



Faithful Entanglement Swapping Based on Sum-Frequency Generation

Nicolas Sangouard, Bruno Sanguinetti, Noé Curtz, Nicolas Gisin, Rob Thew, and Hugo Zbinden

Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

(Received 17 December 2010; published 22 March 2011)

We show that an entanglement swapping operation performed with spontaneous parametric down-conversion can be made faithful without postselection using sum-frequency generation. This invites us to revisit the sum-frequency process and from a proof-of-principle experiment, we demonstrate that it provides a realistic solution for nonlinear optics at the single-photon level. This opens the way to attractive alternatives to six-photon protocols based on linear optics used, e.g., for the heralded creation of maximally entangled pairs or for device-independent quantum key distribution.

DOI: 10.1103/PhysRevLett.106.120403

PACS numbers: 03.65.Ud, 03.67.Bg, 03.67.Hk, 42.50.Ex

Introduction.—A fascinating feature of entanglement is that it can be swapped [1]. Given two entangled photons, say the photons A and B , and another entangled pair C and D [see Fig. 1], it is possible to entangle A and D by performing a joint measurement of photons B and C in the Bell basis, provided that the result of the measurement is communicated to A and D . Hence, the two latter photons end up entangled even though they have never interacted.

The most natural approach to implement an entanglement swapping operation would be to use pair sources based on spontaneous parametric down-conversion (SPDC) and linear optical elements to perform a partial Bell measurement. This would allow one to realize a heralded entangled pair source—the success of the Bell measurement serving as the heralding event for the creation of an entangled pair. However, the emission of multipairs, inherent to SPDC, inevitably reduces the fidelity of the state conditioned on a successful Bell measurement, cf. below. This makes the entanglement swapping protocol useless in practice without postselection. Actually, it has been shown that the heralded production of a maximally entangled photon pair using only conventional SPDC sources, linear optics, and projective measurements, requires at least three entangled pairs [2], making the practical realization very challenging [3]. Here we show that the entanglement swapping operation with pairs coming from SPDC sources can be made faithful if the Bell measurement uses sum-frequency generation (SFG). Such a process can effectively serve as a nonlinear filter, inhibiting multipair emissions that would otherwise corrupt the Bell state measurement. SFG has already exhibited its usefulness in quantum information, e.g., to perform a complete Bell state discrimination [4], to characterize broadband entangled photons [5], to highlight the shaping of entangled-photon waveform [6] and for frequency conversion of single photons [7]. We demonstrate from a proof-of-principle experiment that the SFG in a nonlinear waveguide with two broadband photons can be efficient enough to make our proposal attractive with respect to six-photon schemes that are required, e.g., to herald the

creation of maximally entangled pairs from SPDC sources [8]. Furthermore, since SFG can be driven by telecom wavelengths, our proposal can be used to herald the creation of entangled pairs at a distance. This offers a competitive alternative to linear optics based solutions to overcome the problem of losses in device-independent quantum key distribution [9].

Failure of entanglement swapping with SPDC and linear optics.—We first recall the principle of entanglement swapping with SPDC sources and linear optics, by choosing the time degree of freedom (the discussion would be similar for other degrees of freedom). In SPDC, a strong light pulse is sent through a nonlinear crystal and with a small probability p_{ab} , a photon from the beam decays into two photons, one into the spatial mode A , the other one into B , such that energy and momentum are conserved. If the nonlinear crystal is pumped by two coherent pulses [10], the photon pair is created in a coherent superposition of two modes, the early e and late ℓ modes, with a delay corresponding to the one between the two pump pulses, i.e., the so-called time-bin entanglement. Taking the double-pair emission into account, the resulting state is well described by

$$\begin{aligned} \rho_{ab} \approx & |00\rangle\langle 00| + p_{ab} \left| \frac{a_e^\dagger b_e^\dagger - a_\ell^\dagger b_\ell^\dagger}{\sqrt{2}} \right\rangle \left\langle \frac{a_e^\dagger b_e^\dagger - a_\ell^\dagger b_\ell^\dagger}{\sqrt{2}} \right| \\ & + \frac{3p_{ab}^2}{4} \left| \frac{(a_e^\dagger b_e^\dagger - a_\ell^\dagger b_\ell^\dagger)^2}{2\sqrt{3}} \right\rangle \left\langle \frac{(a_e^\dagger b_e^\dagger - a_\ell^\dagger b_\ell^\dagger)^2}{2\sqrt{3}} \right| \\ & + o(p_{ab}^3). \end{aligned} \quad (1)$$

A second source, located far away from the previous one, is pumped simultaneously to produce another time-bin entangled pair in modes C and D with the probability p_{cd} . The corresponding state ρ_{cd} is similar to the state ρ_{ab} with a and b replaced by c and d , respectively. The modes B and C are then combined on a 50-50 beam splitter. The modes after this beam splitter are $\delta_{e/\ell} = \frac{1}{\sqrt{2}}(b_{e/\ell} + c_{e/\ell})$ and $\bar{\delta}_{e/\ell} = \frac{1}{\sqrt{2}}(b_{e/\ell} - c_{e/\ell})$. We are interested in the detection of two photons—for example, one in δ_e and one in $\bar{\delta}_\ell$.

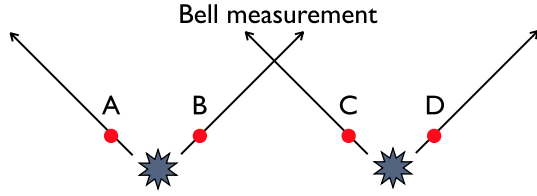


FIG. 1 (color online). Basic scheme for entanglement swapping. Sources (stars) produce entangled pairs, A - B and C - D . The projection of B and C in the Bell basis entangles the photons A and D .

Let us consider separately the different contributions. If one pair is emitted from each of the sources, the expected detections can be produced with probability $\frac{1}{8}P_{ab}P_{cd}$ [11] and the resulting state $\frac{1}{\sqrt{2}}(a_e^\dagger d_\ell^\dagger - a_\ell^\dagger d_e^\dagger)|0\rangle$ corresponds to the desired entanglement of remote photons A and D . However, the terms associated to the emission of two pairs from the same source may also produce a photon in δ_e and another one in δ_ℓ with probability $\frac{1}{16}P_{ab}^2$ ($\frac{1}{16}P_{cd}^2$). Such detections project the remaining modes A and D onto $a_e^\dagger a_\ell^\dagger|0\rangle$ ($d_e^\dagger d_\ell^\dagger|0\rangle$), respectively). Hence, neglecting the terms associated to the emission of more than two pairs, the conditional state shared by A and D

$$\begin{aligned} \rho_{\text{swap}} = & \frac{1}{16}P_{ab}^2|a_e^\dagger a_\ell^\dagger\rangle\langle a_e^\dagger a_\ell^\dagger| \\ & + \frac{1}{16}P_{cd}^2|d_e^\dagger d_\ell^\dagger\rangle\langle d_e^\dagger d_\ell^\dagger| + \frac{1}{8}P_{ab}P_{cd} \\ & \times \left| \frac{1}{\sqrt{2}}(a_e^\dagger d_\ell^\dagger - a_\ell^\dagger d_e^\dagger) \right\rangle \left\langle \frac{1}{\sqrt{2}}(a_e^\dagger d_\ell^\dagger - a_\ell^\dagger d_e^\dagger) \right| \quad \text{A} \quad (2) \end{aligned}$$

is poorly entangled; i.e., its fidelity with respect to a maximally entangled state $F = \langle \frac{1}{\sqrt{2}}(a_e^\dagger d_\ell^\dagger - a_\ell^\dagger d_e^\dagger) | \rho_{\text{swap}} | \frac{1}{\sqrt{2}}(a_e^\dagger d_\ell^\dagger - a_\ell^\dagger d_e^\dagger) \rangle$ is upper bounded by $1/2$. To mitigate the multipair problem, one usually postselects the events corresponding to one detection at both ends (A and D). However, postselection of this kind strongly limits the applications arising from the entanglement swapping operations. For example, they do not allow for the heralded creation of entangled pairs and they are incompatible with device-independent quantum key distribution since they inevitably open the detection loophole; cf. below.

Principle of our proposal.—To overcome the limitation due to the multipair emission, we propose using a nonlinear process for the Bell measurement. Figure 2 shows the setup that we have in mind. The modes B and C , with well distinct frequencies, are combined into a nonlinear medium at the central station. With a small probability, one photon in B combines with one photon in C to create a photon in K with a frequency corresponding to the sum of frequencies B and C . Note that if two input photons come from the same mode, they cannot create a photon in K due to energy conservation. This is at the heart of an attractive Bell measurement that we detail in what follows. Consider

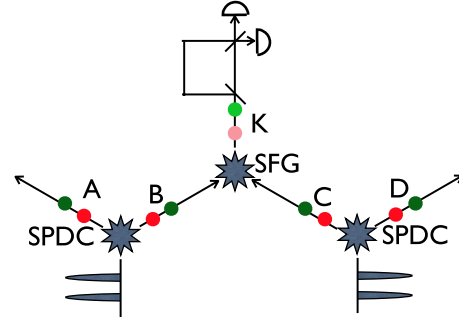


FIG. 2 (color online). Proposed setup for faithful entanglement swapping. The Bell measurement is based on SFG followed by an interferometer (made with one optical switch and one beam splitter) to erase the which-path information; cf. text for details.

two temporal modes: the early and late modes as before. The SFG can generate a photon in K only if the input photons arrive at the same time. Hence, it is described by the Hamiltonian $H = i\alpha(\kappa_e^\dagger b_e c_e - \kappa_\ell^\dagger b_\ell c_\ell) + \text{H.c.}$ where κ_e and κ_ℓ are associated with the photons created by the early and late modes, respectively. The coupling constant α contains the material nonlinear susceptibility and the beam geometry. Let us start with $\rho_{ab} \otimes \rho_{cd}$ where ρ_{ab} and ρ_{cd} are as before (1). The dynamics is given by $\mathbb{1}_{ad} \times e^{-iHt}$ where $\mathbb{1}_{ad}$ is the identity for the modes A and D . Neglecting the terms associated with the emission of more than two pairs, one finds that the state resulting from a successful SFG is given by $\frac{1}{\sqrt{2}}(a_e^\dagger \kappa_\ell^\dagger d_\ell^\dagger - a_\ell^\dagger \kappa_e^\dagger d_e^\dagger)|0\rangle$. To erase the information on the creation time, the modes κ_e and κ_ℓ are then sent into an unbalanced Mach-Zehnder interferometer. The detection of one photon in $\frac{1}{\sqrt{2}}(|\kappa_e^\dagger\rangle + |\kappa_\ell^\dagger\rangle)$ projects the state of the remaining modes into $\frac{1}{\sqrt{2}}(a_e^\dagger d_e^\dagger - a_\ell^\dagger d_\ell^\dagger)|0\rangle$, i.e., in a maximally entangled state. This offers interesting opportunities, e.g., to distribute entanglement at a distance in a heralded way, cf. below. Taking the detection of one photon in $\frac{1}{\sqrt{2}}(|\kappa_e^\dagger\rangle - |\kappa_\ell^\dagger\rangle)$ into account, the success probability is given by $\frac{1}{2}\eta_{\text{SFG}}P_{ab}P_{cd}$ where $\eta_{\text{SFG}} = (\alpha\tau)^2$ is the SFG efficiency, τ being the characteristic interaction time between the photons and the nonlinear medium. This provokes the natural question: is SFG efficient enough to be useful?

Heralded entangled-pair source.—The setup presented in Fig. 2 allows one to conditionally prepare a maximally entangled state of two photons—the successful preparation being unambiguously heralded by the detection of a single photon resulting from the SFG. Alternative proposals associated with this endeavor, but based on linear optics only, require the coincident detection of at least four auxiliary photons [2]. We focus on the proposal presented in Ref. [8] which is the only one performed experimentally [3] so far. It uses the six-photon component of the SPDC output. Specifically, a nonlinear crystal produces two beams containing photons with pairwise correlated polarizations.

A fourfold coincident detection performed on a fraction of the output beams, picked off with variable beam splitters (which transmit a photon with a probability $\cos^2\theta$) leaves the remaining modes in a maximally entangled state. Taking the four-pair emission into account as well as the nonunit detection efficiency η of the auxiliary photons, the fidelity of the heralded pair is well approximated by $F \approx \frac{\cos^4\theta}{(1-\eta\sin^2\theta)^2} [1 - \frac{13}{4}p(1-\eta\sin^2\theta)^2]$ in the limit where the success probability p for the creation of one pair is small. The success probability for the fourfold coincidence is given by $P \approx \frac{1}{4}p^3\eta^4\sin^8\theta(1-\eta\sin^2\theta)^2[1 + \frac{13}{4}p(1-\eta\sin^2\theta)^2]$ [12]. Note that $\eta = \eta_c\eta_d$ contains the efficiency with which a photon is coupled into a monomode fiber η_c and the detection efficiency η_d . If we assume an overall detection efficiency $\eta = 0.6$, and if we require the fidelity of the entangled pairs to be $F \geq 0.9$, one finds the optimal values $p = 1.5 \times 10^{-2}$ and $\cos^2\theta = 0.93$ leading to $P \approx 3 \times 10^{-12}$. For comparison with our proposal, we account for the nonunit coupling efficiency η_c of modes B and C and for the nonunit detection efficiency $\eta = \eta_c\eta_d$ of mode K . One finds that one entangled-photon pair with fidelity $F \approx 1 - 3p$ is heralded with probability $P \approx \frac{1}{2}\eta_c^2\eta\eta_{\text{SFG}}p^2(1+3p)$ where $p = p_{ab} = p_{cd}$. For $\eta_c = \eta_d = \sqrt{0.6}$, $P \approx 3 \times 10^{-12}$, and $F \geq 0.9$ are achieved for $p \approx 3.3 \times 10^{-2}$ provided that the efficiency of the SFG is $\eta_{\text{SFG}} \geq 1.4 \times 10^{-8}$. Note that for lower detection efficiencies, for example $\eta = 0.4$, which is still higher than the overall detection efficiency reported in [3], $\eta_{\text{SFG}} \geq 3.1 \times 10^{-9}$ is sufficient for our proposal to achieve the same rate of entangled states (with $F \geq 0.9$) than the one based solely on linear optics.

Potential application in quantum key distribution.—An attractive feature of the swapping operation described above is that it can be performed at a distance. This is particularly useful to overcome the problem of transmission losses in device-independent quantum key distribution (DI-QKD) [13] where the secrecy of the key relies solely on the violation of a Bell inequality. However, a necessary condition to insure the security in DI-QKD is to close the detection loophole. This is a major challenge in optical Bell tests, since the detection efficiency, i.e., the product of the transmission efficiency (including the coupling into the fiber) and the photon-detector efficiency, required to rule out attacks based on the detection loophole is very high, typically larger than 82.8% for the Clauser-Horne-Shimony-Holt (CHSH) [14] inequality in the absence of other limitations. Even assuming perfect photodetection and lossless components, the transmission efficiency of a 5 km-long optical fiber at telecom wavelength is roughly of 80%. Transmission losses thus represent a fundamental limitation for the realization of a detection-loophole free Bell test on any distance relevant for QKD.

The unique proposal allowing one to circumvent the problem of transmission losses requires three photon pairs, linear optical elements, and projective measurements [9].

The performance of this scheme has been evaluated for a DI-QKD protocol based on the CHSH inequality [15]. Here, we focus on the case where the detectors are trusted. By considering a fiber attenuation of 0.2 dB/km, corresponding to telecom wavelength photons, a coupling efficiency of $\eta_c = 0.9$, a detection efficiency $\eta_d = 0.8$, and sources with a repetition rate of 10 GHz, the proposal of Ref. [9] achieves a rate of about 7 bits/min on a distance of 10 km.

Alternatively, SFG provides a simpler solution requiring only two pairs. The principle is shown in Fig. 3. An entangled-pair source is located close to Alice's location. Each of Alice's and Bob's locations includes a measurement apparatus. Furthermore, Bob's box contains an entangled-pair source and a nonlinear crystal suitable for SFG. When a photon is detected after the SFG crystal, Bob knows that he shares an entangled state with Alice. Performing a measurement only when he gets a heralding signal, Alice and Bob can safely discard all the events where a photon got lost in the quantum channel. Consequently, the overall detection efficiency required to close the detection loophole does not depend anymore on the transmission efficiency but merely reduces to the intrinsic detection efficiency of Alice's and Bob's measurement apparatus. Taking the finite coupling and detection efficiency into account ($\eta_c = 0.9$ and $\eta_d = 0.8$ as before), one finds for a distance of 10 km, the optimal values $p_{ab} \approx p_{cd} = 3.7 \times 10^{-2}$ so that a key rate of 7 bits/min is achieved provided that the efficiency of SFG is $\eta_{\text{SFG}} \geq 6 \times 10^{-7}$.

Efficiency of SFG.—Parametric processes at the single-photon level have usually been considered too inefficient to be of practical interest. Nevertheless, recent experiments have put these processes to good use demonstrating the direct generation of photon triplets [16] and efficient second harmonic generation using entangled pairs [6].

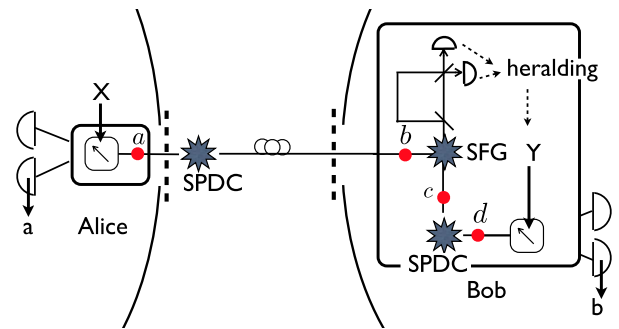


FIG. 3 (color online). Proposed setup to overcome the problem of transmission losses in DI-QKD. Each Alice and Bob boxes includes a measurement apparatus allowing them to choose a measurement (X and Y , respectively) and to obtain outputs (a and b). If the resulting probability distribution $P(ab|XY)$ violates the CHSH inequality by a sufficient amount, a key can be distilled from the remaining data. Since Bob inputs a Y only when a SFG photon is detected, Alice and Bob can safely discard all events where a photon is lost during the transmission.

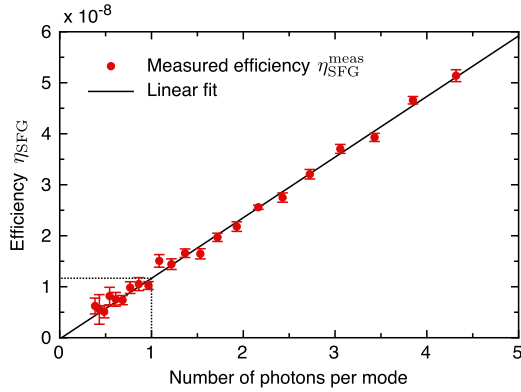


FIG. 4 (color online). Probability η_{SFG} that a signal photon ($\lambda = 1563$ nm, $\Delta\lambda = 0.3$ nm) is upconverted when interacting with a weak pump ($\lambda = 1557$ nm, $\Delta\lambda = 1.2$ nm) inside the waveguide, plotted against the number of photons per mode (equal for pump and signal). Experimentally pump and signal photons are obtained by attenuating and filtering a light-emitting diode. Upconverted photons are separated from the residual pump using a prism, they are then detected with a single photon detector (IDQ ID100, 6% efficiency). Dark counts (2.2 Hz) have been subtracted, and injection (3 dB), reflection (0.6 dB), and propagation (0.2 dB) losses have been taken into account.

Classically, the efficiency of SFG is proportional to the pump power P_{pump} and the square of the crystal length L^2 . Commercially available nonlinear waveguides offer high normalized SFG efficiencies $\hat{\eta} \approx 100\%/(\text{W} \cdot \text{cm}^2)$ [17]. Consider that the pump power is reduced so that a single photon is present per temporal mode. In this regime, the power of the input beam can be calculated as the energy of each photon divided by its coherence time, i.e., $P_{\text{pump}} = h\nu\Delta\nu/\text{tbp}$, where $\Delta\nu$ is the photon bandwidth and tbp is the time-bandwidth product. Furthermore, the bandwidth $\Delta\nu$ is limited by group velocity dispersion, and decreases linearly with the length of the crystal, i.e., $\Delta\nu = \hat{\Delta}\nu/L$ where $\hat{\Delta}\nu$ is the spectral acceptance of the crystal. The overall conversion efficiency when the full bandwidth of the crystal is used, is given by $\eta_{\text{SFG}}^{\text{th}} = \hat{\eta} \hat{\Delta}\nu h\nu L/\text{tbp}$. We experimentally verified that this equation holds by injecting a pair of one-photon-per-mode beams at 1557 nm and 1563 nm into a 2.6 cm periodically poled lithium niobate waveguide with an acceptance bandwidth of $\hat{\Delta}\nu = 300$ GHz \cdot cm and measuring the rate of 780 nm output photons [see Fig. 4].

In our experiment $\hat{\eta} = 15\%/(\text{W} \cdot \text{cm}^2)$ and $\text{tbp} = 0.66$, so that the expected efficiency is $\eta_{\text{SFG}}^{\text{th}} \approx 1 \times 10^{-8}$. We measured an efficiency of $\eta_{\text{SFG}}^{\text{meas}} = 1.2(0.2) \times 10^{-8}$. Hence, with a more appropriate commercial waveguide, 5 cm long and $\hat{\eta} = 100\%/(\text{W} \cdot \text{cm}^2)$ [17], one could realistically get $\eta_{\text{SFG}}^{\text{th}} \approx 1.5 \times 10^{-7}$. With the research device presented in Ref. [18] [10 cm, $\hat{\eta} = 150\%/(\text{W} \cdot \text{cm}^2)$] the efficiency would increase to $\eta_{\text{SFG}}^{\text{th}} \approx 5 \times 10^{-7}$. Note that the efficiency could further be improved using group velocity matching [19], higher spatial confinement of

the modes [20], or the use of highly nonlinear organic materials [21].

Conclusion.—In conclusion, we have shown how SFG can make the entanglement resulting from entanglement swapping faithful. Despite long-held preconceptions, we have demonstrated that the SFG efficiency is high enough to provide efficient, yet simpler solutions to linear optics based protocols for the heralded production of entangled states or for the implementation of DI-QKD.

We thank M. Afzelius, J.-D. Bancal, C. Clausen, C. Osorio, H. de Riedmatten, S. Pironio, Y. Silberberg, and C. Wagenknecht for helpful discussions. We acknowledge support by the ERC-AG QORE and the Swiss NCCR Quantum Photonics.

- [1] M. Zukowski *et al.*, *Phys. Rev. Lett.* **71**, 4287 (1993).
- [2] P. Kok and S.L. Braunstein, *Phys. Rev. A* **62**, 064301 (2000).
- [3] C. Wagenknecht *et al.*, *Nat. Photon.* **4**, 549 (2010); S. Barz *et al.*, *Nat. Photon.* **4**, 553 (2010).
- [4] Y.-H. Kim, S.P. Kulik, and Y. Shih, *Phys. Rev. Lett.* **86**, 1370 (2001).
- [5] B. Dayan *et al.*, *Phys. Rev. Lett.* **94**, 043602 (2005).
- [6] A. Pe'er *et al.*, *Phys. Rev. Lett.* **94**, 073601 (2005); F. Zah *et al.*, *Opt. Express* **16**, 16452 (2008).
- [7] S. Tanzilli *et al.* *Nature (London)* **437**, 116 (2005); R. T. Thew *et al.*, *Appl. Phys. Lett.* **93**, 071104 (2008).
- [8] C. Sliwa and K. Banaszek, *Phys. Rev. A* **67**, 030101(R) (2003).
- [9] N. Gisin, S. Pironio, and N. Sangouard, *Phys. Rev. Lett.* **105**, 070501 (2010).
- [10] J. Brendel *et al.*, *Phys. Rev. Lett.* **82**, 2594 (1999).
- [11] For our purpose, the transmission losses and the nonunit efficiency of the single-photon detectors are not relevant.
- [12] This formula and the one for the fidelity are extensions of those given in Ref. [8] which take the four-pair emission into account.
- [13] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991); D. Mayers and A. C. Yao, *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, New York, 1998), p. 503; J. Barrett, L. Hardy, and A. Kent, *Phys. Rev. Lett.* **95**, 010503 (2005); A. Acin *et al.*, *Phys. Rev. Lett.* **97**, 120405 (2006); M. McKague, *New J. Phys.* **11**, 103037 (2009); L. Masanes, *Phys. Rev. Lett.* **102**, 140501 (2009).
- [14] J.F. Clauser *et al.*, *Phys. Rev. Lett.* **23**, 880 (1969).
- [15] A. Acin, N. Gisin, and L. Masanes, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [16] H. Hubel *et al.*, *Nature (London)* **466**, 601 (2010). Note that it is not straightforward to extend this scheme for the heralded generation of remote entanglement.
- [17] HC Photonics Corporation <http://www.hcphotonics.com>.
- [18] K.R. Parameswaran *et al.*, *Opt. Lett.* **27**, 179 (2002).
- [19] N.E. Yu *et al.*, *Opt. Lett.* **27**, 1046 (2002).
- [20] S. Kurimura *et al.*, *Appl. Phys. Lett.* **89**, 191123 (2006).
- [21] M. Jazbinsek *et al.*, *IEEE J. Sel. Top. Quant.* **14**, 1298 (2008).