubit is initially prepared in the state

$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{1}$$

During the protocol the qubit is sequentially communicated from partner to partner, each acting on it with the unitary phase operator $\widehat{U}_j(\varphi_j) \equiv |0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow e^{i\varphi_j}|1\rangle$ with the randomly chosen value of $\varphi_j \in \{0, \pi, \pi/2, 3\pi/2\}$. Therefore, having passed all parties, the qubit will end up in the state

$$|\chi_N\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i(\sum_j^N \varphi_j)}|1\rangle\right). \tag{2}$$

The last party performs a measurement on the qubit in the basis $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ leading to the result ± 1. As it will be clarified later, for her/him it suffices to choose only between $\varphi_N = 0$ or $\varphi_N = \pi/2$. The expectation value of the measurement is

$$E(\varphi_1, \ldots, \varphi_N) = \cos\left(\sum_j^N \varphi_j\right). \tag{3}$$

Note that this expectation value (Eqn. 3) has the same structure like the correlation function obtained using the GHZ state and can therefore also be used to obtain a shared se-

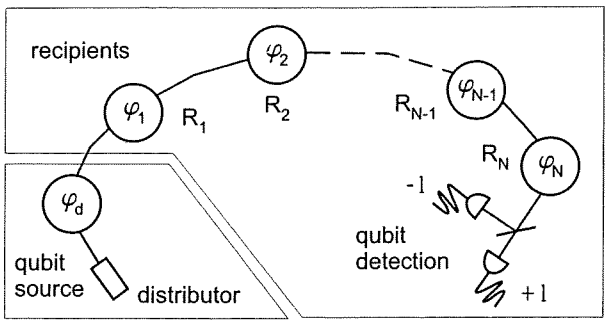

Figure 1. Scheme for N party single qubit secret sharing. A qubit is prepared in an initial state and sequentially communicated from party to party, each acting on it with a phase operator $\widehat{U}(\varphi_j)$, applying a randomly chosen phase φ_j. The last recipient performs a measurement on the qubit leading to the result ± 1. In half of the cases the phases add up such that the measurement result is deterministic. These instances can be used to achieve the aim of secret sharing.

cret. For this purpose each participant divides his action for every run into two classes: a class X corresponding to the choice of $\varphi_j \in \{0, \pi\}$ and a class Y corresponding to $\varphi_j \in \{\pi/2, 3\pi/2\}$. Following this classification they broadcast the class of their action for each run, but keep the particular value of φ_j secret. This corresponds in the GHZ scheme to the announcement of ϕ_j while keeping k_j secret. In our scheme the partners announce their class choice in the reversed order with respect to the order of the qubit transmission [14]. From that procedure they can determine which runs lead to a deterministic measurement result, i.e. when $\cos(\sum_j^N \varphi_j)$ equals to either 1 or -1. Such sets of φ's occur on average in half of the runs. These are valid runs of the protocol. In such cases any subset of $N-1$ parties is able to infer the choice of φ_R of the remaining partner, if themselves their values of φ_j. In case that this subset contains the last partner, he/she must reveal the measurement result. Thus, the collaboration of all recipients is necessary. The task of secret sharing is now achieved via local manipulation of phases on a communicated single qubit, and no multiparticle entangled GHZ state is required anymore.

In order to ensure the security of the protocol against eavesdropping or cheating the partner P_R arbitrarily selects a certain subset (which depends on the degree of security requirements) of valid runs. For these runs the value of φ_R is compared with the one inferred by the recipients. To this end each of the recipients sends the value of his/her phase φ_j. The comparison reveals any eavesdropping or cheating strategy. The security of the presented protocol against a general eavesdropping attack follows from the proven security of the well known BB84 protocol [15,16]. Each communication step between two successive parties can be regarded as a BB84 protocol using the bases x and y. Any set of dishonest parties in our scheme can be viewed as an eavesdropper in BB84 protocol.

2. Single qubit quantum communication complexity problem

Let us introduce the CCP analyzed and implemented here, the so-called *modulo-4 sum* problem [3,4,18]. 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. $(\sum_{k=1}^{N} X_k)\mathrm{mod}2 = 0$. 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 $T = 1 - (\sum_{k=1}^{N} X_k \mathrm{mod}4)$. The partners can freely choose the communication protocol, e.g. they can choose between sequential communication from one to the other, or any arbitrary tree-like structure ending at the last party $\mathcal{P}_N$. The total amount of communication is restricted to only $N - 1$ bits (classical scenario).

For further convenience, one can introduce a different more handy notation, 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 $T = f(x_1, \ldots, x_N) \prod_{k=1}^{N} y_k$, where $f : x_k^N \to \{1, -1\}$, and $p(X_1, \ldots, X_N) = 2^{-N} p'(x_1, \ldots, x_N)$.

Since T is proportional to the product of *all* y_ks, the answer $e_N = \pm 1$ of $\mathcal{P}_N$ is completely random with respect to T, if it does not depend on every y_k. Thus, an unbroken communication 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 $e_k = \pm 1$.

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

$$F = \frac{1}{2^N} \sum_{x_1, \ldots, x_N = 0,1} p'(x_1, \ldots, x_N) f(x_1, \ldots, x_N)$$
$$\times \sum_{y_1, \ldots, y_N = \pm 1} \prod_{k=1}^{N} y_k e_N(x_1, \ldots, x_N; y_1, \ldots, y_N) \tag{4}$$

We have shown that the classical fidelity bound is by Bell-like inequality. This classical bound decrease exponentially with N. One has $F_c \leq 2^{-K+1}$, where $K = N/2$ and $K = (N + 1)/2$ for even and odd number of parties, respectively [17]. This *analytic* result confirms the numerical simulations of [18] for small N.

For the quantum protocols, we note that the Holevo bound [19] 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 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

$$|\psi_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi(\sum_{k=1}^{N} X_k)/2}|1\rangle). \tag{5}$$

Since the sum over X_k is even, the phase factor $e^{i\pi(\sum_{k=1}^{N} X_k)/2}$ is equal to the dichotomic function T to be computed. Thus, a measurement of the qubit in the basis $(|0\rangle \pm |1\rangle)/\sqrt{2}$ reveals the value of T with fidelity $F_q = 1$, that is, *always* correctly [17].

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 $\mathcal{P}_N$. I.e., communication becomes useless. In contrast, P_q does not change with N and it equals 1. The simple, one qubit assisted quantum protocol, without any shared multi-particle entanglement (!), clearly outperforms the best classical protocols.

3. Experiment

We have experimentally implemented the two SSPs and CCPs. We encoded the protocol qubit in a single photon. The basis states $|0\rangle$ and $|1\rangle$ were represented by the polarization states $|H\rangle$ and $|V\rangle$ respectively (horizontal (H) and vertical (V) linear polarization). The single photons were provided by a heralded single photon source. The setup is shown in A pair of polarization entangled photons is created via a spontaneous parametric down conversion (SPDC) process. As the photons of a pair are strongly correlated in time the detection of one photon in D_T heralds the existence of the other one which is used for the protocol. A coincidence detection between D_T and D_+/D_-, within a chosen time window of 4 ns, implies communication of only a single photon. The SPDC process was run by pumping a 2 mm long β-barium borate (BBO) crystal with a blue single mode laser diode (402.5 nm), at an optical output power of 10 mW. Type-II phase matching was used, at the degenerate case leading to pairs of orthogonally polarized photons at a wavelength of $\lambda = 805$ nm ($\Delta\lambda \approx 6$ nm) (see Figure 2. In order to prepare the initial polarization state a polarizer transmitting vertically polarized photons was put in front of the trigger detector D_T ensuring that only (initially) horizontally polarized photons can lead to a coincidence detection. This single qubit source will used to implement our two multiparty protocols [13,17].

3.1. *Experimental single qubit $N = 6$ secret sharing*

The first partner was equipped with a motorized half-wave plate (HWP_1) followed by quarter-wave plate (QWP) at an angle of $45\,^\circ$. By rotation of HWP_1 to the angles $0\,^\circ, 45\,^\circ$ and $22.5\,^\circ, -22.5\,^\circ$ he could transform the horizontally polarized photons coming from the source to $|\pm y\rangle$ and $|\pm x\rangle$. This corresponds to applying the phase-shifts

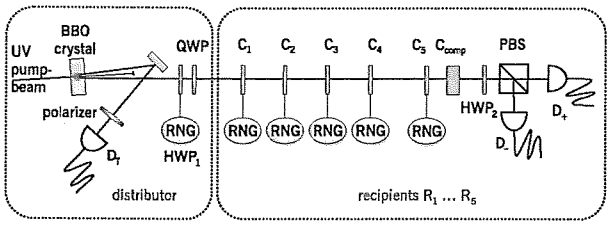

Figure 2. Setup for single qubit secret sharing. Pairs of orthogonally polarized photons are generated via a type II SPDC process in a BBO crystal. The detection of one photon from the pair by D_T heralds the existence of the other one used in the protocol. The initial polarization state is prepared by placing a polarizer in front of the trigger detector. Each of the recipients ($R_1 \ldots R_6$) introduces one out of four phase shifts, according to the output of a pseudo random number generator (RNG), using half- and quarter wave plate (HWP_1, QWP) or YVO_4 crystals ($C_1 \ldots C_5$), respectively. The last party analyzes additionally the final polarization state of the photon by detecting it behind a half-wave plate (HWP_2) and a polarizing beam splitter.

$\varphi \in \{\pi/2, 3\pi/2\}$ and $\varphi \in \{0, \pi\}$ respectively. As the phase-shifts of the other partners had to be applied independently from the incoming polarization state the usage of standard wave plates was not possible. Therefore the unitary phase operator was implemented using birefringent uniaxial 200 μm thick Yttrium Vanadate (YVO_4) crystals (C_i). The crystals were cut such that their optic axis lies parallel to the surface and is aligned in such a way that H and V polarization states correspond to their normal modes. Therefore by rotating the crystals along the optic axis for a certain angle a specific relative phase shift was applied independently from the incoming polarization state. An additional YVO_4 crystal (C_{comp}, 1000 μm thick) was used to compensate for dispersion effects (see fig. 2. The last party performed the measurement behind a half-wave plate (HWP_2) at an angle of 22.5 ° followed by polarizing beam-splitter (PBS). The photons were detected at D_+/D_- and D_T by passively quenched silicon avalanche photo diodes (Si-APD) with an efficiency of about 35 % [13].

The protocol was repeated $z_{total} = 25000$ times. One run consisted of choosing pseudo-random variables, rotating the crystals accordingly and opening the detectors for a collection time window $\tau = 200\,\mu$s, what took together about 1 s. The requirement of communicating a single photon imposes that only those runs were included into the protocol in which just one coincidence between D_T and either D_+ or D_- (coincidence gate time $\tau_c \approx 7ns$) was detected during τ. In these runs a single coincidence detection happened $z_{raw} = 2107$ times which provided us with the raw key. From this we extracted $z_{val} = 982$ valid runs where $|\cos(\sum_j^N \varphi_j)| = 1$ (506 times $\cos(\sum_j^N \varphi_j) = 1$ and 476 times $\cos(\sum_j^N \varphi_j) = -1$) with a quantum bit error rate (QBER) of 2.34 ± 0.48 [13].

3.2. *Experimental single qubit $N = 5$ communication complexity*

We implemented the quantum protocols for $N = 5$ parties, using a our heralded single photon as the carrier of the qubit communicated sequentially by the partners. A half-wave plate (HWP_1) transforms the qubit to the initial state $2^{-1/2}(|H\rangle + |V\rangle)$. 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 [17].

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

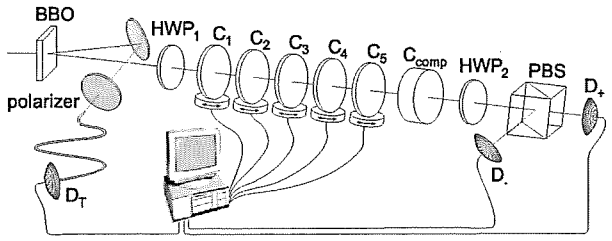

Figure 3. Color online) Set-up for qubit-assisted CCPs. Pairs of orthogonally polarized photons are emitted from a BBO crystal via the type-II SPDC process. The detection of one trigger photon at D_T indicates the existence of the protocol photon. The polarization state is prepared with a half-wave plate (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 analysis of a photon-polarization state using a half-wave plate (HWP_2) followed by a polarizing beam-splitter (PBS).

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/single ratio for our set-up, is essential for an unambiguous demonstration of the superiority of qubit-assisted protocol [18].

The individual phase shifts of parties are also implemented by rotating 200 μm thick Yttrium-Vanadate (YVO_4) birefringent crystals (C_i) along their optic axis. 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 (see Figure 3).

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_{exp}.

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/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. 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 $P_{exp} = \eta\gamma + (1-\eta)0.5$, or a fidelity of $F_{exp} = \eta(2\gamma - 1)$.

Due to a finite measurement sample, our experimental results for the success probability are distributed around the value P_{exp} as shown in Figure 4. 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 $P_{exp} = 0.711 \pm 0.005$.

The bound $P_c = 5/8$ for the optimal classical protocol is violated by 17 standard deviations. We have obtained for $n = 6692$ the values $\eta = 0.452 \pm 0.010$ and $\gamma = 0.966 \pm 0.003$.

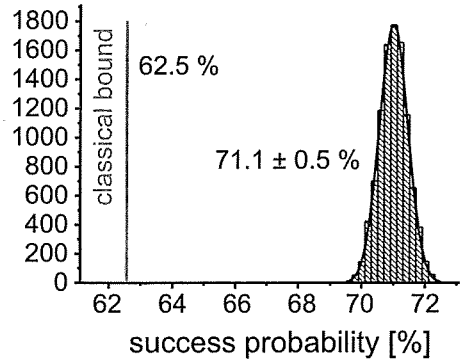

Figure 4. Histograms of measured quantum success probabilities. The bounds for optimum classical protocols are displayed as well.

Summary

In summary, we introduced a new scheme for solving the multi-party secret sharing and communication complexity protocols. Unlike other quantum schemes employing multi-particle entangled states our protocols uses only the sequential communication of a single qubit. As single qubit operations using linear optical elements and the analysis of photon polarization states are quite well accomplishable with present day technology we were therefore able to present the first experimental demonstration of the secret sharing protocol for $N = 6$ parties. This is to our knowledge the highest number of actively performing parties in a quantum protocol ever implemented. we have experimentally demonstrated the superiority of quantum communication over its classical counterpart for distributed computational tasks by solving two examples of CCPs. In our experiment we have reached higher-than-classical performance even when including 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 multi-party quantum communication. In principle we see no experimental barrier to extend the performed protocol to even significantly higher number of participants. Most importantly, our method gives a generic prescription to simplify many multi-party quantum communication protocols.

Acknowledgements

This work was supported by Polish MNiI, German DFG, Swedish Research Council (VR) grants, and the European Commission through the IST FET QIPC QAP.

References

[1] A. C.-C. Yao, *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, ACM Press, NewYork, **209** (1979).
[2] R. Cleve and H. Buhrman, *Phys. Rev. A* **56**, 1201 (1997).
[3] H. Buhrman, R. Cleve, and W. van Dam, *SIAM J. Comput.* **30**, 1829 (2001).
[4] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp, *Phys. Rev. A* **60**, 2737 (1999).
[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, *Phys. Rev. Lett.* **92**, 127901 (2004).
[7] E. Kushilevitz and N. Nisan, *Communication complexity*, Cambridge University Press, England, 1997.
[8] B. Schneier,*Applied Cryptography*, John Wiley & Sons, Inc., 1996.
[9] M. Żukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter, *Acta Phys. Pol* **93** 187, (1998).
[10] M. Hillery, V. Bužek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).
[11] R. Cleve, D. Gottesma, and H.-K. Lo, *Phys. Rev. Lett.* **83**, 648 (1999).
[12] A. Karlsson, M. Koashi, and N. Imoto, *Phys. Rev. A* **59**, 162 (1998).
[13] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, *Phys. Rev. Lett.* **95**, 230505 (2005).
[14] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, *Phys. Rev. Lett.* **98** 028902 (2007).
[15] C. Bennett and G. Brassard, *Proc. of IEEE International Conference on Computer, Systems & Signal Processing, Bangalore, India*, 175 (1984).
[16] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
[17] P. Trojek, C. Schmid, M. Bourennane, Časlav Brukner, M. Żukowski, and H. Weinfurter, *Phys. Rev. A* **72**, 050305(R) (2005).

[18] E. F. Galvão, *Phys. Rev. A* **65**, 012318 (2002).
[19] A. S. Holevo, *Probl. Peredachi Inf.* **9**, 3 (1973) [*Probl. Inf. Transm.* **9**, 177 (1973)].

ISBN 978-1-58603-749-9

9 781586 037499

www.iospress.nl

ISBN 978-1-58603-749-9
ISSN 1874-6268