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 ($95.7 \pm 1.4\%$) 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.** © 2017 Optical Society of America

***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 $\mu$, 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 $\tau$ 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 $\tau$, 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 $\eta$ 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].

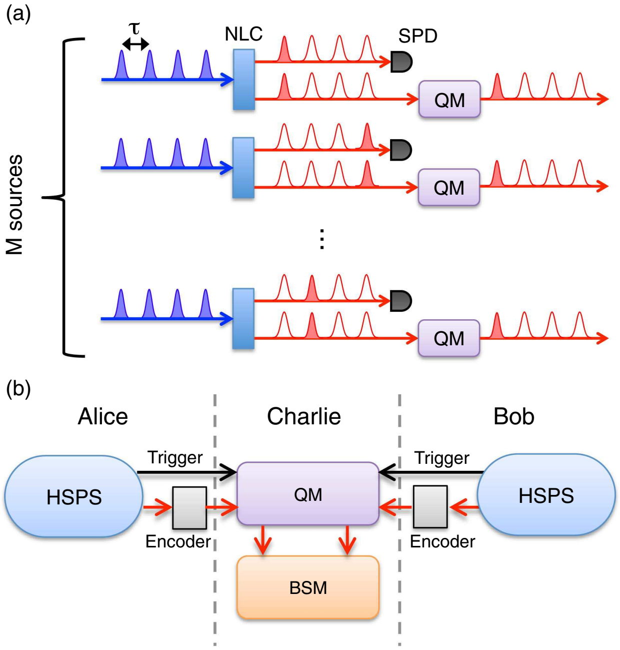

**Fig. 1.** (a) A scheme to generate $M$ single photons from $M$ HSPSs synchronized by quantum memories. NLC, nonlinear crystal; SPD, single-photon detector; QM, quantum memory. NLCs in general produce single-photon pairs only rarely, and thus simultaneous $M$-photon generation occurs only with very 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 $\tau$ 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 $\tau$ (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 ×30.5  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  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, $\Delta$  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).

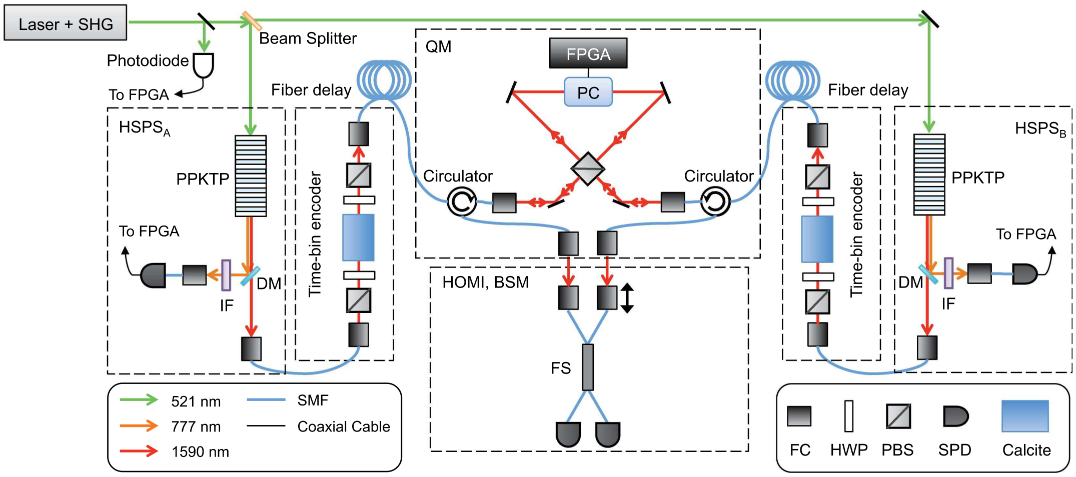

**Fig. 2.** Schematic diagram of our experimental setup, with FC, fiber coupler; HWP, half-wave plate; PBS, polarizing beam splitter; SPD, single-photon detector; PC, Pockels cell; IF, interference filter (Δ   1.1 nm); DM, dichroic mirror; SMF, single-mode fiber; FPGA, field-programmable gate array;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

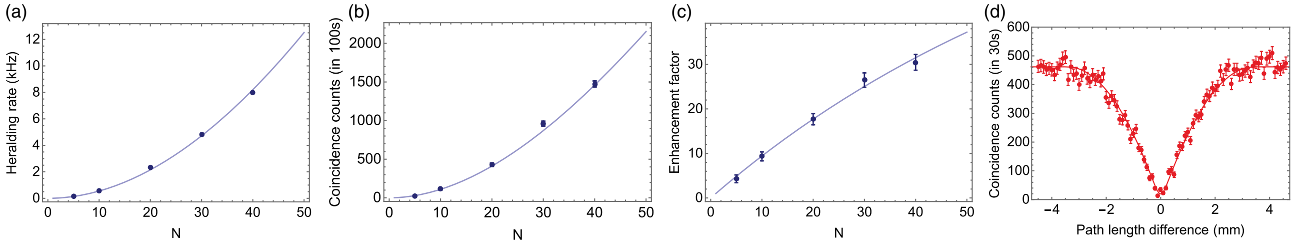

**Fig. 3.** (a) Synchronized trigger signal rate, (b) coincidence count rate of synchronized heralded photons, and (c) enhancement factor of coincidence count rates in the synchronized case compared to the asynchronous case, versus maximum storage cycle number $N$. (d) Observed HOMI for synchronized 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 $|e\rangle \quad |l\rangle$, $| \quad \rangle \quad (|e\rangle \quad |l\rangle)/\sqrt{2}$. Coincidence events are collected for $N_p \quad 4 \times 10^9$ pump pulses. With our BSM setup projecting two qubits onto a singlet state $| \ ^{-}\rangle \quad (|el\rangle - |le\rangle)/\sqrt{2} \quad (|+-\rangle - |-+\rangle)/\sqrt{2}$, 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 $R \quad 2.12 \times 10^{-8}$ 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

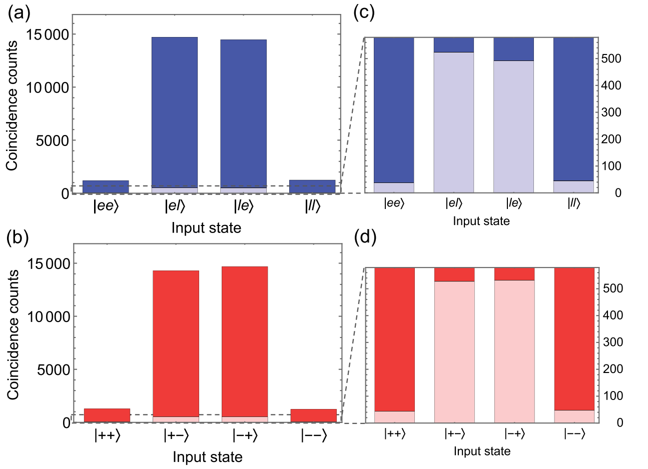

**Fig. 4.** Coincidence counts (without subtracting background counts) from BSM of different time-bin encoded photons. (a) $\{|e\rangle, |l\rangle\}$ basis. (b) $\{|+\rangle, |-\rangle\}$ basis. We observed very high contrast in coincidence count rates, implying low quantum bit error rates. (c) and (d) 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 $N_p \quad 4 \times 10^9$ 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 $\mu$, 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 ( 1/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).

192.17.210.33 {ts '2017-10-12 10:47:31'}

optica

# Quantum-memory-assisted multi-photon generation for efficient quantum information processing: supplementary material

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, IL 61801, USA
[2] Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
[*] Corresponding author: fkaneda@illinois.edu

Published 25 August 2017

**This document provides supplementary information to "Quantum-memory-assisted multi-photon generation for efficient quantum information processing," https://doi.org/10.1364/optica.4.001034.** © 2017 Optical Society of America

https://doi.org/10.6084/m9.figshare.5270905

## 1. EXPERIMENTAL DETAILS

### A. Heralded single-photon source

We used a frequency-doubled mode-locked Yb laser ( $= 521$ nm, $= 10.0$ ns) to pump two 20-mm-long periodically-poled potassium titanyl phosphate (PPKTP) crystals each of which generates collinear photon pairs centered at 777 and 1590 nm via SPDC. We used a shared pump merely for a convenience, not necessity; it is feasible to have independent but locked pump lasers [1]. The spectral purity is estimated to be 97% after filtering the original 2.5-nm bandwidth of the 777-nm mode with 1.1-nm bandpass filters. Due to the spectral filtering, we observed largely different transmissions in the two SPDC modes after a collection SMF; the transmission for the heralded (1590-nm) mode is 88%, while only 30% for the trigger (777-nm) mode. Each trigger detector, a Si avalanche photodiode, has a →60% detection efficiency and 10 $^{6}$ background count rate per 1-ns coincidence window.

### B. Quantum memory and synchronization procedure

We implemented a bulk-optics-based QM, consisting of a 10-ns delay loop, custom Brewster-angled PBS, and PC comprising a pair of rubidium titanyl phosphate (RTP) crystals. The two PBS inputs allow the QM to delay photons from either of the sources, with photons from different HSPSs always cycling in opposite directions in the optical delay cavity. A field-programmable gate array (FPGA) module processes input signals from trigger SPDs, triggering the PC to store/release early-born photons. When an early-born photon from either source enters into the cavity, the PC is activated, rotating that photon's polarization by 90 to store and delay it in the cavity. To switch a photon from one HSPS into and out of the QM without affecting a potential photon from the other HSPS, the two sources have a time-slot offset by $/2 = 5$ ns, greater than the 4-ns rise/fall time of our PC. After delaying the early-born photon for the necessary integer multiples of , photons from the two HSPS are synchronously emitted (but offset by $/2$) from the different ports of the PBS, each coupling to a fiber circulator that directs it to a fiber splitter (whose input arm lengths are chosen to remove the $/2$ offset between the two photons). The single-pass cavity transmission $T_c$ is 98.8%, and the corresponding photon lifetime in the QM is →830 ns (i.e., 83 cycles for $1/e$ total switching transmission). The slightly imperfect cavity transmission is due to the transmission of the PC (99.2%) and the reflection of the two concave mirrors (99.8%). The group-velocity dispersion in the QM cavity is very small (→1.2 10 $^{3}$ ps$^{2}$ at 1590 nm) compared to the photon coherence time ( $t = 6.1$ ps); thus, the cycle-dependent chromatic dispersion, which could degrade indistinguishability of the synchronized photons, is negligible for up to $N = 40$. Our QM cavity built with high-mechanical-stability optics mounts in a temperature-stabilized laboratory has a small long-term cycle length drift (→0.01 ps per hour), much less than $t = 6.1$ ps. Thus, our QM can maintain high indistinguishability of heralded single photons from different sources. Note that we do not need to have phase stabilization of the QM cycle length since HOMI, a key effect in many quantum information application, is typically insensitive to phase, depending only on spectral-temporal indistinguishability of the photons. Each fiber delay line can hold photons for →500 ns to compensate for the electronic latencies (→ 100 ns from a trigger photon to firing the PC). In addition, the rest of the delay ($>$ 400 ns) after the compensation allows us to select the *latest* heralded time slot (for up to $N = 40$) of the first-heralding HSPS, thus minimizing the effective storage loss in the QM [2] (for example, if HSPS$_A$ produces photons in time slots 3 and 29, and HSPS$_B$ produces a photon in slot 31, we only need to store the second HSPS$_A$ photon for 2 cycles instead of 28).

### C. Time-bin encoder

A time-bin qubit state is created by using a common-path polarization-dependent unbalanced interferometer. For this proof-of-concept MDI-QKD experiment, no random number generator or fast active switch is used to encode qubits. Horizontally polarized photons generated from an HSPS first pass through a HWP with its optic axis at either 0°, 45°, 22.5°, or $-22.5°$, respectively creating the horizontal, vertical, diagonal, or anti-diagonal state ($|H\rangle$, $|V\rangle$, $|D\rangle$, or $|A\rangle$), where $|H\rangle \perp |V\rangle$, $|D\rangle \equiv (|H\rangle + |V\rangle)\sqrt{2}$, and $|A\rangle \equiv (|H\rangle - |V\rangle)\sqrt{2}$. A pair of 40-mm-long calcite crystals provides a group delay ($\sim$ 25 ps) between $|H\rangle$ and $|V\rangle$ without transverse walk-off, correlating the polarization state to a temporal one, i.e., $|H\rangle \rightarrow |H\rangle|e\rangle, |V\rangle \rightarrow |V\rangle|l\rangle$. This group delay is much larger than $\Delta t$ but much smaller than the 4-ns switching rise/fall time of our PC, so that both time-bin states can be efficiently switched in the PC. A HWP at 22.5° after the calcite crystals rotates the polarization from $|H\rangle$ ($|V\rangle$) to $|D\rangle$ ($|A\rangle$), and a following PBS transmits only $|H\rangle$. Thus, time-bin qubit states ($|e\rangle$, $|l\rangle$, $|+\rangle \equiv (|e\rangle + |l\rangle)/\sqrt{2}$, $|-\rangle \equiv (|e\rangle - |l\rangle)/\sqrt{2}$) with an identical polarization state $|H\rangle$ are successfully generated with a 50% postselection probability; the overall transmission including optics loss, fiber coupling efficiency, and this postselection, is about 22%.

### D. Measurement of synchronized photons

In order to perform the HOMI experiment as well as the BSM, we implemented an interferometer with a 50:50 fiber splitter. The path length difference between the two fiber input mode is adjusted to be zero by translating one of input fiber couplers. Coincidence counts of the synchronized photons are measured by two fiber-coupled superconducting nanowire detectors (SNSPDs) with ∼75% detection efficiency and $\sim 10^{-6}$ dark count probability per 1-ns coincidence window. This setup with zero path-length difference and coincidence measurements performs as a BSM projecting onto $|\psi^-\rangle \equiv (|el\rangle - |le\rangle)/\sqrt{2} = (|+-\rangle - |-+\rangle)/\sqrt{2}$ for time-bin qubits [3–5]. For the measurement of coincidence counts versus $N$ shown in Fig. 3(b) in the main text, we used the large path-length difference (∼15 mm) of the interferometer to avoid two-photon interference.

## 2. SPECTRAL CHARACTERIZATION OF HSPSS

In order to estimate an attainable visibility of our HOMI measurement, we measured joint spectral intensities (JSIs) of the two SPDC sources (see Fig. S1), using frequency-resolved optical parametric amplification [6, 7]. As shown in Fig. S1, the SPDC sources have a very similar JSI, each of which is estimated to generate heralded single-photons with 97.1% purity, assuming for no spectral phase shift in the JSI. We then estimate the final indistinguishability of the heralded photons from the two independent sources to be 96.4%; our experimental visibility (95.7 ± 1.5%) is very close to this estimate.

## 3. THEORY OF SYNCHRONIZED HSPSS

Here we show theoretical details of $M$ synchronized HSPSs with imperfect optical components. We first define following probabilities:

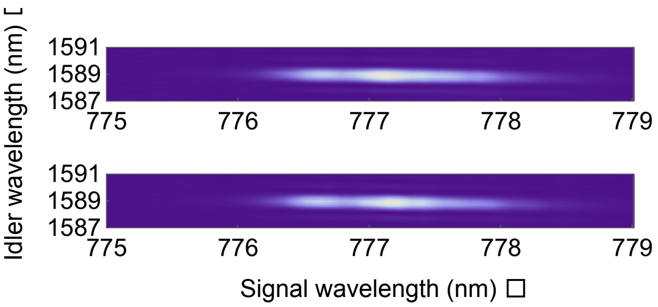

**Fig. S1.** Observed JSI for two SPDC sources.

$$P_c(k) = \frac{\mu^k}{(1+\mu)^{k+1}}, \tag{S1}$$

$$P_d(k) = \sum_{l=1}^{k} \eta_d^l (1-\eta_d)^{k-l} \binom{k}{l} \left(\frac{1}{D}\right)^{l-1}, \tag{S2}$$

$$P_e(k'|k,j,j') = (T_c T_{QM}^{j-j'+1})^{k'} (1 - T_c T_{QM}^{j-j'+1})^{k-k'} \binom{k}{k'}. \tag{S3}$$

$P_c(k)$ is the probability that an SPDC source generates $k$-photon pairs; for an SPDC source generating pure heralded photons, its photon number statistics follow a thermal distribution. $P_d(k)$ is the probability of a trigger detector click, given that an SPDC source generates a $k$-photon state. $\eta_D$ is the total transmission of the signal photons from the SPDC crystal to SPDs, and $D$ is the number of SPDs used for a trigger-detector cascade to herald idler photons. Here, we assume that the SPDs are "bucket" detectors that only discriminate between zero and one-or-more photons, and the detector cascade distributes the signal photons to $D$ detectors with an equal probability ($1/D$). $P_e(k'|k,j,j')$ is the idler photon's transmission to an output time slot, where $T_{QM}$ denotes the storage efficiency in a QM for a delay time $\tau$, and $T_c$ is the net transmission of the other optics (including an initial delay line, fiber coupling efficiency, etc.).

We also define $P_h(j)$ as the probability that one HSPS heralds at least one single photon within $j$ time slots:

$$P_h(j) = 1 - \{1 - P_h(1)\}^j, \tag{S4}$$

$$P_h(1) = \sum_{k=1}^{\infty} P_c(k) P_d(k). \tag{S5}$$

With the above definitions, the probability that all $M$ HSPS's synchronously generate single photons, is given by

$$P_s(M) = P_l(1|1)^M + \sum_{j=2}^{N} \sum_{q=1}^{M} \binom{M}{q} P_l(1|j)^q P_e(1|j)^{M-q}, \tag{S6}$$

$$P_l(1|j) = (1 - P_h(j-1)) \sum_{k'=1}^{\infty} P_c(k') P_d(k') P_t(1|k',j,j), \tag{S7}$$

$$\begin{aligned} P_e(1|j) = & \sum_{j'=1}^{j-1} (1 - P_h(j-1-j')) \\ & \times \sum_{k'=1}^{\infty} P_c(k') P_d(k') P_t(1|k',j,j')(1 - P_h(1)) \\ & + P_h(j-1) \sum_{k'=1}^{\infty} P_c(k') P_d(k') P_t(1|k',j,j). \end{aligned} \tag{S8}$$

**Table S1.** Experimental parameters and predicted $M$-photon coincidence rates in this work and feasible values with efficient components. The values in ( ) are for our current setup without the time-bin encoders, the HOMI setup, and the bandpass filters in the trigger modes.

| Description | Symbol | Value in this work | Value with efficient components |
|---|---|---|---|
| Mean photon number per pulse | | 0.013 | — |
| Trigger-mode system detection efficiency | $_t$ | 0.18 (0.47) | 0.84 |
| Number of detectors in a trigger-photon mode | $D$ | 1 | 4 |
| Optical channel transmission | $T_c$ | 0.083 (0.63) | 0.85 |
| Quantum memory transmission | $T_{QM}$ | 0.988 | 0.988 |
| HOMI/BSM detector efficiency | $_d$ | 0.75 | 0.93 |
| Maximum number of storage time slots | $N$ | 40 | 100 |
| Repetition rate of synchronization processes (MHz) | $R$ | 1 | 1 |
| Predicted $M$-photon coincidence rate (/s) | | | |
| $M = 2, \ \ = 0.013$ | $P_s(2)R$ | $1.4\ \ 10^1$ $(1.5\ \ 10^3)$ | $2.2\ \ 10^5$ |
| $M = 2, \ \ = 0.050$ | $P_s(2)R$ | $(6.9\ \ 10^4)$ | $5.4\ \ 10^5$ |
| $M = 5, \ \ = 0.050$ | $P_s(5)R$ | $(9.2\ \ 10^2)$ | $1.2\ \ 10^5$ |
| $M = 10, \ \ = 0.050$ | $P_s(10)R$ | $(6.4\ \ 10^{\ 1})$ | $1.0\ \ 10^4$ |
| $M = 20, \ \ = 0.050$ | $P_s(20)R$ | $(3.0\ \ 10^{\ 7})$ | $5.7\ \ 10^2$ |
| $M = 30, \ \ = 0.050$ | $P_s(30)R$ | $(8.3\ \ 10^{\ 11})$ | $3.2\ \ 10^{\ 1}$ |

where $N$ is the maximum number of storage time slots. $P_l(k\ j)$ is the probability that an HSPS initially heralds and generates a $k$-photon state in the $j$-th time slot, while $P_e(k\ j)$ is the probability of heralding at least one time within $j\ \ 1$ time slots and then emitting a $k$-photon state at the $j$-th time slot. The first and second term in Eq. (S6) describe, respectively, the probabilities that all $M$ sources generating single photons in the first time slot and from the second to the $N$-th time slots.

For $M = 2$, as used for our experiment, we extended Eq. Eq. (S6) to calculate multi-photon emission probabilities from each HSPS. The probability of Source A and B respectively producing $k_A$ and $k_B$ photons is given by

$$P_s(k_A,k_B) = P_l(k_A\ 1)P_l(k_B\ 1) + \overset{N}{\underset{j=2}{\ }}\ P_l(k_A\ j)P_e(k_B\ j) + P_l(k_B\ j)P_e(k_A\ j) + P_l(k_A\ j)P_l(k_B\ j)\ \ . \qquad \textbf{(S9)}$$

The experimental parameters used for our theoretical estimations as well as predicted $M$-photon coincidence rates are shown in Table S1. Our predictions with the above equations are in excellent agreement with the experimental results for $M = 2$ (see Fig. 3 a,b,c in the main text). Due to lossy components (i.e., two time-bin encoders, HOMI setup, and bandpass filters in each trigger modes) in our current setup, we predicted and observed a two-photon coincidence rate of only →14 /s; clearly, this is not scalable for generating larger number of photons. However, we can remove the lossy time-bin encoders and HOMI setup for multi-photon generation purposes. Also, our heralded single photons still have a high spectral indistinguishability (91%) even without the bandpass filters [7] (although the residual distinguishability would make it difficult to generate secure keys in our MDI-QKD experiment). We predict that observing up to 10 photon coincidences with a reasonably high success rate ($\gtrsim$ 1 /s) is possible by implementing our setup without such lossy optics and increasing  from 0.013 to 0.05 (and still retain the ratio of multi-photon states to single-photon states is →5% for each HSPS). Note that a recent ten-photon experiment [8] has observed only 0.003 /s with  →0.05. We also estimated $M$-photon coincidence rates, assuming feasible and more efficient technologies: high-efficiency (93%) SNSPDs [9] for both the trigger and heralded modes, long delay fibers holding photons for 100 pump pulse cycles, and a number of HSPS linked to independent QM cavities, so that slightly lossy fiber circulators (85% transmission for each) could be eliminated. Those feasible improvements will enable 30-photon coincidences every few seconds.

## 4. SECURE KEY RATE EVALUATION AND POSSIBLE IMPROVEMENTS IN THE MDI-QKD EXPERIMENT

We determined the gain and quantum bit error rate (QBER) respectively as $Q_W = (C_{00} + C_{11} + C_{01} + C_{10})/N_p$, $e_W = (C_{00} + C_{11})/(C_{00} + C_{11} + C_{01} + C_{10})$, where $W\ \ [Z = \ \ e\ ,\ l\ \ , X = \ \ +\ ,\ \ \ ]$ is the basis choice, and $C_{ij}$ $(i,j\ \ \ 0,1\ )$ is the number of coincidence counts for input qubits $\ ij\ $, given a total number of pump pulses $N_p$ [10]. In our proof-of-principle implementation, a lower bound of secure key rate $R$ is estimated by assuming that our HSPS is an ideal single-photon source (i.e., ignoring the low multi-pair contributions):

$$R = Q_Z^L\ \ 1\ \ \ h(e_X^U)\ \ \ f_e h(e_Z^U)\ \ . \qquad \textbf{(S10)}$$

**Table S2.** Experimental MDI-QKD quantities and estimated key rate.

| | With synchronization | Without synchronization |
|---|---|---|
| $Q_Z$ ( $10^{7}$ per pulse) | 1.976 0.033 | 0.0688 0.0060 |
| $Q_X$ ( $10^{7}$ per pulse) | 1.969 0.033 | 0.0718 0.0062 |
| $e_Z$ | 0.0771 0.0045 | 0.0747 0.0237 |
| $e_X$ | 0.0797 0.0046 | 0.0791 0.0239 |
| $N_p$ | 4 $10^{9}$ | 4 $10^{9}$ |
| $R$ ( $10^{7}$ per pulse) | 0.212 | -0.00107 |

Here, $Q_Z^L$, $e_X^U$, $e_Z^U$ are the lower (L) and upper (U) bounds of gain and QBER due to statistical fluctuations (we consider 3 standard deviations); $h(x) = \quad x \log x \quad (1 \quad x)\log(1 \quad x)$ is the binary entropy, and $f_e = 1.16$ is the error correction inefficiency factor [11]. Our observed QKD parameters as well as estimated secure key rates $R$ are shown in Table S2.

We expect that our current observed secure key rate can be increased by a factor of →500 by using efficient optics, a deterministic time-bin encoding method, and decoy-state method with parameter optimizations. Since we used this postselective method for simplicity of implementation (see Methods), each time-bin encoder has only 22% transmission; however, lossless and deterministic encoding can be achieved, for example, by using time-bin entangled photon sources instead of an HSPS, detecting trigger photons with projection onto corresponding time-bin states. $e_Z$ can be reduced to $< 1\%$ by extending the time bin's separation from our current 25 ps to 200 ps such that SNSPDs can resolve time-bin states. This has already been demonstrated in previous weak-coherent-pulse(WCP)-based MDI-QKD experiments [3–5]. Our BSM setup has only →60% transmission due to the high fiber-coupling loss; employing free-space BSM would make this loss negligibly small. Overall, these improvement would increase $Q_z$ and $Q_x$ by a factor of $(0.22 \quad 0.6)^{\;2} = 57$, reduce $h(e_z)$ from 0.408 to $< 0.081$, and therefore $R$ increased by a factor of →250. In addition, decoy-state methods together parameter optimizations can substantially increase the secure key rate, potentially by as much as another factor of →10–20. The resulting $R$ could then be →$10^{\;5}$ bit per pulse, which is comparable to WCP-based MDI-QKD experiments [3–5, 12–14]. Finally, a faster Pockels cell which can repeat a synchronization process immediately after previous one, is able to increase the success event rate of the BSM as well as the secure key rate *per second* by a factor of 2.5.

## REFERENCES

1. R. Kaltenbaek, B. Blauensteiner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger, "Experimental Interference of Independent Photons," Phys. Rev. Lett. **96**, 240502 (2006).
2. F. Kaneda, *et al.*, "Time-Multiplexed Heralded Single-Photon Source," Optica **2**, 1010 (2015).
3. A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks," Phys. Rev. Lett. **111**, 130501 (2013).
4. Y. Liu, *et al.*, "Experimental measurement-device-independent quantum key distribution," Phys. Rev. Lett. **111**, 130502 (2013).
5. H.-L. Yin, *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett. **117**, 190501 (2016).
6. B. Fang, O. Cohen, M. Liscidini, J. E. Sipe, and V. O. Lorenz, "Fast and highly resolved capture of the joint spectral density of photon pairs," Optica **1**, 281 (2014).
7. F. Kaneda, K. Garay-Palmett, A. B. U'Ren, and P. G. Kwiat, "Heralded single-photon source utilizing highly nondegenerate, spectrally factorable spontaneous parametric downconversion," Opt. Express **24**, 10733 (2016).
8. X.-L. Wang, *et al.*, "Experimental Ten-Photon Entanglement," Phys. Rev. Lett. **117**, 210502 (2016).
9. F. Marsili, *et al.*, "Detecting single infrared photons with 93% system efficiency," Nature Photon. **7**, 210 (2013).
10. H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. Lett. **108**, 130503 (2012).
11. G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in "Advances in Cryptology — EUROCRYPT '93," (Springer, New York, 1993), p. 410.
12. T. Ferreira da Silva, *et al.*, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," Phys. Rev. A **88**, 052303 (2013).
13. Z. Tang, *et al.*, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," Phys. Rev. Lett. **112**, 190503 (2014).
14. L. C. Comandar, *et al.*, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," Nature Photon. **10**, 312 (2016).