AUTHOR QUERY FORM

AIP Publishing	Journal: Appl. Phys. Lett. Article Number: APL19-AR-06644	**Please provide your responses and any corrections by annotating this PDF and uploading it to AIP's eProof website as detailed in the Welcome email.**

Dear Author,

Below are the queries associated with your article; please answer all of these queries before sending the proof back to AIP.

Article checklist: In order to ensure greater accuracy, please check the following and make all necessary corrections before returning your proof.

1. Is the title of your article accurate and spelled correctly?
2. Please check affiliations including spelling, completeness, and correct linking to authors.
3. Did you remember to include acknowledgment of funding, if required, and is it accurate?

Location in article	Query / Remark: click on the Q link to navigate to the appropriate spot in the proof. There, insert your comments as a PDF annotation.
AQ1	Please check that the author names are in the proper order and spelled correctly. Also, please ensure that each author's given and surnames have been correctly identified (given names are highlighted in red and surnames appear in blue).
AQ2	References 30 and 31 were not cited in text. We have inserted a citation in the sentence beginning "Alternatives such as advanced photonic…." Please check our placement and reposition if necessary.
AQ3	If preprint Ref. 15 has subsequently been published elsewhere, please provide updated reference information (journal title, volume number, and page number).
AQ4	Please supply more information for Ref. 2.
	Please confirm ORCIDs are accurate. If you wish to add an ORCID for any author that does not have one, you may do so now. For more information on ORCID, see https://orcid.org/. Jianwei Lee - 0000-0001-7861-6364 Lijiong Shen - 0000-0002-5854-5236 Alessandro Cerè - 0000-0002-4745-4451 James Troupe- Antia Lamas-Linares- Christian Kurtsiefer - 0000-0003-2190-0684
	Please check and confirm the Funder(s) and Grant Reference Number(s) provided with your submission: Applied Research Laboratories, UT Austin, Award/Contract Number Ministry of Education - Singapore, Award/Contract Number Please add any additional funding sources not stated above:

Thank you for your assistance.

Applied Physics Letters ARTICLE scitation.org/journal/apl

Asymmetric delay attack on an entanglement-based bidirectional clock synchronization protocol

Cite as: Appl. Phys. Lett. **115**, 000000 (2019); doi: 10.1063/1.5121489
Submitted: 26 July 2019 · Accepted: 18 September 2019 ·
Published Online: 0 Month 0000

View Online Export Citation CrossMark

AQ1 Jianwei Lee,[1] Lijiong Shen,[1,2] Alessandro Cerè,[1] James Troupe,[3] Antia Lamas-Linares,[1,4] and Christian Kurtsiefer[1,2,a)]

AFFILIATIONS

[1]Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore
[2]Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117551, Singapore
[3]Applied Research Laboratories, The University of Texas at Austin, 10000 Burnet Rd, Austin, Texas 78758, USA
[4]SpeQtral, 73 Science Park Drive, Singapore 118254, Singapore

[a)]Electronic mail: christian.kurtsiefer@gmail.com

ABSTRACT

We demonstrate an attack on a clock synchronization protocol that attempts to detect tampering of the synchronization channel using polarization-entangled photon pairs. The protocol relies on a symmetrical channel, where propagation delays do not depend on the propagation direction, for correctly deducing the offset between clocks—a condition that could be manipulated using optical circulators, which rely on static magnetic fields to break the reciprocity of propagating electromagnetic fields. Despite the polarization transformation induced within a set of circulators, our attack creates an error in time synchronization while evading detection.

Clock synchronization protocols that bidirectionally exchange signals, e.g., the Network Time Protocol (NTP) or the two-way satellite time transfer (TWSTFT), are widely used to estimate the absolute time offset between remote clocks without first characterizing network propagation times.[1–4] By assuming that propagation delays are symmetric in the two directions of travel in a synchronization channel, parties estimate one-way propagation times as half of the round trip time. Although convenient, this assumption exposes the protocol to attacks that introduce unknown asymmetric channel delays which cannot be detected by better encryption or authentication.[5] Existing countermeasures,[6–8] e.g., based on monitoring round trip times, have been evaded by sophisticated intercept, spoofing, and delay techniques.[9]

Recently, protocol implementations using entangled photons have suggested measuring nonlocal properties to ensure that synchronization networks have not been tampered with—a technique associated with entanglement-based quantum key distribution.[10–12] Tight time correlations between entangled photons prepared by spontaneous parametric downconversion (SPDC) allow synchronizing independent atomic clocks at photon rates of order 100 pairs/s[10] and with potential accuracies <1 ps.[11] Monogamy of entanglement ensures that a counterfeit photon entangled with the legitimate signal cannot be generated, allowing signal authentication.[13] The no-cloning theorem prevents intercept, copy, and resend of an identical quantum state with an arbitrary delay.[14]

Despite these security enhancements, the vulnerability to an asymmetric delay attack remains since photons traveling in opposite directions can be passively rerouted with a circulator (Fig. 1) by using the Faraday effect to break the reciprocity of the channel. A recent proposal suggests that even polarization-insensitive circulators, which rotate input polarizations back to the same state, impose a measurable change in the phase of the joint state.[15] The proposal was based on the fact that the phase change after a cyclic quantum evolution is measurable under certain conditions.[16] Previous experiments with entangled photons[17–20] seemed to support this proposed protection.

In this work, we examine the circulator-based asymmetric delay attack.[15] We experimentally show that the attack "cannot" be detected by the proposed mechanism and demonstrate an induced error in synchronization of over 25 ns between two rubidium clocks.

We briefly review the clock synchronization protocol considered.[15] The protocol involves two parties, Alice and Bob, connected by a single mode optical channel. Each party has a source of polarization-entangled photon pairs generated by SPDC. One photon of the pair is detected locally, while the other is sent and detected on the remote side (Fig. 1). Every photodetection event is time-tagged with respect to a local clock which assigns time stamps t and t'.

Photon pairs emerging from SPDC are tightly time-correlated. Thus, for an offset δ between the clocks, a propagation time Δt_{AB} from

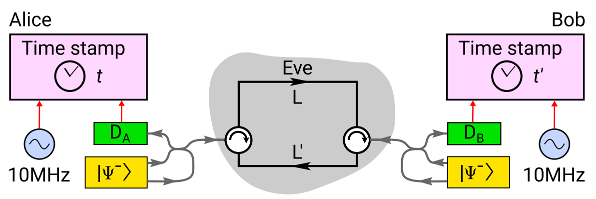

FIG. 1. Clock synchronization scheme. Alice and Bob each have a source of polarization-entangled photon pairs $|\Psi^-\rangle$ and avalanche photodetectors at $D_{A,B}$. One photon of the pair is detected locally, while the other photon is sent through a fiber to be detected on the remote side. Arrival times for all detected photons are recorded at each side with respect to local clocks, each locked to a rubidium frequency reference. Gray region: asymmetric delay attack. An adversary (Eve) uses a pair of circulators to introduce a direction-dependent propagation delay: photons originating at Bob's site will always take the bottom path, while photons originating at Alice's side will take the top path.

Alice to Bob, and Δt_{BA} in the other direction, the second-order correlation function $G^{(2)}(\tau = t' - t)$ of the time difference has two peaks at

$$\tau_{AB} = \delta + \Delta t_{AB} \quad \text{and} \quad \tau_{BA} = \delta - \Delta t_{BA} \tag{1}$$

due to pairs created by Alice and Bob.[21] A round trip time ΔT for photons can be calculated using the interpeak separation,

$$\Delta T = \Delta t_{AB} + \Delta t_{BA} = \tau_{AB} - \tau_{BA}, \tag{2}$$

while the offset,

$$\delta = \frac{1}{2}\left[(\tau_{AB} + \tau_{BA}) - (\Delta t_{AB} - \Delta t_{BA})\right], \tag{3}$$

is given by the midpoint of the peaks and a propagation delay asymmetry. Assuming a symmetrical propagation delay, $\Delta t_{AB} = \Delta t_{BA}$, the clock offset,

$$\delta = \frac{1}{2}(\tau_{AB} + \tau_{BA}), \tag{4}$$

is obtained directly from the midpoint.

Eve may now may exploit this assumption by separating the two propagation directions with a pair of circulators (Fig. 1, gray region), introducing a direction dependent delay $\Delta t_{AB} - \Delta t_{BA} = (L - L')/v$, where L is the additional propagation length from Alice to Bob and L' in the other direction and v is the speed of light in the fiber. If Alice and Bob continue to rely on the midpoint between the peaks to estimate δ, they will obtain instead $\delta + (L - L')/2v$.

In an attempt to detect the circulators, Ref. 15 suggests that Alice and Bob monitor polarization correlations using avalanche photodiodes (APDs) preceded by a polarization measurement in the appropriate bases ($D_{A,B}$). The detection scheme is based on the fact that circulators use Faraday Rotation (FR) to separate photons propagating in opposite directions—Faraday Rotation is a time-reversal symmetry breaking mechanism that rotates polarization, potentially changing the input state.

For each individual polarization state to be preserved, the circulators must rotate the state by an integer multiple of 180° so that for a Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$ distributed by Alice, the rotation of Bob's state $(|\psi\rangle_B \rightarrow \pm|\psi\rangle_B)$ does not result in any measurable change,

$$|\Psi^-\rangle \rightarrow \pm\frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \pm|\Psi^-\rangle. \tag{5}$$

However, as the evolution of Bob's state follows a closed trajectory on the Poincaré sphere, Ref. 15 predicted that a geometric phase—the phase determined by the geometry of the trajectory on the sphere[16]—is imposed on the Bell state and can be detected in a nonlocal measurement. We show in the supplementary material that when other phase contributions are taken into account, the net effect of the circulators nonetheless produces no measurable change to the Bell state [Eq. (5)]. In subsequent paragraphs, we use this result to experimentally demonstrate an asymmetric delay attack which evades detection.

We first implement the clock synchronization protocol. For two independent rubidium clocks, the following setup was previously characterized to achieve a synchronization precision of 51 ps in 100 s, comparable to the relative intrinsic frequency instability of each clock.[10]

Two identical SPDC sources generate polarization-entangled photon pairs (Fig. 1). The output of a laser diode (power $\approx$ 10 mW; central wavelength 405 nm) is coupled into a single mode optical fiber (SMF) for spatial mode filtering and focused to a beam waist of 80 μm into a 2 mm thick β-Barium Borate crystal cut for noncollinear type-II phase matching.[22] Down-converted photons at 810 nm are coupled into two single mode fibers with an overall detected pair rate of about 200 s^{-1}. Fiber beam splitters separate the photon pairs so that one photon is detected locally with an avalanche photodetector ($D_{A,B}$), while the other photon is transmitted to the remote party.

Time-stamping units assign detection times t and t' to the events detected at Alice and Bob, respectively. We compute the histogram $G^{(2)}(\tau = t' - t)$ of the time differences and resolve two coincidence peaks (FWHM $\approx$ 500 ps) with a resolution of 16 ps, one from each source.[23] The offset and round trip-times are determined from the mean and separation of the peaks, respectively. For the purposes of this demonstration, we lock the clocks with unknown offset to a common rubidium frequency reference, thus avoiding frequency drifts that can detract from the main point of the experiment, i.e., demonstrating an induced error in offset estimation.

To implement the asymmetric delay attack, we use two 3-port polarization-insensitive optical circulators of design-wavelength 810 nm and two single mode fibers of lengths L and L'.

We first estimate the initial offset δ_o between the two clocks with a symmetric channel delay $L = L' = L_o$. Figure 2(a) shows $g^{(2)}(\tau)$, the second-order correlation function $G^{(2)}(\tau)$ normalized to background coincidences, acquired from the time stamps recorded for about 5 min. In Fig. 3, we plot the offset and round trip times estimated every 40 s.

To illustrate the difference in the cross correlation measured between a symmetric and an asymmetric delay attack, we use two 5 m fibers to impose an additional round trip of 10 m but distribute them differently during each attack. For the symmetric delay attack, we extend L and L' equally by 5 m. We observe in Fig. 2(b) that although the peak separation increases, the midpoint of the peaks used for estimating the offset remains unchanged. For the asymmetric delay attack, both fibers are used to extend L by 10 m, while L' remains unchanged. We observe in Fig. 2(c) that the peak separation remains the same as in Fig. 2(b), but the midpoint of the peaks has shifted by 25.24(2) ns corresponding to half the additional round trip time incurred. This indicates a successful attack.

Applied Physics Letters ARTICLE scitation.org/journal/apl

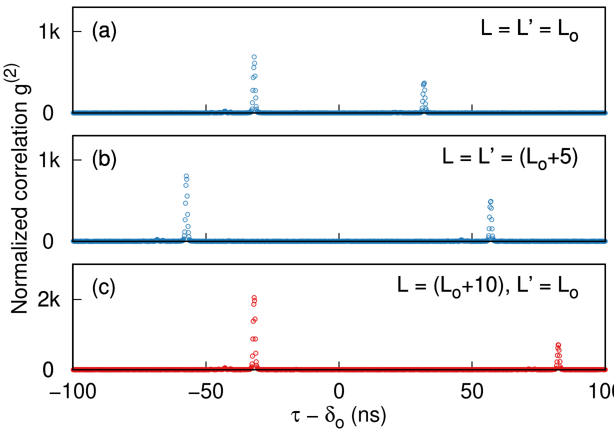

FIG. 2. Time correlations of Alice and Bob's detection events normalized to background coincidences. The separation between peaks corresponds to the round trip time ΔT, and the midpoint is the offset between the clocks δ. Symmetric delays with $L = L'$ show that the offset remains constant for both the (a) initial and (b) extended round trip times. An asymmetric delay with (c) $L = L' + 10$ results in an offset shift. $L_o/2$: minimum length of the fiber belonging to each circulator port. δ_o: the offset estimated in (a).

As a proof-of-principle demonstration of how the circulators influence the distributed entanglement, we measure polarization correlations of Alice's pair source before and after the circulators are inserted in one of its output modes with the setup shown in Fig. 4. For each output mode, a quarter-wave plate (QWP), half-wave plate (HWP), and polarizing beam splitter (PBS) project the polarization mode into horizontal, vertical, diagonal (+45°), antidiagonal (−45°), left-circular, or right-circular polarization ($|H\rangle, |V\rangle, |D\rangle, |A\rangle, |L\rangle$ or $|R\rangle$). Fiber polarization controllers (FPCs) correct for the polarization errors introduced by the fibers. We note that since FPCs do not break time-reversal symmetry, they cannot invert the polarization transformation induced by the circulators. We detect photon pairs with APDs for 36 wave plate settings and numerically search for the density matrix most likely to have returned the observed pair rates.[24]

Figure 5 shows the reconstructed density matrices of Alice's state before (ρ_o) and after (ρ) the introduction of the circulators into the path of Bob's photons. We compare ρ_o and ρ by computing the fidelity $F(\rho, \rho_o) = (\mathrm{Tr}\sqrt{\sqrt{\rho}\rho_o\sqrt{\rho}})^2$. The uncertainty in F due to errors in counting statistics was obtained by Monte Carlo simulation, where 36 new measurement results are numerically generated, each drawn randomly from a Poissonian distribution with a mean equal to the original number of counts.[24] From these numerically generated results, a new density matrix can be calculated and consequently a new value

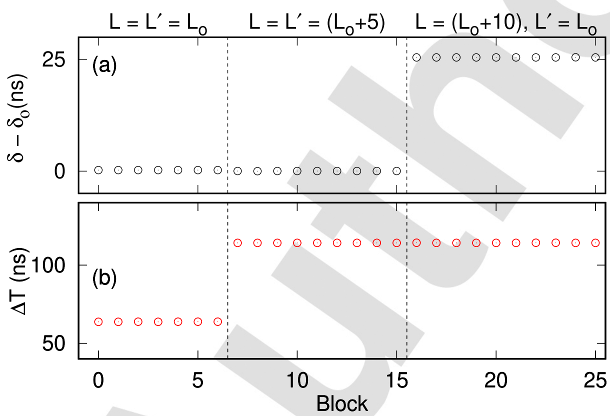

FIG. 3. (a) Measured offset δ between two clocks, both locked on the same frequency reference. Each value of δ was evaluated from measuring photon pair timing correlations from a block of photodetection times recorded by Alice and Bob. Each block is 40 s long. (b) The round trip time ΔT. Blocks 6–7: increasing the symmetric delay ($L = L'$) does not change δ. Blocks 15 to 16: introducing an asymmetric delay ($L \neq L'$) creates an offset error. The delay was created by redistributing the additional delays in blocks 7–15, so that ΔT remains the same. δ_o: offset measured in the first block.

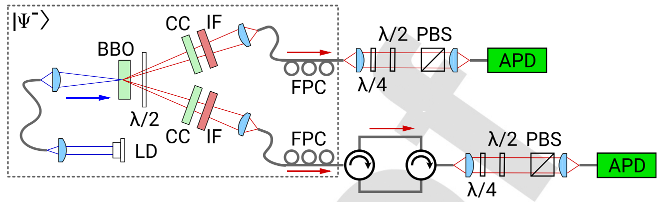

FIG. 4. Setup for quantum state tomography on a polarization-entangled photon pair state, with one photon passing through a pair of circulators. Dashed box: optical setup of our polarization-entangled photon source. LD: laser diode, BBO: β-Barium Borate, CC: compensation crystals, FPC: fiber polarization controller, SMF: single mode fiber, $\lambda/4$: quarter-wave plate, $\lambda/2$: half-wave plate, PBS: polarizing beam splitter, and APD: avalanche photodiode.

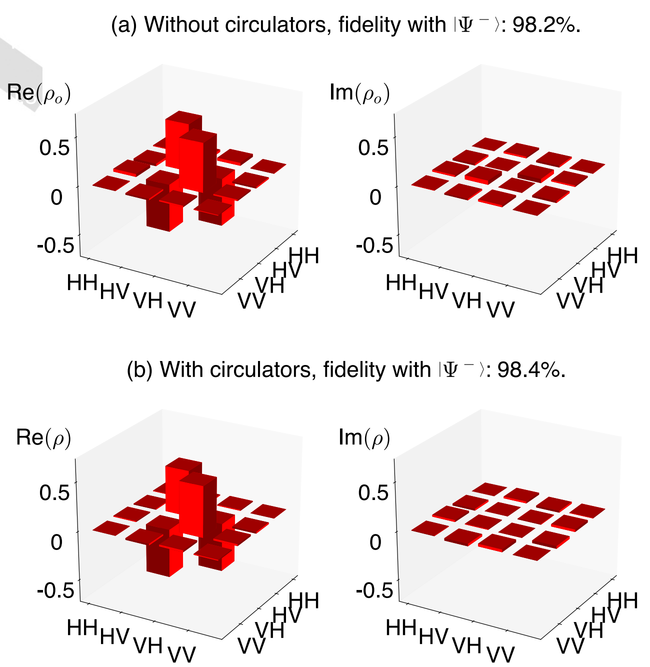

FIG. 5. Real and imaginary part of the reconstructed density matrix for the target Bell state $|\Psi^-\rangle$ originating from Alice's source. Bob receives one photon of the pair through the synchronization channel. The density matrices obtained (a) without and (b) with polarization-insensitive circulators in the line (Fig. 4) do not deviate significantly from $|\Psi^-\rangle$.

Applied Physics Letters ARTICLE scitation.org/journal/apl

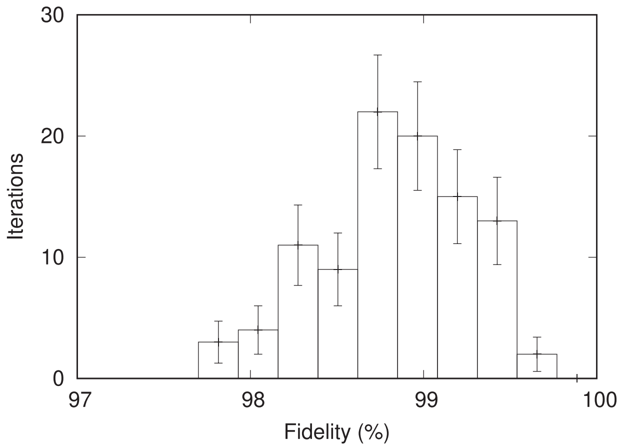

FIG. 6. Fidelity distribution comparing the Bell state originating from Alice's source before and after introducing the circulators. The distribution is generated by numerically propagating errors due to counting statistics. A high mean fidelity suggests that the state remains unchanged and cannot be used to detect the attack. Error bars: Poissonian standard deviation.

of F. Repeating this process 100 times, we obtain the fidelity distribution shown in Fig. 6 from which we compute a 95% confidence interval $98.7\% < F < 98.9\%$. The distribution of F does not include 100%, which we attribute to imperfect control of the polarization state in the optical fiber. From the near-unity value of F, we conclude that the circulators do not affect the distributed Bell state.

We have demonstrated an attack of a clock synchronization protocol that tries to achieve security by detecting changes in polarization-entanglement distributed across a synchronization channel. The attack was implemented by rerouting photons with polarization-insensitive circulators and imposing a direction-dependent propagation delay. The observed shift in the estimated clock offset is equal to half the propagation delay asymmetry, as expected for a protocol which assumes a symmetric channel.[5] Although circulators reroute photons using a polarization-rotation mechanism, we experimentally verify that they produce no measurable change in the distributed entangled state, indicating that they cannot be detected using the protocol.

In this work, we focused on detecting its underlying mechanism—Faraday Rotation (FR)—which must be performed in any circulator. Methods based on characterizing light intensities, e.g., identifying additional reflections, may still allow the detection of circulators, but they rely on the specific characteristics of the device (e.g., reflectivity). We also note that when Alice and Bob exchange photons that are identical in every other degree-of-freedom apart from the propagation direction, there are few technologies besides a FR-based circulator capable of discreetly separating their photons. Alternatives such as advanced photonic structures[25–29] and quantum nondemolition measurements[12] still pose a significant technological barrier for any adversary, and so entanglement-based clock synchronization still may provide a significant security advantage compared to traditional
AQ2 methods.[30,31]

Our result corrects the prediction in Ref. 15 and clarifies the effectiveness of directly replacing classical signals with entangled photons to protect the synchronization channel—we demonstrate that propagation delays can be introduced without affecting the entanglement degree-of-freedom, rendering the proposed protection ineffective against asymmetric delay attacks.

See the supplementary material for the examination of the geometric phase associated with polarization state rotation in the circulators, previously thought to be observable,[15] and an additional phase, associated with photon dynamics in the Faraday Rotator, which neutralizes this geometric phase.

We acknowledge support of the National Research Foundation & Ministry of Education in Singapore. J.T. acknowledges support from the ARL:UT Independent Research and Development Program.

REFERENCES

1D. L. Mills, IEEE Trans. Commun. **39**, 1482 (1991).
2IEC 61588:2009(E), C1 (2009). AQ4
3D. Piester, A. Bauch, L. Breakiron, D. Matsakis, B. Blanzano, and O. Koudelka, Metrologia **45**, 185 (2008).
4Z. Jiang, Y. Huan, V. Zhang, and P. Dirk, "BIPM 2017 TWSTFT SATRE/SDR calibrations for UTC and non-UTC links," Technical Report, BIPM Technical Memorandum, TM268 V2a, 2017.
5L. Narula and T. E. Humphreys, IEEE J. Sel. Top. Signal Process. **12**, 749 (2018).
6T. Mizrahi, in *2012 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication Proceedings* (IEEE, 2012), pp. 1–6.
7M. Ullmann and M. Vögeler, in *2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication* (IEEE, 2009), pp. 1–6.
8J. Tsang and K. Beznosov, in *International Conference on Information and Communications Security* (Springer, 2006), pp. 50–59.
9D. Rabadi, R. Tan, D. K. Yau, and S. Viswanathan, in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (ACM, 2017), pp. 874–886.
10J. Lee, L. Shen, A. Cerè, J. Troupe, A. Lamas-Linares, and C. Kurtsiefer, Appl. Phys. Lett. **114**, 101102 (2019).
11F. Hou, R. Quan, R. Dong, X. Xiang, B. Li, T. Liu, X. Yang, H. Li, L. You, Z. Wang, and S. Zhang, Phys. Rev. A **100**, 023849 (2019).
12A. Lamas-Linares and J. Troupe, in *Advances in Photonics of Quantum Computing, Memory, and Communication XI* (International Society for Optics and Photonics, 2018), Vol. 10547, p. 105470L.
13D. Yang, Phys. Lett. A **360**, 249 (2006).
14W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
15J. E. Troupe and A. Lamas-Linares, preprint arXiv:1808.09019 (2018). AQ3
16M. V. Berry, J. Mod. Opt. **34**, 1401 (1987).
17P. G. Kwiat and R. Y. Chiao, Phys. Rev. Lett. **66**, 588 (1991).
18D. V. Strekalov and Y. H. Shih, Phys. Rev. A **56**, 3129 (1997).
19J. Brendel, W. Dultz, and W. Martinessen, Phys. Rev. A **52**, 2551 (1995).
20A. K. Jha, M. Malik, and R. W. Boyd, Phys. Rev. Lett. **101**, 180405 (2008).
21R. J. Glauber, Phys. Rev. **130**, 2529 (1963).
22P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
23C. Ho, A. Lamas-Linares, and C. Kurtsiefer, New J. Phys. **11**, 045011 (2009).
24J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, Adv. At., Mol., Opt. Phys. **52**, 105 (2005).
25D. Jalas, A. Y. Petrov, and M. Eich, Opt. Lett. **39**, 1425 (2014).
26V. Dmitriev, G. Portela, and D. Zimmer, Opt. Lett. **38**, 4040 (2013).
27V. Dmitriev, M. N. Kawakatsu, and G. Portela, Opt. Lett. **38**, 1016 (2013).
28L. Bi, J. Hu, P. Jiang, D. H. Kim, G. F. Dionne, L. C. Kimerling, and C. Ross, Nat. Photonics **5**, 758 (2011).
29Z. Yu and S. Fan, Nat. Photonics **3**, 91 (2009).
30J. Anandan, Nature **360**, 307 (1992).
31J. Zak, Phys. Lett. A **154**, 471 (1991).