Setting a disordered password on a photonic memory

Su, Shih-Wei; Gou, Shih-Chuan; Chew, Lock Yue; Chang, Yu-Yen; Yu, Ite A.; Kalachev, Alexey; Liao, Wen-Te

2017

Su, S.-W., Gou, S.-C., Chew, L. Y., Chang, Y.-Y., Yu, I. A., Kalachev, A., et al. (2017). Setting a disordered password on a photonic memory. *Physical Review A*, 95(6), 061805-.

<https://hdl.handle.net/10356/83032>

<https://doi.org/10.1103/PhysRevA.95.061805>

© 2017 American Physical Society (APS). This paper was published in *Physical Review A* and is made available as an electronic reprint (preprint) with permission of American Physical Society (APS). The published version is available at: [<http://dx.doi.org/10.1103/PhysRevA.95.061805>]. One print or electronic copy may be made for personal use only. Systematic or multiple reproduction, distribution to multiple locations via electronic or other means, duplication of any material in this paper for a fee or for commercial purposes, or modification of the content of the paper is prohibited and is subject to penalties under law.

Downloaded on 26 Apr 2023 20:49:55 SGT

Setting a disordered password on a photonic memory

Shih-Wei Su,¹ Shih-Chuan Gou,¹ Lock Yue Chew,² Yu-Yen Chang,^{3,4} Ite A. Yu,⁵ Alexey Kalachev,⁶ and Wen-Te Liao^{7,*}

¹*Department of Physics and Graduate Institute of Photonics, National Changhua University of Education, Changhua 50058, Taiwan*

²*Division of Physics and Applied Physics, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Singapore*

³*CEA Saclay, Service d'Astrophysique, 91191 Gif-sur-Yvette Cedex, France*

⁴*Academia Sinica Institute of Astronomy and Astrophysics, Taipei 10617, Taiwan*

⁵*Department of Physics and Frontier Research Center on Fundamental and Applied Sciences of Matters, National Tsing Hua University, Hsinchu 30013, Taiwan*

⁶*Zavoisky Physical-Technical Institute of the Russian Academy of Sciences, Sibirsky Trakt 10/7, Kazan 420029, Russia*

⁷*Department of Physics, National Central University, Taoyuan City 32001, Taiwan*

(Received 31 October 2016; published 30 June 2017)

An all-optical method of setting a disordered password on different schemes of photonic memory is theoretically studied. While photons are regarded as ideal information carriers, it is imperative to implement such data protection on all-optical storage. However, we wish to address the intrinsic risk of data breaches in existing schemes of photonic memory. We theoretically demonstrate a protocol using spatially disordered laser fields to encrypt data stored on an optical memory, namely, encrypted photonic memory. To address the broadband storage, we also investigate a scheme of disordered echo memory with a high fidelity approaching unity. The proposed method increases the difficulty for the eavesdropper to retrieve the stored photon without the preset password even when the randomized and stored photon state is nearly perfectly cloned. Our results pave ways to significantly reduce the exposure of memories, required for long-distance communication, to eavesdropping and therefore restrict the optimal attack on communication protocols. The present scheme also increases the sensitivity of detecting any eavesdropper and so raises the security level of photonic information technology.

DOI: [10.1103/PhysRevA.95.061805](https://doi.org/10.1103/PhysRevA.95.061805)

The value of encrypted data processing and storage has been proven by its benefits of protection against data breaches and theft through the physical removal of computer memory [1,2]. An encrypted memory is composed of two components, namely, data storage and encryption. Over past decades the photon has been regarded as an ideal information carrier, and several schemes of optical quantum memory [3,4] have been well established, e.g., electromagnetically induced transparency (EIT) [5–12], gradient echo memory (GEM) [13–17], and atomic frequency comb (AFC) [18,19]. It is worth mention that photonic memories made of cold atomic media with very high optical depth >1000 and very low ground-state decoherence rate around 10^{-4} times spontaneous decay rate have been experimentally achieved [12,20]. The missing piece of the optical encryptor may open a vastly unexplored realm of encrypted photonic memory at a security level higher than existing optical storage systems. In this Rapid Communication, we theoretically demonstrate not only the capability but also the flexibility of using disordered fields [21–23] to set passwords on various schemes of photonic memory. Incorporating spread spectrum methods [24] with our scheme, long-distance quantum communication with a high degree of multiplexing and noise immunity can be implemented via trusted and secure local gadgets. This will restrict the optimal attack on communication protocols via nearly perfect cloning of photon states stored in photonic memories [25,26]. Our scheme may also encrypt higher dimensional information, e.g., two-dimensional images [27–31].

As illustrated in Fig. 1, an echo memory [32] is typically made of an atomic ensemble (gray spheres) whose absorption of a probe pulse (blue wavy lines) is modified by another external control field. The following phase of atomic coherence evolves in a nonuniform way due to the position-dependent control field strength. When the control field is inverted at some instant, the time reversal of the atomic phase leads to an echo output. In Fig. 1(a), we put forward the idea of disordered echo memory (DEM) using a disordered field (colored surface below gray spheres) whose strength statistics follows the normal distribution depicted in Fig. 1(c). The disordered field is not propagating in the medium but is a random speckled field transversely shined from the side [23]. Green arrows aligned aside the system represent the spatial randomness of DEM atomic dynamics. As a comparison Fig. 1(d) shows a linearly GEM having ordered atomic dynamics and equal probability for each field strength [Fig. 1(e)]. We find that DEM leads to very high fidelity of broadband retrieval [33,34] when the strength statistics of the disordered field [Fig. 1(b)] matches the Fourier spectrum of the incident probe [Fig. 1(c)]. In addition, other methods of disorder-induced symmetric encryption on optical memories will be presented.

Figure 2(a) illustrates the DEM based on the three-level Λ -type scheme depicted in Fig. 2(b). The medium of length L includes two ground states $|1\rangle$, $|2\rangle$ and an excited state $|3\rangle$ whose lifetime is τ and spontaneous decay rate $\Gamma = 1/\tau$. The system under study is described by the optical-Bloch equation [10,14,16,35] (see Supplemental Material [36])

$$\partial_t \hat{\rho} = \frac{1}{i\hbar} [\hat{H}, \hat{\rho}] + \mathcal{L}\rho,$$

$$\left(\frac{1}{c} \partial_t + \partial_z \right) \Omega_p = i\eta \rho_{31},$$

*wente.liao@g.ncu.edu.tw

FIG. 1. (a) Disordered echo memory is composed of an atomic ensemble interacting with a spatially disordered field (colored surface) and a probe pulse (blue line) to be stored. The green randomly oriented arrows demonstrate the quantum phase evolution of memory atoms at various sections of the disorder. (b) The probability distribution of the Rabi frequency of a disordered field should cover (c), (f) the Fourier spectrum of the incident probe field. (d) Gradient echo memory is made of an atomic ensemble interacting with a linearly gradient field which introduces a spatially ordered phase modulation. (e) The equal probability distribution of the linearly gradient field strength is distinct from that in panel (f).

where $\hat{\rho}$ is the density matrix for the state vector $\sum_{i=1}^3 B_i |i\rangle$ of the three-level atom, and each coherence $\rho_{ij} = B_i B_j^*$; $\mathcal{L}\rho$ describes the spontaneous decay of the excited state $|3\rangle$ characterized by rate Γ . $\hat{H} = \frac{\hbar}{2}[\Omega_p|3\rangle\langle 1| + \Omega_d|3\rangle\langle 2| + \text{H.c.}]$ is the Hamiltonian describing the atom-light interaction with Rabi frequency Ω_p of the probe field and Ω_d of the disordered field; $\eta = \Gamma\xi/2L$ with ξ , and L the optical depth and the length of the medium, respectively. The low decoherence between ground states $|2\rangle$ and $|1\rangle$ is neglected in the Lindblad form $\mathcal{L}\rho$ for the time scale of interest [12,20]. The boundary condition gives the Rabi frequency of the incident probe field $\Omega_p e^{-[(t-t_p)/\kappa]^2}$, and the initial condition describes the initial population $\rho_{11}(0,z) = 1$, $\rho_{ii}(0,z) = 0$ for $i > 1$ and zero coherences $\rho_{ij}(0,z) = 0$ for $i \neq j$. Two dipole transitions $|1\rangle \leftrightarrow |3\rangle$ and $|2\rangle \leftrightarrow |3\rangle$ are resonantly coupled to a probe field and a disordered field, respectively. The incident broadband probe field peaks at t_p with a duration of κ ($1/\kappa \gg \Gamma$), and the disordered field satisfies the spatial correlation function $\langle \Omega_d(t,z)\Omega_d(t',z') \rangle = \mathbf{D}_c^2 e^{-(z-z')^2/\sigma^2}$. The generation of disorder is given by Ref. [37]. Here we consider $\kappa = 5 \times 10^{-3}\tau$ and the correlation length $\sigma = L/100$. The present broadband DEM relies on the spatially inhomogeneous Autler-Townes splitting (ATS) [15–17,22,38] induced by $\Omega_d(t,z)$ such that each Fourier component of probe field is absorbed by the modified medium at corresponding resonant positions [15]. The probe

field is then stored as atomic coherence $\rho_{21}(t,z) \propto \sin \theta(t,z)$ and $\rho_{31}(t,z) \propto \cos \theta(t,z)$ where the local phase is [16]

$$\theta(t,z) = \frac{1}{2} \int_0^t \Omega_d(t',z) dt'. \quad (1)$$

By inverting $\Omega_d(t,z)$ at some instant t_i , i.e., $\Omega_d(t \geq t_i, z) = -\Omega_d(t < t_i, z)$, an echo signal will be retrieved due to the global phase revival of $\theta(t,z)$. For a broadband storage we use $\mathbf{D}_c > 1/\kappa \gg \Gamma$ which spreads the absorption line width enough to cover the whole spectrum of the probe pulse. The success of the encryption is based on the cooperation between the disorder field and time reversal of phase $\theta(t,z)$. As illustrated in Fig. 2(a), we use a disordered field depicted in Fig. 2(e) with $\mathbf{D}_c = 1000\Gamma$, $t_i = 0.22\tau$, and optical depth $\xi = 1200$ to simultaneously store and encrypt the broadband probe (green dashed line). The red solid line shows the only successful retrieved echo by using the key1 profile demonstrated in Fig. 2(f) where $\Omega_d(t \geq t_i, z) = -\Omega_d(t < t_i, z)$, namely, the inversion of the encryption key in Fig. 2(e). To test the security of the present encryption scheme, $\Omega_d(t \geq t_i, z)$ is replaced by a distinct disorder as key2 depicted in Fig. 2(g) and a linearly gradient field as key3 in Fig. 2(h) for decryption tests. The blue long-dashed line and gray dotted line show that two attempts on memory both fail. Another 100 different

FIG. 2. Panel (a) illustrates broadband disordered echo memory based on (b) a three-level Λ -type scheme, and panel (c) depicts narrowband EIT memory based on (d) a four-level N -type system. Incident probe pulses (green dashed lines) driving transition $|1\rangle \leftrightarrow |3\rangle$ are encrypted by the disorder in panel (e), and decrypted by different keys in panels (f)–(h). The red solid lines depict the only successful retrieval with the correct key in panel (f). The blue long-dashed lines and gray dotted lines are the attempted retrievals by two wrong keys depicted respectively in panels (g) and (h). In panel (a) the access and encryption of a broadband probe are accomplished by the disorder, inverted at $t = 0.22\tau$ for decryption, driving transition $|2\rangle \leftrightarrow |3\rangle$. In panel (c) the brown dashed dotted line illustrates the temporal sequence of control field for EIT storage. Two disordered pulses (orange dashed dotted dotted line), driving transition $|2\rangle \leftrightarrow |4\rangle$, are far detuned respectively with Δ_d and $-\Delta_d$ for, in turn, encryption and decryption.

disorders are also utilized to decrypt the echo, but none is successful (see Ref. [36]).

The advantage of Λ -type DEM is depicted in Fig. 3, i.e., a high fidelity

$$\mathcal{F} = \frac{|\int_{t_i}^{\infty} \Omega_p^*(t - t_d, 0) \Omega_p(t, L) dt|^2}{[\int_{t_i}^{\infty} |\Omega_p(t, 0)|^2 dt][\int_{t_i}^{\infty} |\Omega_p(t, L)|^2 dt]}$$

FIG. 3. The mean fidelity of the disordered echo memory with correlation length $\sigma = L/100$ of Ω_c at various optical depths ξ and control field strengths $\mathbf{D}_c$. The results are obtained by averaging more than 1000 realizations of different disorder.

approaching unity for a wide range of $\mathbf{D}_c$ and ξ . Also, we numerically observe that in the domain of interest the present broadband scheme may share the same upper limit of storage efficiency $SE = [\int_{t_i}^{\infty} |\Omega_p(t, L)|^2 dt] / [\int_{t_i}^{\infty} |\Omega_p(t, 0)|^2 dt]$ of around 54% with other echo memory schemes because of reabsorption [14,19]. This limit can be overcome by the cavity-assisted interaction [39,40]. The underlying reason for the very high fidelity is that the solution of an echo signal (see Ref. [36]) can be replaced by the inverse Fourier transformation $\int_{-\infty}^{\infty} P(\Omega_d) \cos[\frac{\Omega_d(t-t_i)}{2}] d\Omega_d$. The statistics $P(\Omega_d)$ behind the disordered field strength preserves the shape of the incident probe field when $P(\Omega_d) \approx \int_{-\infty}^{\infty} \Omega_p(t, 0) \cos[\frac{\Omega_d t}{2}] dt$. Our numerical result in Fig. 3 confirms this optimization of fidelity when $\mathbf{D}_c \geq 1/\kappa$, i.e., the width of the absorption spectrum of the memory greater than or equal to that of the Fourier transformation of the incident pulse.

To demonstrate the encryption on a narrow-band ($1/\kappa < \Gamma$) EIT-based memory, we invoke the time sequence and the four-level N -type system [41] respectively illustrated in Figs. 2(c) and 2(d). In Fig. 2(c), the green dashed line shows the incident probe pulse with $\kappa = 10\tau$ driving the transition $|1\rangle \leftrightarrow |3\rangle$. The brown dashed dotted line illustrates the temporal sequence of the spatially uniform control field with Rabi frequency $\Omega_c = 5\Gamma$, which drives transition $|2\rangle \leftrightarrow |3\rangle$. The EIT light storage is accomplished by turning off the control field at $t_{\text{off}} = 50\tau$, and the probe pulse is stored as long-lived ground state coherence $\rho_{21}(t, z)$. The control field is subsequently turned on at $t_{\text{on}} = 195\tau$ for light retrieval [8–10,12,42,43]. As

demonstrated in Fig. 2(d), during the storage period $t_{\text{off}} < t < t_{\text{on}}$, a third disordered field with Rabi frequency $\Omega_d(t, z)$ and far detuning $\Delta_d = 500\Gamma$ shines on the memory to drive transition $|2\rangle \leftrightarrow |4\rangle$. The local phase of $\Omega_d(t, z)$ -encrypted $\rho_{21}(t, z)$ is given by (see Ref. [36])

$$\phi(t, z) \approx \frac{1}{4\Delta_d} \int_{t_{\text{off}}}^{t > t_{\text{off}}} |\Omega_d(t', z)|^2 dt'. \quad (2)$$

The randomized phase can be recovered by subsequently shining a decryption pulse with a detuning $-\Delta_d$ and an identical disorder. In Fig. 2(c) with $\xi = 1200$, the orange dashed-dotted line shows that two spatially disordered pulses $\Omega_d(t, z)$ encrypt and decrypt the memory with keys respectively in Figs. 2(e) and 2(f). Two disorders lead to $\phi(t \geq 185\tau, z) = 0$ and obey $\langle \Omega_d(t, z)\Omega_d(t, z') \rangle = \mathbf{D}_s^2 e^{-(z-z')^2/\sigma^2}$ where $\mathbf{D}_s = 30\Gamma$ and $\sigma = L/100$. To check whether other keys can recover the encrypted memory, we use key2 and key3 for decryption. As demonstrated in Fig. 2(c), the blue long-dashed line and gray dotted line reveal that no signal is retrieved by using keys other than key1 when Ω_c is turned on. The retrieval is also futile when either the encryption pulse ($60\tau < t < 120\tau$) or decryption pulse ($125\tau < t < 185\tau$) is applied. Moreover, the decrypted signal peaking at 225τ in Fig. 2(c) perfectly matches the pure EIT retrieval without any phase modulation, namely, the disordered encryption procedure preserves the performance of an EIT-based memory.

To verify the degree of the confidentiality and quantitatively demonstrate security of our scheme, we consider the case that the stored optical memory is retrieved by not only inverting the encryption key but also with a spatial shift δ as depicted in Figs. 4(a) and 4(b). At $\delta = 0$, the mean storage efficiency averaged over 100 realizations is maximized as expected, as increasing δ the storage efficiency gradually decreases as shown in Fig. 4(c) and 4(d) for Λ -type and N -type schemes, respectively. Those faint retrievals in Fig. 4(c) with normalized SE of about 2%–5% at large δ for $\sigma = L/50$ and $\sigma = L/30$ are too noisy to determine their fidelity. The very narrow σ -dependent window of retrieval ($< 10^{-3}L$ for both schemes at $\sigma = L/100$) suggests a securer encryption scheme that one can prepare a much longer disorder with length α than the memory size L , but only a tiny and privately known section is applied. In order to access the stored photon, the precise knowledge of the used section is needed, which ensures the confidentiality. The degree of the confidentiality of the scheme can be quantitatively defined as $\chi = \frac{\alpha^2}{\sigma^2 L}$, which reflects the increase of confidentiality by using the condition $\alpha \gg L \gg \sigma$. A study of the error bars of the averaged fidelity suggests that a small σ guarantees identical retrievals for different disorders (see Ref. [36]).

The present scheme is robust against brute-force attack if the key length of the pseudorandom number generator (PRNG) is large enough. More tenable attacks would come in the form of cryptanalysis, where the adversary exploits the system vulnerabilities either directly, through the inputs, or the internal states of the PRNG. Approaches to enhance the cryptographic strength of the PRNG against such attacks employ cryptographic primitives like the hash function and by gathering randomness from external sources to maximize its entropy [44]. Cryptographically secure PRNG

FIG. 4. (a) Disordered encryption key with length α interacting with a memory of size L . (b) The decryption key is made of the inversion of an encryption key spatially shifted by δ . The mean δ -dependent normalized storage efficiency over 100 realizations for (c) disordered echo memory and (d) EIT-based memory with $|\Delta_d| = 500\Gamma$, $\mathbf{D}_e = 1500\Gamma$ and $\xi = 1500$ are used in both panels (c) and (d). Three lines correspond to different correlation lengths of disorder $\sigma = L/100$ (red solid), $\sigma = L/50$ (green dashed), and $\sigma = L/30$ (blue dashed dotted).

passes a suite of statistical tests [45], with good examples being the Advanced Encryption Standard [2] and the PRNGs published by National Institute of Standards and Technology [1].

In conclusion, we have demonstrated using disordered fields to encrypt photonic memories with both high fidelity and high confidentiality. The present method would therefore increase the sensitivity of the detection of any eavesdropper [25] because any interception made on encrypted memories becomes nearly impossible, and an unsuccessful retrieval attempt of the signal with the wrong speckled field also precludes the subsequent retrieval by the correct decrypting field. Our scheme significantly lowers the intrinsic risk of data loss in existing memory schemes and makes an impact on photonic information technology.

W.-T.L. thanks Y.-C. Chen and H.-K. Lau for fruitful discussions. S.-W.S. and S.-C.G. are supported by the Ministry of Science and Technology, Taiwan (Grant No. MOST 103-2112-M-018-002-MY3). A.K. acknowledges support from the Russian Science Foundation (Grant No. 14-12-00806). W.-T.L. is supported by the Ministry of Science and Technology, Taiwan (Grant No. MOST 105-2112-M-008-001-MY3). S.-C.G. and W.-T.L. are also supported by the National Center for Theoretical Sciences, Taiwan.

- [1] E. Barker and J. Kelsey, NIST Spec. Publ. 800-90A Revision 1, <http://csrc.nist.gov/publications/nistpubs/> (2015).
- [2] P. Hellekalek and S. Wegenkittl, *ACM Trans. Mod. Comput. Simul.* **13**, 322 (2003).
- [3] A. I. Lvovsky, B. C. Sanders, and W. Tittel, *Nature Photon.* **3**, 706 (2009).
- [4] G. Brennen, E. Giacobino, and C. Simon, *New J. Phys.* **17**, 050201 (2015).
- [5] O. Kocharovskaya and Y. I. Khanin, *Sov. Phys. JETP* **63**, 945 (1986).
- [6] K.-J. Boller, A. Imamoglu, and S. E. Harris, *Phys. Rev. Lett.* **66**, 2593 (1991).
- [7] L. V. Hau, S. E. Harris, Z. Dutton, and C. H. Behroozi, *Nature (London)* **397**, 594 (1999).
- [8] O. Kocharovskaya, Y. Rostovtsev, and M. O. Scully, *Phys. Rev. Lett.* **86**, 628 (2001).
- [9] D. F. Phillips, A. Fleischhauer, A. Mair, R. L. Walsworth, and M. D. Lukin, *Phys. Rev. Lett.* **86**, 783 (2001).
- [10] Y.-H. Chen, M.-J. Lee, I.-C. Wang, S. Du, Y.-F. Chen, Y.-C. Chen, and I. A. Yu, *Phys. Rev. Lett.* **110**, 083601 (2013).
- [11] Y.-W. Cho and Y.-H. Kim, *Phys. Rev. A* **82**, 033830 (2010).
- [12] Y.-F. Hsiao, P.-J. Tsai, H.-S. Chen, S.-X. Lin, C.-C. Hung, C.-H. Lee, Y.-H. Chen, Y.-F. Chen, I. A. Yu, and Y.-C. Chen, [arXiv:1605.08519](https://arxiv.org/abs/1605.08519) (2016).
- [13] G. Hétet, J. J. Longdell, M. J. Sellars, P. K. Lam, and B. C. Buchler, *Phys. Rev. Lett.* **101**, 203601 (2008).
- [14] M. Hosseini, B. M. Sparkes, G. Hétet, J. J. Longdell, P. K. Lam, and B. C. Buchler, *Nature (London)* **461**, 241 (2009).
- [15] B. M. Sparkes, M. Hosseini, G. Hétet, P. K. Lam, and B. C. Buchler, *Phys. Rev. A* **82**, 043847 (2010).
- [16] W.-T. Liao, C. H. Keitel, and A. Pálffy, *Phys. Rev. Lett.* **113**, 123602 (2014).
- [17] T. Chanelière and G. Hétet, *Opt. Lett.* **40**, 1294 (2015).
- [18] H. De Riedmatten, M. Afzelius, M. U. Staudt, C. Simon, and N. Gisin, *Nature (London)* **456**, 773 (2008).
- [19] M. Afzelius, C. Simon, H. de Riedmatten, and N. Gisin, *Phys. Rev. A* **79**, 052329 (2009).
- [20] Y.-F. Hsiao, H.-S. Chen, P.-J. Tsai, and Y.-C. Chen, *Phys. Rev. A* **90**, 055401 (2014).
- [21] A. A. Kalachev, L. A. Nefed'ev, V. A. Zuikov, and V. V. Samartsev, *Opt. Spectrosc.* **84**, 731 (1998) [original Russian text published in *Optika i Spektroskopiya* **84**, 811 (1998)].
- [22] L. Nefed'ev and G. G. Khakimzyanova, *Opt. Spectrosc.* **105**, 924 (2008).
- [23] J. Billy, V. Josse, Z. Zuo, A. Bernard, B. Hambrecht, P. Lugan, D. Clément, L. Sanchez-Palencia, P. Bouyer, and A. Aspect, *Nature (London)* **453**, 891 (2008).
- [24] C. Belthangady, C.-S. Chuu, I. A. Yu, G. Y. Yin, J. M. Kahn, and S. E. Harris, *Phys. Rev. Lett.* **104**, 223601 (2010).
- [25] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, *Rev. Mod. Phys.* **77**, 1225 (2005).
- [26] J. Y. Haw, J. Zhao, J. Dias, S. M. Assad, M. Bradshaw, R. Blandino, T. Symul, T. C. Ralph, and P. K. Lam, *Nature Commun.* **7**, 13222 (2016).
- [27] M. Shuker, O. Firstenberg, R. Pugatch, A. Ron, and N. Davidson, *Phys. Rev. Lett.* **100**, 223601 (2008).
- [28] Y.-W. Cho, J.-E. Oh, and Y.-H. Kim, *Opt. Express* **20**, 5809 (2012).
- [29] G. Heinze, C. Hubrich, and T. Halfmann, *Phys. Rev. Lett.* **111**, 033601 (2013).
- [30] D.-S. Ding, Z.-Y. Zhou, B.-S. Shi, and G.-C. Guo, *Nature Commun.* **4**, 2527 (2013).
- [31] J.-C. Lee, K.-K. Park, Y.-W. Cho, and Y.-H. Kim, *Phys. Rev. A* **88**, 043824 (2013).
- [32] S. A. Moiseev and S. Kröll, *Phys. Rev. Lett.* **87**, 173601 (2001).
- [33] K. Reim, J. Nunn, V. Lorenz, B. Sussman, K. Lee, N. Langford, D. Jaksch, and I. Walmsley, *Nature Photon.* **4**, 218 (2010).
- [34] H. de Riedmatten, *Nature Photon.* **4**, 206 (2010).
- [35] M. O. Scully and M. S. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, 2006).
- [36] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevA.95.061805> for complete equations.
- [37] M. S. Simon, J. Sancho, and A. Lacasta, *Fluctuation Noise Lett.* **11**, 1250026 (2012).
- [38] W.-T. Liao, S. Das, C. H. Keitel, and A. Pálffy, *Phys. Rev. Lett.* **109**, 262502 (2012).
- [39] M. Sabooni, Q. Li, S. Kröll, and L. Rippe, *Phys. Rev. Lett.* **110**, 133604 (2013).
- [40] P. Jobez, I. Usmani, N. Timoney, C. Laplane, N. Gisin, and M. Afzelius, *New J. Phys.* **16**, 083005 (2014).
- [41] Y.-F. Chen, C.-Y. Wang, S.-H. Wang, and I. A. Yu, *Phys. Rev. Lett.* **96**, 043603 (2006).
- [42] M. Fleischhauer and M. D. Lukin, *Phys. Rev. Lett.* **84**, 5094 (2000).
- [43] C. Liu, Z. Dutton, C. H. Behroozi, and L. V. Hau, *Nature (London)* **409**, 490 (2001).
- [44] A. J. Menezes, P. C. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, FL, 1997).
- [45] A. Rukhin, J. Soto, J. Nechvatal, M. S. E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray *et al.*, NIST Spec. Publ. 800-22 Revision 1a, <http://csrc.nist.gov/publications/nistpubs/> (2010).