Reference-frame-independent quantum key distribution

Anthony Laing,[1,*] Valerio Scarani,[2,†] John G. Rarity,[1,‡] and Jeremy L. O'Brien[1,§]
[1]*Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, BS8 1UB, United Kingdom*
[2]*Centre for Quantum Technologies and Department of Physics, National University of Singapore, Singapore*
(Received 18 March 2010; published 7 July 2010)

We describe a quantum key distribution protocol based on pairs of entangled qubits that generates a secure key between two partners in an environment of unknown and slowly varying reference frame. A direction of particle delivery is required, but the phases between the computational basis states need not be known or fixed. The protocol can simplify the operation of existing setups and has immediate applications to emerging scenarios such as earth-to-satellite links and the use of integrated photonic waveguides. We compute the asymptotic secret key rate for a two-qubit source, which coincides with the rate of the six-state protocol for white noise. We give the generalization of the protocol to higher-dimensional systems and detail a scheme for physical implementation in the three-dimensional qutrit case.

DOI: 10.1103/PhysRevA.82.012304 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Hk

I. INTRODUCTION

Technologies based on the principles of quantum information [1] promise a revolution in informational tasks such as computer processing [2,3] and communication [4]. Secure communication via quantum key distribution (QKD) is one quantum information application that can be realized with current technologies [5–8]. In general, all the QKD protocols proposed to date have in common the need for a *shared reference frame* between the authorized partners Alice and Bob: alignment of polarization states for polarization encoding, interferometric stability for phase encoding. This requirement can, in principle, be dispensed with by encoding logical qubits in larger-dimensional many-photon physical systems [9]. However, the creation, manipulation, and detection of many-photon entangled states is both technically challenging and very sensitive to the losses on the Alice-Bob channel—in a word, impractical. More feasible single-photon physical implementations have been proposed which seek to address the alignment limitations of standard protocols [10–13] yet these schemes can inherit further complications that require active compensation between parties [14]. To date, therefore, all practical implementations of QKD within an environment of varying phase have required the frames of Alice and Bob to be actively aligned by classical communication.

In this paper, we present a *reference frame independent* (rfi) *protocol* that is separate from any particular physical implementation, can be implemented with ordinary sources and operate without frame alignment, beyond the obvious establishment of a particle delivery link. Moreover, there are at least two emerging scenarios in QKD that will benefit from an rfi implementation (Fig. 1). The first such scenario is *earth-to-satellite* QKD [10,14–21]. In this case, one axis of the reference frame is well defined: The beam must obviously connect the earth station with the satellite. On this beam, information encoded in circular polarization is very stable, but the linear polarizations may vary in time because the satellite may be rotating with respect to the ground station. The second scenario is path-encoded *chip-to-chip* QKD. The monolithic structures of planar waveguides have been successfully used to perform the stable interferometric measurements required in time and phase-encoded QKD [22–25]. More recently, integrated quantum photonic circuits have demonstrated their potential as components for more

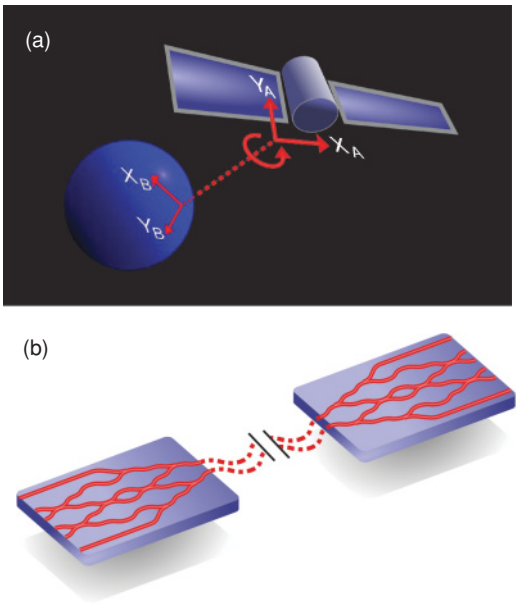

FIG. 1. (Color online) Two meaningful scenarios for reference frame independent QKD. (a) Polarization encoding in earth-to-satellite quantum communication. Here the circular polarization states are stable, but the linear states can vary with the rotation of the satellite. (b) Path encoding in chip-to-chip quantum communication. While the path information is stable, the unpredictable wavelength-scale changes in relative path length amount to a varying reference frame. This may occur between chips communicating through free space, or between chips connected by optical fibres.

*anthony.laing@bristol.ac.uk
†physv@nus.edu.sg
‡john.rarity@bristol.ac.uk
§jeremy.obrien@bristol.ac.uk

general quantum information tasks [26–30]. In these latter cases path encoding is typically used, enabling deterministic single-photon manipulations, in contrast to the probabilistic manipulations used in time-bin encoding. In a path-encoded chip-to-chip setup, the "which path" information is very stable, but it is unthinkable to expect interferometric stability between two separate channels connecting the Alice and Bob chips. In these and similar scenarios, our protocol leads to the generation of a secure key without aligning the frames, as long as the repetition rate of the signals is faster than the rate of change of frame.

II. THE PROTOCOL FOR TWO QUBITS

For ease of notation, we denote by $\{X,Y,Z\}$ the three Pauli matrices usually written $\{\sigma_x,\sigma_y,\sigma_z\}$. We assume that one direction is well defined, which is the case for all the usual encodings in QKD: the circular basis in polarization encoding, the time basis in time-bin encoding, and the which-path basis in path encoding. So we set $Z_A = Z_B$. The other two directions are related by $X_B = \cos\beta X_A + \sin\beta Y_A$ and $Y_B = \cos\beta Y_A - \sin\beta X_A$, where β may vary in time.

We present the protocol in its entanglement-based version where Alice and Bob share the state ρ_{AB}, which in the ideal case is the $|\phi^+\rangle$ Bell state; an equivalent prepare-and-measure version can be obtained through the usual recipe (see, e.g., Sec. II.B.2 in [7]).

In each run, Alice and Bob choose independently one of the three directions (randomly but not necessarily with the same probability) and measure the quantum signal they receive in the corresponding basis. At the end of the signal exchange they reveal their bases. The *raw key* consists of the cases where both have measured in the Z basis; so the quantum bit-error rate is given by

$$Q = \frac{1 - \langle Z_A Z_B\rangle}{2}. \tag{1}$$

To estimate Eve's knowledge, Alice and Bob need to use the information collected on the bases complementary to Z. The quantity

$$C = \langle X_A X_B\rangle^2 + \langle X_A Y_B\rangle^2 \tag{2}$$

$$+ \langle Y_A X_B\rangle^2 + \langle Y_A Y_B\rangle^2, \tag{3}$$

is independent of the relative angle β and will be used to bound Eve's knowledge. The maximal value under Pauli algebra is $C = 2$, achievable only by (a subset of) two-qubit maximally entangled states—note that, in this case, one has $Q = 0$ as well: the two parameters C and Q are not independent, as we shall see in more detail later.

Before turning to a formal security proof, it is important to understand how the protocol is affected by the fact that β may vary in time. C being a statistical quantity, its estimation requires several repetitions of the experiment. A variation of β during the run will have the effect of smearing the estimated correlations. For the protocol to be useful, therefore, Alice and Bob should collect sufficient signals to create a key above the finite-size effects [31,32], in a time short enough for β not to vary too much. Now, while the expected variations of β should be estimated to assess the feasibility of an implementation, during the run of the protocol β is not a parameter available to Alice and Bob: Its monitoring would amount to aligning the frames, which defeats the purpose. In the context of security assessment, any smearing of the correlations will be attributed to Eve's intervention.

III. SECURITY BOUND

Since β is not monitored by Alice and Bob, we have to assume the worst-case scenario. For an observed value of C, the worst-case scenario is that β is fixed and known to Eve: This way, all the smearing of the correlations is due to Eve's intervention [33]. We derive an asymptotic security bound against coherent attacks by an eavesdropper, under the assumption that the source produces a two-qubit state.

As a *first step*, we notice that Alice and Bob process each pair independently of the others. This fact, together with the assumption that we are dealing with finite-dimensional systems, guarantees that we can compute the bound by restricting to collective attacks [34,35]. Thus, each pair shared by Alice and Bob is supposed to be in the two-qubit state ρ_{AB}, of which Eve holds a purification.

The *second step* consists in proving that we can consider ρ_{AB} (or just ρ for ease of notation) to be Bell diagonal in some Bell basis known to Eve, without loss of generality. The proof is similar to the one presented in Refs. [36,37]. First, we use the fact that C is invariant under the transformation $X_A \to -X_A$, $Y_A \to -Y_A$, $X_B \to -X_B$ and $Y_B \to -Y_B$. This transformation can be implemented on ρ itself as the unitary $Z_A Z_B$. In the presence of such a symmetry, it is not restrictive to replace ρ by $\tilde\rho = \frac{1}{2}\left(\rho + Z_A Z_B \rho Z_A Z_B\right)$: Indeed, if Eve can gain some knowledge out of ρ, she can gain the same knowledge out of $Z_A Z_B \rho Z_A Z_B$; by mixing them, she can therefore gain at least the same knowledge, and maybe more because the state is more mixed. As for Alice and Bob, they do not notice any difference since they are looking *only* at Q and C. So presently we have

$$\tilde\rho_{AB} = \mu_1 P_{\Phi^+} + \mu_2 P_{\Phi^-} + \left(\frac{a}{2}|\Phi^-\rangle\langle\Phi^+| + \text{H.c.}\right)$$

$$+ \mu_3 P_{\Psi^+} + \mu_4 P_{\Psi^-} + \left(\frac{b}{2}|\Psi^-\rangle\langle\Psi^+| + \text{H.c.}\right), \tag{4}$$

where $P_\psi = |\psi\rangle\langle\psi|$ and the four states represent the usual Bell basis. For convenience of notation, let us call this state $\tilde\rho(a,b)$. Now, we have $C = 2[(\mu_1 - \mu_2)^2 + (\mu_3 - \mu_4)^2 + \text{Im}(a)^2 + \text{Im}(b)^2]$. Therefore C will be the same for the state $\tilde\rho(-a^*, -b^*)$. By the same argument as above we can then study rather the mixture $\rho' = \frac{1}{2}[\tilde\rho(a,b) + \tilde\rho(-a^*, -b^*)] = \tilde\rho(iA, iB)$ with $A = \text{Im}(a)$ and $B = \text{Im}(b)$. This last state is Bell diagonal

$$\rho'_{AB} = \sum_{k=1}^{4} \lambda_k |\Phi_k\rangle\langle\Phi_k|, \tag{5}$$

where $|\Phi_{1,2}\rangle = \frac{1}{\sqrt{2}}(e^{i\chi}|00\rangle \pm e^{-i\chi}|11\rangle)$ and $|\Phi_{3,4}\rangle = \frac{1}{\sqrt{2}}(e^{i\chi'}|01\rangle \pm e^{-i\chi'}|10\rangle)$. The parameters are related as follows. Let $A' = \sqrt{(\mu_1 - \mu_2)^2 + A^2}$: then $\lambda_{1,2} = \frac{1}{2}(\mu_1 + \mu_2 \pm A')$ and $\cos^2\chi = \frac{1}{2} + (\mu_1 - \mu_2)/A'$. The expressions of $\lambda_{3,4}$ and χ' are similar with $\mu_{3,4}$ and B. In particular, C has the same value as previously and now reads

$$C = 2[(\lambda_1 - \lambda_2)^2 + (\lambda_3 - \lambda_4)^2]. \tag{6}$$

The *third step* is now formally identical to the one for the BB84 protocol (we refer to Appendix A of [7] for details). The four nonnegative numbers λ_j are constrained by three conditions: they must sum up to 1 and yield the measured values of Q and C. This leaves one parameter free that will be chosen as to maximize Eve's information. The first two constraints are taken into account by choosing the parametrization $\lambda_1 = (1-Q)\frac{1+u}{2}$, $\lambda_2 = (1-Q)\frac{1-u}{2}$, $\lambda_3 = Q\frac{1+v}{2}$, $\lambda_4 = Q\frac{1-v}{2}$, where $u,v \in [0,1]$; in which case, Eve's information reads

$$I_E(Q,u,v) = (1-Q)h\left(\frac{1+u}{2}\right) + Qh\left(\frac{1+v}{2}\right), \qquad (7)$$

where h is binary entropy. The third constraint (6) reads $C = 2[(1-Q)^2u^2 + Q^2v^2]$ and we have to compute $I_E(Q,C) = \max_C I_E(Q,u,v)$.

First note that $I_E(0,C) = h[(1+\sqrt{C/2})/2]$. For $Q > 0$, we have $v(u) = \sqrt{C/2 - (1-Q)^2u^2/Q}$; the condition $v \in [0,1]$ translates as $u \in [u_{\min},u_{\max}]$ where $u_{\min} = \frac{1}{1-Q}\sqrt{\max[C/2 - Q^2,0]}$ and $u_{\max} = \min[\frac{1}{1-Q}\sqrt{C/2},1]$. We have not found an analytical optimization for the whole parameter range. However, Q is expected to be small in a practical implementation; and for all $Q \lesssim 15.9\%$, one can show that $\frac{d}{du}I_E\big(Q,u,v(u)\big)$ is strictly positive between $u_{\min}$ and $u_{\max}$, for all C; whereas

$$I_E(Q,C) = I_E\big(Q,u_{\max},v(u_{\max})\big). \qquad (8)$$

A rapid benchmark for qubit protocols is their robustness to white noise. For Werner states, $C = 2(1-2Q)^2$: assuming this relation, we find $I_E(Q,C) = Q + (1-Q)h\big((1-3Q/2)(1-Q)\big)$. This is exactly the same expression obtained for the six-state protocol [7,38]. The corresponding secret key rate $r = 1 - h(Q) - I_E$ is positive for $Q \lesssim 12.62\%$, so well within the validity of (8).

IV. EXTENSION TO HIGHER DIMENSIONS

Several QKD protocols using higher-dimensional quantum systems (qudits) have been proposed (see, e.g., [39]). In principle, they yield both higher key rates and larger robustness to noise. Qudit encoding in photonic states has been demonstrated using angular momentum modes [40] or time bins [41]. However, the control of the various relative phases (i.e., the stabilization of the reference frame) is very delicate: This is the reason why practical QKD has largely ignored higher-dimensional protocols. Even at the theoretical level, to our knowledge, nobody has explicitly computed security bounds against coherent attacks for these protocols, even if the general theoretical framework is, in principle, the same as for qubits.

A generalization of the rfi protocol, by removing the need for frame alignment, may provide the benefits of higher-dimensional encoding without the technical problems. Here we present such a generalization for qutrits. The derivation of rigorous security bounds for qudit protocols is a challenge in itself and is left for future work.

It is known that $d+1$ sets of mutually unbiased bases (MUB's) exist for particles of dimension d, where d is a power prime [42,43]. The joint space of any pair of qudits can be quantified by the $(d+1) \otimes (d+1)$ measurements. The protocol requires Alice and Bob to share an ensemble of qudit Bell states and randomly project their own particles onto the MUB's. Their joint computational basis outcomes provide the d-dimensional key which is impervious to the effects of a changing phase between the computational states. The joint outcomes of the complementary bases from the remaining d^2+2d measurements are used to calculate a fixed-but-unknown phase-invariant quantity C_d, the higher-dimensional analog of the qubit case C.

For example, a natural operator representation of MUB's are the so-called Weyl operators which have been studied in the context of entanglement [44–46]. In the case of the $d = 3$ qutrit the Weyl matrices are often denoted by the set of eight τ_i matrices, each of which has a conjugate transpose twin in the set, with the same eigenvectors but with two permuted eigenvalues. C_3 is calculated on the unique eigenvector half set (neglecting the key forming computational basis operators). With joint expectation values defined by $e_{ij} = \mathrm{Tr}(\tau_i \otimes \tau_j \rho_{AB})$ we find

$$C_3 = \sum_{i,=2}^{4}\sum_{j,=2}^{4} e_{ij}e_{ij}^* + \sum_{i,=2}^{4}\sum_{j,=-2}^{-4} e_{ij}e_{ij}^* \leqslant 3, \qquad (9)$$

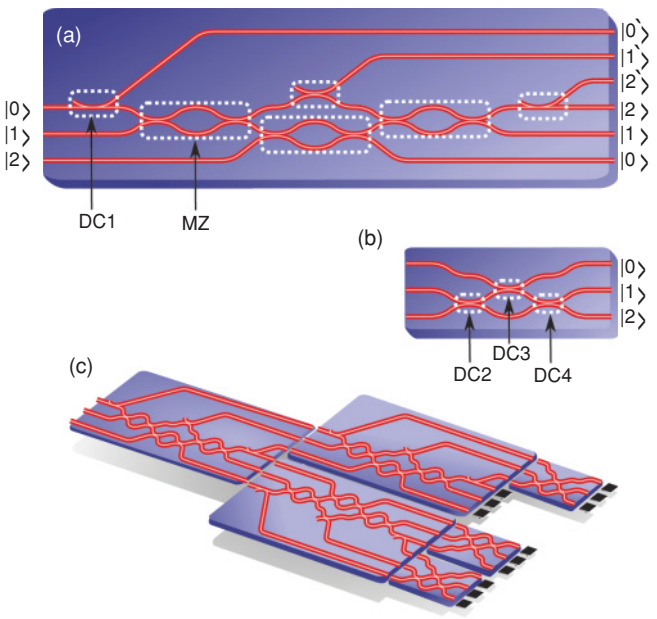

FIG. 2. (Color online) Integrated photonic components for measurement in the qutrit version of reference-frame-independent QKD. (a) The state-splitter chip takes an arbitrary qutrit input state and splits it into a superposition of two probabilistic copies. The reflectivity of directional couplers (DC) can be set to select the relative probability of the copy. Two directional couplers implement a Mach Zender interferometer (MZ) with internal phase such that a photon exits from the path opposite to the one in which it entered. (b) A qutrit Hadamard chip takes a particular equal superposition basis and rotates to the computational basis in preparation for measurement. (c) Three state-splitter chips are used to make a superposition of four probabilistic copies of the incoming states. One probabilistic copy is immediately measured in the computational basis while the other three are fed into different Hadamard chips before measurement.

where τ_1 is the computational basis operator and those operators with negative indices are the conjugate transpose twin. The maximal value is $C_3 = 3$, achievable only by (a subset of) two-qutrit maximally entangled states.

One possible physical implementation of the qutrit version of rfiQKD uses integrated photonic waveguides. The rigid monolithic structure provides phase stability between spatial modes, so while chip-to-chip communication is phase-unstable, all unitaries implemented on-chip are highly stable. With a network of variable beam splitters, or directional couplers (DC's), one can implement any unitary operator [47]. A pair of maximally entangled qutrits can be created on a single chip via post selection and with the aid of ancilla photons [48,49]; alternatively one may use a spontaneous parametric down-conversion source and select three pairs of points on the down-conversion cone [50].

To measure the incoming qutrits, Alice and Bob each require a device that randomly projects onto the four mutually unbiased bases. This device may be assembled from two types of components: a state splitter and a qutrit Hadamard gate. The state splitter is a three-input mode by six-output mode circuit that splits the incoming signal with three directional couplers of equal reflectivity and permutes the order of modes with MZ interferometers, as shown in Fig. 2(a). The qutrit Hadamard device, shown in Fig. 2(b), is composed of three directional couplers. In terms of Pauli matrices, $D_2 = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x)_{12}$; $D_3 = \frac{1}{\sqrt{3}}(\sigma_z + \sqrt{2}\sigma_x)_{01}$; $D_4 = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_y)_{12}$, where the modes acted upon are noted by the subscripts. One can confirm that $D_4 \cdot D_3 \cdot D_2$ is represented by a matrix in the Hadamard set; all other Hadamards in the set are accessible by adding phases to two of the three modes [51]. Three state splitters and three Hadamards fit together to make the random projector device shown in Fig. 2(c).

V. CONCLUSION

We have described a protocol for the exchange of a secure quantum key in an unknown and slowly varying reference frame and identified specific cases in which the protocol is useful. The two contrasting scenarios of earth-satellite links and chip-to-chip communication highlight the generality of the scheme. Further scenarios can also be envisaged, for example, rfiQKD may be useful in an environment of intermittent rapid fluctuation where the key is exchanged during the periods of relative stability without the need to realign the reference frame. We expect further situations in which rfiQKD is helpful to emerge. We have provided a security proof for the qubit version of the protocol and described how the protocol can be developed into higher dimensions, with specific details of physical implementation in the qutrit case.

ACKNOWLEDGMENTS

We thank Nicolas Brunner, Mark Godfrey, Graham Marshall, Jonathan Matthews, Alberto Peruzzo, Alberto Politi, Sandu Popescu, and Terry Rudolph for helpful discussions. This work was supported by EPSRC, QIP IRC, IARPA, ERC, the Leverhulme Trust, EU IP QAP (IST015848), the National Research Foundation, and the Ministry of Education, Singapore. J.G.R. and J.L.OB acknowledge Royal Society Wolfson Merit Awards.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, Cambridge, England, 2000).

[2] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 1994), pp. 124–134.

[3] D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).

[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[6] M. Dušek, N. Lütkenhaus, and M. Hendrych, Prog. Opt. **49**, 381 (2006).

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[8] H.-K. Lo and Y. Zhao, "Quantum cryptography" in *Encyclopedia of Complexity and System Science* (Springer, New York, 2009), Vol. 8, p. 7265.

[9] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).

[10] F. M. Spedalieri, Opt. Commun. **260**, 340 (2006).

[11] L. Aolita and S. P. Walborn, Phys. Rev. Lett. **98**, 100501 (2007).

[12] C. E. R. Souza, C. V. S. Borges, A. Z. Khoury, J. A. O. Huguenin, L. Aolita, and S. P. Walborn, Phys. Rev. A **77**, 032345 (2008).

[13] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Nat. Phys. **4**, 282 (2008).

[14] The QKD without reference-frame alignment schemes of [10–12] which make use of encoding photonic states in Laguerre-Gaussian modes, ultimately require adaptive optics to compensate for phase front distortion when transmitting through air.

[15] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, New J. Phys. **4**, 82 (2002).

[16] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature (London) **419**, 450 (2002).

[17] C.-Z. Peng *et al.*, Phys. Rev. Lett. **94**, 150501 (2005).

[18] E.-L. Miao, Z.-F. Han, T. Zhang, and G.-C. Guo, Phys. Lett. A **361**, 29 (2007).

[19] R. Ursin *et al.*, Nature Physics **3**, 481 (2007).

[20] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).

[21] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, New J. Phys. **11**, 045017 (2009).

[22] G. Maxwell, P. Townsend, K. Lear, M. Harlow, and R. Cecil, in *Proceedings of the Pacific Rim Conference on Lasers and Electro-Optics, 1999. CLEO/Pacific Rim '99* (IEEE, New York, 1999), Vol. 3, pp. 589–590.

[23] T. Honjo, K. Inoue, and H. Takahashi, Opt. Lett. **29**, 2797 (2004).
[24] H. Takesue and K. Inoue, Phys. Rev. A **72**, 041804(R) (2005).
[25] M. Fujiwara, M. Toyoshima, M. Sasaki, K. Yoshino, Y. Nambu, and A. Tomita, Appl. Phys. Lett. **95**, 261103 (2009).
[26] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, Science **320**, 646 (2008).
[27] J. C. F. Matthews, A. Politi, A. Stefanov, and J. L. O'Brien, Nature Photon. **3**, 346 (2009).
[28] A. Politi, J. C. F. Matthews, and J. L. O'Brien, Science **325**, 1221 (2009).
[29] G. D. Marshall, A. Politi, J. C. F. Matthews, P. Dekker, M. Ams, M. J. Withford, and J. L. O'Brien, Opt. Express **17**, 12546 (2009).
[30] B. J. Smith, D. Kundys, N. Thomas-Peter, P. G. R. Smith, and I. A. Walmsley, Opt. Express **17**, 13516 (2009).
[31] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[32] R. Y. Cai and V. Scarani, New J. Phys. **11**, 045024 (2009).
[33] If, on the contrary, β would be known to vary, part of the smearing of C could be attributed to this effect: That part would not have to be removed in privacy amplification. In other words, the best-case scenario would consist in attributing all the smearing to variations of β and declare that the state is actually always maximally entangled.
[34] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[35] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[36] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[37] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[38] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[39] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[40] G. Molina-Terriza, A. Vaziri, J. Řeháček, Z. Hradil, and A. Zeilinger, Phys. Rev. Lett. **92**, 167903 (2004).
[41] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **93**, 010503 (2004).
[42] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).
[43] W. K. Wootters and B. D. Fields, Annals of Physics **191**, 363 (1989).
[44] R. A. Bertlmann and P. Krammer, J. Phys. A **41**, 235303 (2008).
[45] A. B. Klimov, D. Sych, L. L. Sánchez-Soto, and G. Leuchs, Phys. Rev. A **79**, 052101 (2009).
[46] A. Kalev, F. C. Khanna, and M. Revzen, Phys. Rev. A **80**, 022112 (2009).
[47] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[48] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[49] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn, Phys. Rev. A **65**, 012314 (2001).
[50] R. Ceccarelli, G. Vallone, F. De Martini, P. Mataloni, and A. Cabello, Phys. Rev. Lett. **103**, 160401 (2009).
[51] G. J. Pryde and A. G. White, Phys. Rev. A **68**, 052315 (2003).