optica

Quantum-memory-assisted multi-photon generation for efficient quantum information processing

FUMIHIRO KANEDA,[1,*] FEIHU XU,[2] JOSEPH CHAPMAN,[1] AND PAUL G. KWIAT[1]

[1]Department of Physics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801, USA
[2]Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
*Corresponding author: fkaneda@illinois.edu

Received 15 June 2017; revised 1 August 2017; accepted 2 August 2017 (Doc. ID 298089); published 25 August 2017

Efficient preparation of large, but definite, numbers of photons is of great importance for scaling up and speeding up photonic quantum information processing. Typical single-photon generation techniques based on nonlinear parametric processes face challenges of probabilistic generation. Here we demonstrate efficient synchronization of photons from multiple nonlinear parametric heralded single-photon sources, using quantum memories. Our low-loss optical memories greatly enhance (∼30×) the generation rate of coincidence photons from two independent sources, while maintaining high indistinguishability (95.7 ± 1.4%) of the synchronized photons. As an application, we perform the first demonstration of parametric-source-based measurement-device-independent quantum key distribution. The synchronization technique demonstrated here paves the way toward efficient quantum communication and larger-scale optical quantum computing.

OCIS codes: (270.0270) Quantum optics; (270.5585) Quantum information and processing; (270.5565) Quantum communications; (270.5290) Photon statistics.

https://doi.org/10.1364/OPTICA.4.001034

In the last two decades, many quantum optics experiments have demonstrated small-scale quantum information processing applications with several photons [1–3]. For further scaling up and speeding up photonic quantum information processing, however, highly efficient generation of pure and indistinguishable photons is essential. Solid-state single-emitter sources [4] such as quantum dots and nitrogen-vacancy centers, in addition to requiring cryogenic cooling, suffer from source inhomogeneity and difficulty achieving high-efficiency collection of emitted photons into a single spatial mode, e.g., optical fiber. For this reason, quantum optics experiments have typically used nonlinear optical parametric sources due to experimental convenience and their stable performances. However, these cannot generate single-photon pairs deterministically; for a mean number of photon pairs μ, the generation probability of k photon pairs is $\mu^k/(\mu+1)^{k+1}$. Therefore, the single-pair generation probability peaks at only 25% due to the non-negligible likelihood ($\sim\mu^k$) of unwanted zero- and multiple-pair generations. For example, a recent 10-photon experiment [5] using five spontaneous parametric downconversion (SPDC) sources needed to keep $\mu < 0.05$ to suppress the multi-pair emissions, resulting in a 10-photon coincidence rate of only several events per hour.

Here we employ quantum memories (QMs) to synchronize such probabilistic parametric sources to efficiently generate multiple simultaneous single photons, as shown in Fig. 1(a). M parametric sources pumped with a period τ generate photon pairs probabilistically, though in general not simultaneously. Each parametric source works as a heralded single-photon source (HSPS) in which photons generated in a trigger mode are sent to a single-photon detector (SPD), whose click "heralds" in which time slot the corresponding twin photon is present. Each QM triggered by a heralding signal from its corresponding HSPS stores heralded photons for an arbitrary integer time of τ, until other sources produce their pairs. After the last source heralds a "last-born" photon, the $M-1$ memories storing the earlier-born photons release them simultaneously, thereby producing M simultaneous photons. Given each source's heralding probability per pump pulse $p \sim \mu\eta \ll 1$ (where η is the system detection efficiency of the trigger mode), a maximum number of storage time slots N, and lossless QMs, the M-fold coincidence probability is given by $\{1-(1-p)^N\}^M \simeq (pN)^M$. Hence, one can obtain up to $\times N^{M-1}$ enhancement over a non-synchronized case that requires M sources to simultaneously herald M photons (with probability $p^M N$). Theoretical details of the synchronization scheme are discussed in Refs. [6,7] and Supplement 1. Related schemes have been demonstrated by using optical parametric oscillators [8] and atomic ensembles [9]; however, our pulsed-pump scheme is advanced in high-speed capability and low loss, which determine the net rate enhancement. Note that this synchronization scheme even has a higher generation rate compared to recently demonstrated *periodic* time-multiplexed HSPSs [10–12]: M periodic time-multiplexed sources need to wait for periodic output time windows even if all QMs have loaded photons earlier. In contrast, our proposed scheme needs to store $M-1$ photons only for the *difference* of the generation time slots, substantially reducing total storage loss in imperfect (and practical) QMs. Also, the synchronization process can be repeated immediately after the last source heralds its photon.

Our scheme in general can be applied to multiple HSPSs not only in a local laboratory together but also in remote locations; the former case is very useful for quantum computing applications [13–15], while the latter has great potential for realizing efficient quantum networking. Particularly, synchronized remote sources can be directly applicable to an important quantum communication application—measurement-device-independent quantum key distribution (MDI-QKD) [16]—that is secure against all detector side-channel attacks. Our proposed MDI-QKD scheme with QMs is depicted in Fig. 1(b). In general MDI-QKD, Alice and Bob, who want to share secure cryptographic keys with each other, both need to simultaneously send qubit-encoded photons to Charlie, who identifies the correlation between Alice's and Bob's qubits (but not those qubits themselves) via Bell-state measurement (BSM), i.e., projection measurement of them into the Bell-state basis. Therefore, since MDI-QKD requires two-photon coincidences in the BSM, efficient simultaneous generation of single-photon states is more critical to realize high secure key rate, while a traditional BB84 protocol in principle needs only one single-photon source (but then requires additional assumptions about the detectors [17]). In our scheme, in addition to the standard BSM configuration, Charlie possesses a QM module so that an early-arrival photon from Alice's (Bob's) HSPS is delayed to be sent to the BSM setup simultaneously with a late-arrival photon from Bob's (Alice's) source. Thus, the success event rate of the BSM and thereby the secure key rate and transmission distance are significantly increased compared to the standard (non-synchronized) case [18,19].

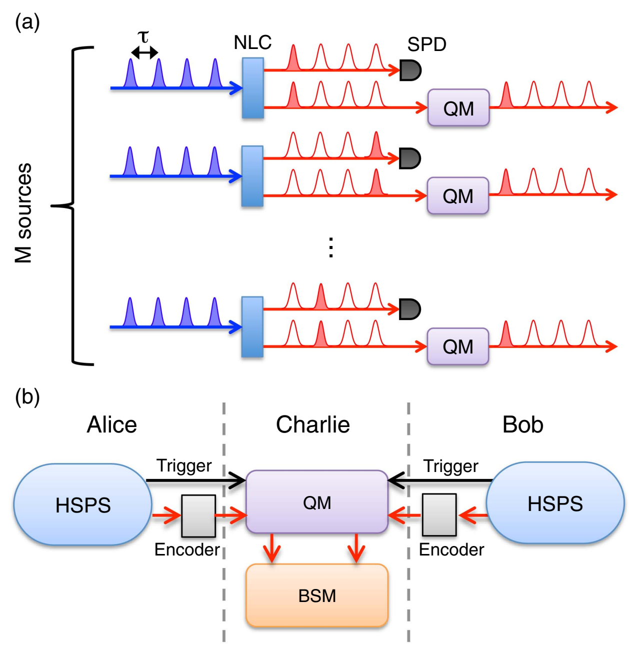

Fig. 1. (a) A scheme to generate M single photons from M HSPSs synchronized by quantum memories. NLC, nonlinear crystal; SPD, single-photon detector; QM, quantum memory. NLCs in general produce single-photon pairs only rarely, and thus simultaneous M-photon generation occurs only with very low probability. QMs can compensate for the relative delay of photons from each source, and release them simultaneously. (b) Our proposed MDI-QKD scheme, in which Charlie can synchronize the photons from two remote HSPSs. In MDI-QKD, Alice and Bob each possess qubit encoders and probabilistic single-photon sources, e.g., HSPSs or faint laser sources. Charlie receives Alice's and Bob's photons, performing a Bell-state measurement (BSM) on them. Informed by Charlie's observation of the Bell state, Alice and Bob know the specific correlation between their respective qubits, perform post-processing, and generate a shared secure key. Therefore, in MDI-QKD, efficient simultaneous generation of single-photon states is more critical to produce higher secure key rates than in a traditional BB84 protocol. A QM module in our scheme delays an early-arrival photon to be sent to the BSM setup simultaneously with a late-arrival photon.

A schematic diagram of our experiment for synchronizing two HSPSs is shown in Fig. 2. Our HSPSs [20] pumped by a common pulsed laser source (with period $\tau = 10$ ns) generate heralded photons at 1590 nm with 96% spectral indistinguishability. We operated the pair generation rate at $\mu = 0.013$ per pulse, for which the SPDC multi-pair contribution to the total coincidence counts was limited to ~4%. Our QM, consisting of a bulk optics delay cavity with a matched cycle length τ and a high-speed polarization switch (a Pockels cell, PC), has 98.8% transmission per cycle. Incorporating two fiber optic circulators, the QM can delay photons coming from *either* of the HSPSs for an arbitrary integer time of τ (see Supplement 1). Due to the low switching rate (1 MHz) of the PC, the synchronization process is not repeated immediately after synchronizing two photons, but after a fixed cycle (every 1 μs).

Figures 3(a) and 3(b) show, respectively, synchronized trigger signal rates from two HSPSs and two-photon coincidence count rates versus N. The synchronized trigger signal rate increases approximately as N^2 as expected; an $\sim N^2$ increase is also observed for the two-photon coincidence count rates, due to the high storage efficiency. Without the synchronization process, we observed a coincidence count rate of only 121 ± 6 per 100 s with the pump repetition rate of $1/\tau = 100$ MHz. We determined the enhancement factor for the two-photon coincidence count rate as the ratio of the synchronized and non-synchronized case's coincidence count rates per pump pulse [see Fig. 3(c)]; the enhancement factor increases almost linearly as N, and $\times 30.5 \pm 1.6$ enhancement was obtained with $N = 40$. Note that this same approach, generalized to preparing, e.g., 10 simultaneous photons, would have an enhancement factor of $30.5^9 = 2.28 \times 10^{13}$. Our results are in agreement with the theoretical predictions, shown as solid lines in Figs. 3(a)–3(c) (see Supplement 1).

We characterized the indistinguishability of the synchronized photons by Hong–Ou–Mandel interference (HOMI) [21], of which visibility is a direct measure, and essential for BSM (as will be demonstrated). Our observed HOMI with $N = 40$, as well as the best-fit theoretical curve [20], is shown in Fig. 3(d). The estimated visibility and dip width after subtracting background counts (23.2 counts for each data point) were $95.7 \pm 1.5\%$ and 6.00 ± 0.02 ps, respectively, which closely matches our prediction based on the observed joint spectral intensities of the HSPSs (see Supplement 1); the background counts are mainly due to the multi-photon emissions. This high HOMI visibility indicates that our QM well preserves the time-bandwidth characteristics ($\Delta t = 6.1$ ps, $\Delta\lambda = 0.8$ nm) and indistinguishability of the heralded photons.

Last, we apply our synchronization technique to demonstrate proof-of-concept MDI-QKD with time-bin-encoded heralded single photons. Note that polarization qubits are not switchable because our QM switches polarization to control a photon's delay, so instead we use time-bin encoding (see Supplement 1).

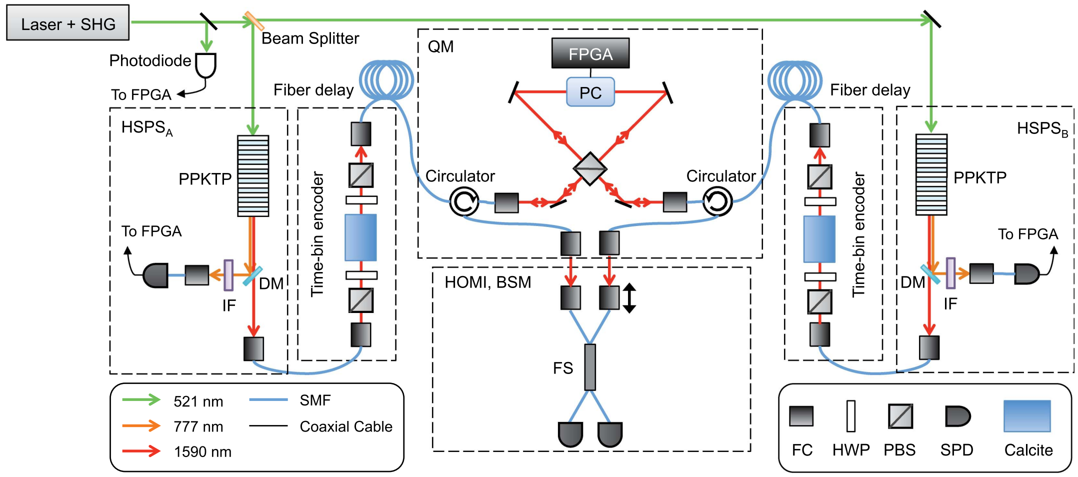

Fig. 2. Schematic diagram of our experimental setup, with FC, fiber coupler; HWP, half-wave plate; PBS, polarizing beam splitter; SPD, single-photon detector; PC, Pockels cell; IF, interference filter ($\Delta\lambda = 1.1$ nm); DM, dichroic mirror; SMF, single-mode fiber; FPGA, field-programmable gate array; and FS, fiber splitter. See Supplement 1 for experimental details.

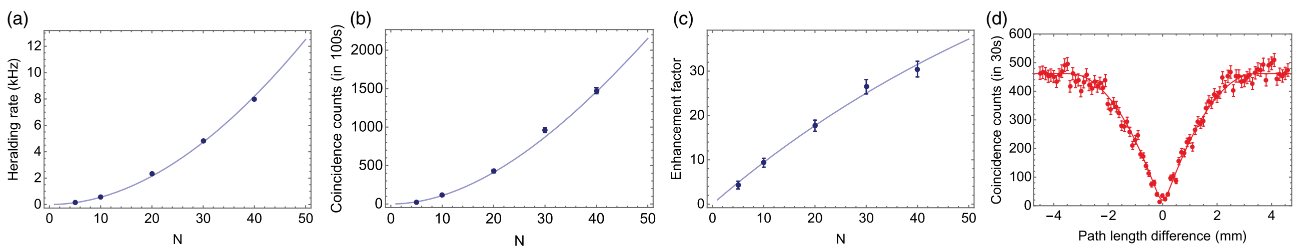

Fig. 3. (a) Synchronized trigger signal rate, (b) coincidence count rate of synchronized heralded photons, and (c) enhancement factor of coincidence count rates in the synchronized case compared to the asynchronous case, versus maximum storage cycle number N. (d) Observed HOMI for synchronized photons, with $N = 40$. Error bars are estimated by Poissonian photon counting statistics.

Figures 4(a) and 4(b) show experimental results of the BSM for the early-/late-qubit basis $\{|e\rangle, |l\rangle\}$ and their superposition basis $\{|+\rangle, |-\rangle\}$, where $|e\rangle \perp |l\rangle$, $|\pm\rangle = (|e\rangle \pm |l\rangle)/\sqrt{2}$. Coincidence events are collected for $N_p = 4 \times 10^9$ pump pulses. With our BSM setup projecting two qubits onto a singlet state $|\psi^-\rangle \equiv (|el\rangle - |le\rangle)/\sqrt{2} = (|+-\rangle - |-+\rangle)/\sqrt{2}$, our observed coincidence counts (without subtracting background counts) from identical qubits are only ~8% of those from orthogonal qubits, due to high-visibility HOMI (~92%). Note that these highly suppressed error count rates depend on the low multi-photon contributions (~4%); in contrast, previous demonstrations [22–26] of MDI-QKD with weak coherent pulses could only have 50% HOMI visibility because of their large photon-number noise.

Based on the result of the BSM, we estimate the lower bound of secure key rate $R = 2.12 \times 10^{-8}$ bit per pump pulse (corresponding to 0.851 bit/s with our 1-MHz system repetition rate) over an equivalent loss, i.e., the total loss of two optical channels from each SPDC crystal to the first circulator, of ~14 dB. See Supplement 1 for details of secure key rate evaluations. For comparison, we also performed our MDI-QKD experiment without synchronization. Although a similar distribution of coincidence counts is observed [see Figs. 4(c) and 4(d)], no positive key could be guaranteed because of the large uncertainty in the estimates of the QKD bit error rates, due to ~30× fewer photon count rates

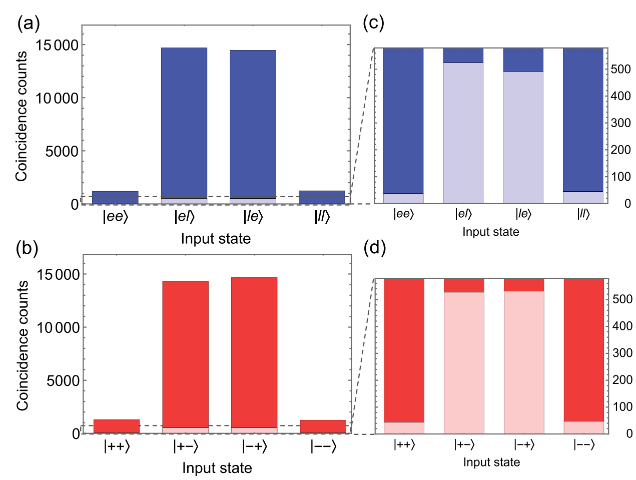

Fig. 4. Coincidence counts (without subtracting background counts) from BSM of different time-bin encoded photons. (a) $\{|e\rangle, |l\rangle\}$ basis. (b) $\{|+\rangle, |-\rangle\}$ basis. We observed very high contrast in coincidence count rates, implying low quantum bit error rates. (c) and (d) are enlarged figures of (a) and (b), showing the corresponding coincidence counts without synchronization, in light colors; while error probabilities are similar, the count rates are ~30× lower. Coincidence counts are collected for $N_p = 4 \times 10^9$ pump pulses in each data point.

compared to the synchronized case. Therefore, the enhanced coincidence count rate with our synchronization technique is critical to enable useful HSPS-based MDI-QKD.

Our current secure key generation rate could be enhanced by a factor of ~250 by several improvements on our current physical setup (see Supplement 1). In addition, we expect that employing decoy-state methods would allow us to use much higher values of μ, thereby further increasing the secure key rate [18,19]. Furthermore, passive decoy-state methods [27,28] can be applied for HSPS-based MDI-QKD to remove active decoy intensity modulations.

Extending our current setup would allow us to generate up to 10 synchronized single photons with a reasonably high generation rate ($\gtrsim 1/\mathrm{s}$). An even larger number of photons can be generated by reducing optics loss in both the trigger and heralded photons; we predict that generation rates up to 30 coincident photons every few seconds should be possible, a 23-order-of-magnitude improvement over current state of the art [5]. See Supplement 1 for the details of our prediction. Although we demonstrated this memory-assisted scheme with bulk optics, our scheme can be compatible with integrated optics having a great scalability in terms of the physical implementation. However, mitigating loss in such integrated optics remains a challenge.

In conclusion, we have demonstrated QM-assisted synchronization of multiple HSPSs for efficiently generating multiple single-photon states. Our synchronization scheme can be applied with both local and remote HSPSs; the former is valuable for larger-scale quantum computing, while the latter has great potential for realizing efficient and low-noise quantum communication. We observed greatly enhanced coincidence count rates as well as high indistinguishability of photons from two synchronized HSPSs. Moreover, for the first time, we obtained secure keys via HSPS-based MDI-QKD, with the help of the source synchronization. We anticipate that these synchronization methods will pave the way toward larger-scale optical quantum computation and communication applications.

Funding. National Science Foundation (NSF) (PHY 12-12439, PHY 15-20991); Army Research Office (ARO) (DURIP W911NF-12-1-0562, W911NF-13-1-0402); Office of Naval Research (ONR) (MURI N00014-13-1-0627).

See Supplement 1 for supporting content.

REFERENCES

1. J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski, Rev. Mod. Phys. **84**, 777 (2012).
2. M. Tillmann, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Nat. Photonics **7**, 540 (2013).
3. A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvão, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, Nat. Photonics **7**, 545 (2013).
4. I. Aharonovich, D. Englund, and M. Toth, Nat. Photonics **10**, 631 (2016).
5. X.-L. Wang, L.-K. Chen, W. Li, H. L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z. E. Su, D. Wu, Z. D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N. L. Liu, Y.-A. Chen, C.-Y. Lu, and J.-W. Pan, Phys. Rev. Lett. **117**, 210502 (2016).
6. J. Nunn, N. K. Langford, W. S. Kolthammer, T. F. M. Champion, M. R. Sprague, P. S. Michelberger, X. Jin, D. G. England, and I. A. Walmsley, Phys. Rev. Lett. **110**, 133601 (2013).
7. M. Gimeno-Segovia, H. Cable, G. J. Mendoza, P. Shadbolt, J. W. Silverstone, J. Carolan, M. G. Thompson, J. L. O'Brien, and T. Rudolph, New J. Phys. **19**, 063013 (2017).
8. K. Makino, Y. Hashimoto, J.-I. Yoshikawa, H. Ohdan, T. Toyama, P. van Loock, and A. Furusawa, Sci. Adv. **2**, e1501772 (2016).
9. D. Felinto, C. W. Chou, J. Laurat, E. W. Schomburg, H. De Riedmatten, and H. J. Kimble, Nat. Phys. **2**, 844 (2006).
10. F. Kaneda, B. G. Christensen, J. J. Wong, H. S. Park, K. T. McCusker, and P. G. Kwiat, Optica **2**, 1010 (2015).
11. G. J. Mendoza, R. Santagati, J. Munns, E. Hemsley, M. Piekarek, E. Martín-López, G. D. Marshall, D. Bonneau, M. G. Thompson, and J. L. O'Brien, Optica **3**, 127 (2016).
12. C. Xiong, X. Zhang, Z. Liu, M. J. Collins, A. Mahendra, L. G. Helt, M. J. Steel, D. Y. Choi, C. J. Chae, P. H. W. Leong, and B. J. Eggleton, Nat. Commun. **7**, 10853 (2016).
13. P. Kok, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).
14. S. Aaronson and A. Arkhipov, in *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing* (ACM, 2011), p. 333.
15. A. M. Childs, D. Gosset, and Z. Webb, Science **339**, 791 (2013).
16. H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
17. H. K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
18. S. Abruzzo, H. Kampermann, and D. Bruß, Phys. Rev. A **89**, 012301 (2014).
19. C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, New J. Phys. **16**, 043005 (2014).
20. F. Kaneda, K. Garay-Palmett, A. B. U'Ren, and P. G. Kwiat, Opt. Express **24**, 10733 (2016).
21. C. Hong, Z. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
22. A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
23. T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).
24. Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).
25. L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W. B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Nat. Photonics **10**, 312 (2016).
26. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **117**, 190501 (2016).
27. Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).
28. W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305 (2007).