Strathprints Institutional Repository

Roga, Wojciech and Jeffers, John (2016) Security against jamming in imaging with partially-distinguishable photons. In: Quantum Information Science and Technology II. Proceedings of SPIE, 9996 . SPIE, Bellingham, WA. ISBN 9781510603967 , http://dx.doi.org/10.1117/12.2246800

Security against jamming in imaging with partially-distinguishable photons

Wojciech Roga and John Jeffers

SUPA, Department of Physics, University of Strathclyde, John Anderson Building, 107
Rottenrow, Glasgow G4 0NG, UK

ABSTRACT

We describe a protocol in which we detect intercept-resend jamming of imaging and can reverse its effects. The security is based on control of the polarization states of photons that are sent to interrogate an object and form an image at a camera. The scheme presented here is a particular implementation of a general anti-jamming protocol established by Roga and Jeffers in Ref. 5. It is applied here to imaging by photons with partially distinguishable polarisation states. The protocol in this version is easily applicable as only single photon states are involved, however the efficiency is traded off against the intrusion detectability because of a leak of information to the intruder.

Keywords: imaging, security against jamming, intercept-resend jamming, quantum protocol

1. INTRODUCTION. LACK OF PERFECT SECURITY.

Any informational advantage creates the possibility to ensure security of information transmission.[1–5] Claude Shannon formulated this rule in his seminal paper on information-theoretic secrecy in the following way "The enemy [...] does not know what key was chosen and the *might have been* keys are as important for him as the actual one. Indeed it is only the existence of these other possibilities that gives the system any secrecy".[1] In the same paper it was specified that perfect security of an encrypted message is achieved if the knowledge of an encrypted message does not reduce uncertainty about which message has been encrypted. Here, we analyse security against jamming in imaging that is achievable due to an informational advantage possessed by legitimate imagers over an intruder who applies intercept-resend jamming.[5–9] We consider a particular implementation of a jamming detection and correct information recovery protocol established recently in.[5]

Before formulating this protocol as it was originaly posed let us introduce its equivalent in terms of communication scheme in the language of Shannon's secure communication theory. Imagine a communication setup that uses images as messages. The set of all possible messages $\mathcal{M}$ is commonly known to all parties, i.e. a sender, a legitimate receiver and an eavesdropper. For instance, let $\mathcal{M}$ consists of T and Λ-shaped images and all their superpositions, $\alpha\Lambda + (1-\alpha)T$, where $0 \leq \alpha \leq 1$. Information about an image is carried by light reflected from or transmitted through the corresponding object. On the way, at the stage of encryption, the light can be partially intercepted and resent to the receiver in such a way that the image it carries is modified, so encrypted. The set of intercept-resend maps $\mathcal{K} : \mathcal{M} \to \mathcal{M}$ parametrised by r and β as follows

$$\Phi_{r,\beta}(\alpha\Lambda + (1-\alpha)T) = (1-r)(\alpha\Lambda + (1-\alpha)T) + r(\beta\Lambda + (1-\beta)T) \tag{1}$$

forms a set of cryptographic keys. This set is also known by all parties. Knowledge of the actual key parameters r and β allows a legitimate receiver to reverse the action of the key and get the correct message. By knowing only the output, but not the key the eavesdropper cannot say anything about the message. All the messages from $\mathcal{M}$ are equally likely. Indeed, for all outputs there exists a key that leads to all possible messages. Hence, the situation is characterised by perfect security. However, as usual, the devil is hidden in the details of a practical implementation.

The origine of messages consists of a light source that does not possess any information about the message and an object. The light, after interacting with the object, creates the message. The source of light is not

Further author information: Send correspondence to Wojciech Roga: E-mail: wojciech.roga@strath.ac.uk free from different kinds of noise, for instance, undefined polarisation, spectral impurity, mechanical instability, fluctuating temperature etc. All these features are assumed to be random modulations of corresponding quantities and are ignored during the encryption stage, which is focused only on the variables relevant to the set of messages. However, the uncontrolled modulations do not need to be random. Some features such as fluctuations of temperature or polarisation could be carefully designed by a producer of the lamp that collaborates with the enemy. The anti-jamming protocol by Roga and Jeffers[5] essentially indicates that such a source of light is a Trojan Horse that provides precious information to the eavesdropper due to which all the encryption is completely useless. The importance of really random sources in cryptography is also a subject of extensive study, for instance in.[10–14]

On the other hand, if we switch the receiver and the eavesdropper and prevent the new receiver from knowing the key that is now added by the new eavesdropper (called from now on the intruder) the Trojan Horse information that established robustness against privacy is a source of security against unknown intercept-resend jamming, exactly as described in.[5] Again, informational advantage is a source of security.

Detection of jamming in imaging based on additional polarisation degrees of freedom has been analysed in.[6] In this scenario a variation of BB84[15] was applied. The appealing feature of the polarisation degrees of freedom is that in a single photon realisation non-orthogonal polarisations cannot be perfectly distinguished by an eavesdropper's measurement. This is a source of necessary errors that reveal the presence of the intruder. The extended protocol by[5] is based on comparison of static images formed for different polarisation states, where it is assumed that the intruder cannot distinguish the states because, for instance, they have access only to local parts of entangled states in so-called ghost imaging.[16–20] In this scenario no *which state* knowledge leaks to the intruder and the false part of the image introduced by him is uncorrelated to the choice of the state and can be easily eliminated. In this paper we relax the condition of perfect ignorance of the intruder.

We analyse the probability of detection of jamming based only on the images correlated to the different states chosen by legitimate imagers. Moreover, we modify the correct image recovery strategy taking into account that the resent signal can be correlated with the intercepted one to some extent. The correlations cannot be perfect as information of the intruder from a measurement of a quantum state of polarisation of single photons is smaller than information of legitimate imagers who prepare the states.

2. JAMMING IN IMAGING BY PHOTONS WITH PARTIALLY-DISTINGUISHABLE POLARISATION STATES

Let us consider an imaging situation shown in Fig. 1. We assume that photons carrying spatial information about an object are also characterised by one of the polarisation states

$$\rho_1 = |\updownarrow\rangle\langle\updownarrow|, \tag{2}$$
$$\rho_2 = |\leftrightarrow\rangle\langle\leftrightarrow|, \tag{3}$$
$$\rho_3 = |\nwsearrow\rangle\langle\nwsearrow|, \tag{4}$$
$$\rho_4 = |\neswarrow\rangle\langle\neswarrow|. \tag{5}$$

where $|\nwsearrow\rangle = (|\updownarrow\rangle + |\leftrightarrow\rangle)/\sqrt{2}$ and $|\neswarrow\rangle = (|\updownarrow\rangle - |\leftrightarrow\rangle)/\sqrt{2}$. Photons produced by a source of light are sent to interrogate an object, are reflected and directed to a camera. However, before reaching the camera the signal is filtered by a polariser inclined by a fixed angle θ. On the way, a part of the signal is intercepted with rate r by an intruder who resends photons carrying false spatial information. The intruder's photons genuinely carry polarisation states different than the photons sent from the legitimate source. However, states (2)-(5) are not completely indistinguishable. Indeed, the intruder could use a measuring device that can perfectly distinguish, for instance, ρ_1 from ρ_2 but which can detect no difference between the remaining states. The intruder could resend photons with false information with two different polarisation states ρ_1^E and ρ_2^E depending on results of the measurement. In this way some correlations between the polarisations of the false photons with the correct ones are established. As the camera is in the same place as the source the imagers know exactly when particular states from the set (2)-(5) are chosen and can record four images related to the four states. If there is no intrusion the figures should differ only in brightness as there is different probability that the different states pass the polariser. In the detection and recovery strategy delivered in[5] the states could not be distinguished by the intruder, therefore the false contribution to each image was the same and it was easily filtered out just by taking the difference between images corresponding to different states from the legitimate source. However, partial distinguishability of states (2)-(5) allows the false contribution to depend on the state chosen by the legitimate imagers. Simple differencing of images does not filter out this false contribution. This fact has implications for the probability of the intrusion detection based on the images as well as forcing a modification of the correct image recovery protocol. These items are addressed in the following sections.

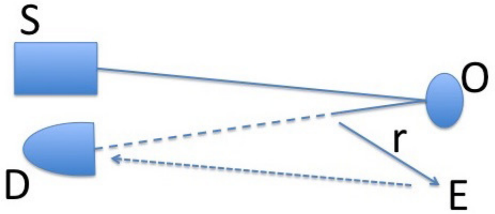

Figure 1. Jamming scheme. A source S produces photons with polarisation states (2)-(5) that are chosen by a legitimate imager. The photons are sent to interrogate an object O. Before arriving at detector D they are partially intercepted with intercepting rate r by intruder E who resends photons with false information to the detector in order to jam the imaging system.

Finally, let us comment on the equivalent communication problem. In this approach the states (2)-(5) would be the Trojan Horse states of the source of light. *Which state* information would lead the eavesdropper to reveal the correct message independently of the applied key that is the counterpart of the intercept-resend jamming process. The recovery protocol would be the same for both approaches as described in Sec. 4.

3. DETECTION OF JAMMING PROBABILITY

The probability that a photon with a polarisation state ρ_j passes an analyser rotated by an angle θ and is detected is given by

$$P\left(\theta,\rho_j\right)=\langle a(\theta)|\rho_j|a(\theta)\rangle, \tag{6}$$

where $|a(\theta)\rangle=\cos\theta|\leftrightarrow\rangle+\sin\theta|\updownarrow\rangle$. By switching between ρ_i and ρ_j we change the probability in a way quantified by the state dependent visibility[5]

$$V(\rho_i,\rho_j,\theta)=\frac{|P_i-P_j|}{P_i+P_j}, \tag{7}$$

where P_i and P_j are photon detection probabilities for states ρ_i and ρ_j respectively as in (6). For brevity, we omit the arguments of P_i and P_j. We assume that $P_j=P_j\left(\theta,\rho_j\right)$, so that P_j is defined for a specific state and for a chosen analyser angle. The state-dependent visibility allows us to compare quantitatively images formed by photons with different polarization states at a given point in the imaging plane. Notice that for $\rho_i=\rho_j$ the visibility $V(\rho_i,\rho_j,\theta)$ vanishes, showing that the images are identical. If, instead, for two different states $V\neq 0$ then the intensity distributions of two images are different.

Jamming is detected if for two given legitimate states ρ_i and ρ_j the measured state dependent visibility is different from than the expected one $V(\rho_i,\rho_j,\theta)$. In realistic experiments we need to decide whether an observed deviation of the measured from expected visibility is an effect of jamming or of the experimental uncertainty we tolerate. To solve this problem we estimate the probability of jamming detection based on hypotheses testing, see.[5] The probability is a monotonic function of the normalised difference between the expected and measured state dependent visibility

$$d=\frac{1}{\sigma}\Big(V(\rho_i,\rho_j,\theta)-V(\rho_i',\rho_j',\theta)\Big), \tag{8}$$

where σ is the variance of the noise which we assume to be Gaussian. The formula can be optimised to find the optimal pair of states and polariser angle such that the intruder detection probability is maximized. We assume the worst case scenario in which the intruder knows the polariser position θ and the set of chosen states.

Unlike in[5] where the intruder's states were completely independent of the choice of states by the legitimate imagers, here the intruder can resend more than one state ρ_j^E. Which of them is to be resent depends on the choice of the legitimate imagers to some extent. This is a consequence of the partial distinguishability of (2)-(5). Let us examine the possible behaviour of the intruder. They can use a polarising beam splitter oriented along an angle ϕ that allows them to distinguish a state that has a component along a given axis from the states that do not have this component. By knowing this partial information about the choice by the legitimate imagers, the intruder can resend the photons with polarisations partially correlated to the correct states. Therefore, the false contribution to images may depend on the choice of states, as does the correct contribution. In consequence, $V(\rho_i', \rho_j', \theta)$ in (8) is non-zero and closer to $V(\rho_i, \rho_j, \theta)$. Hence, d and the probability of detection are reduced.

Let us consider an intrusion strategy and see how it affects the probability of detection. Assume that the imager uses a polarisation state ρ_j to test an object. An intruder intercepts this photon with probability r, measures its polarization using an analyser inclined by an angle ϕ. Depending on the effect of the measurement the intruder chooses their state in the state ρ_1^E or ρ_2^E. The imager obtains a photon in the mixed polarisation state as follows

$$\rho_j' \quad = \quad (1-r)\rho_j + r(\langle a(\phi)|\rho_j|a(\phi)\rangle\rho_1^E + (1 - \langle a(\phi)|\rho_j|a(\phi)\rangle)\rho_2^E), \tag{9}$$

where $|a(\phi)\rangle$ is given as in (6).

$\rho_j' = (1-r)\rho_j + r(\langle\phi|\rho_j|\phi\rangle\rho_1^E + (1 - \langle\phi|\rho_j|\phi\rangle)\rho_2^E)$

In the scenario with partially distinguishable legitimate states ρ_i, in order to minimize d, the intruder can tune the jamming by choosing carefully the set of parameters r, ϕ and states ρ_1^E and ρ_2^E.

Taking into account that also the legitimate imagers can choose imaging parameters to maximize the chance of jamming detection. If the imagers do not know the strategy of the opponent then the worst case scenario should be assumed. Then probability of jamming detection should be estimated based on

$$d = \frac{1}{\sigma}\max_{\theta}\left\{\min_{r,\phi,\rho_1^E,\rho_2^E}\left[\max_{i,j}\Big(V(\rho_i,\rho_j,\theta) - V(\rho_i',\rho_j',\theta)\Big)\right]\right\}, \tag{10}$$

This complicated chain of optimisations contains the logic of the process. This formula expresses the fact that the imagers collect images obtained from 4 states in the same imaging process and can choose after the process which images will be compared in order to detect jamming. The choice of ρ_i^E by the intruder does not depend on this optimisation stage. In other words, the intruder has to decide which states to use in jamming assuming the worst case scenario, i.e. that the legitimate imagers will maximize the detection chances. On the other hand the legitimate imagers need to decide the angle θ of their polariser before the imaging process. To choose it reasonably, they need to assume the worst case attack, i.e. the intruder is using best strategy.

To illustrate the detection strategy we analyse a concrete example. The polariser angle θ is such that ρ_1 passes and ρ_2 is blocked. Therefore, $\langle a(\phi)|\rho_1|a(\phi)\rangle = 1$ and $\langle a(\phi)|\rho_2|a(\phi)\rangle = 0$. Hence, the intruder is able to perfectly distinguish ρ_1 from ρ_2 and resend photons with false information in the polarisation state $\rho_1^E = \rho_1$ and $\rho_2^E = \rho_2$ depending on the result of the measurement. In this case visibility $V(\rho_1, \rho_2, \theta)$ is equal to $V(\rho_1', \rho_2', \theta)$ and the probability of detection based on these two states is zero. The image can be jammed arbitrarily well. On the other hand, images obtained when ρ_3 and ρ_4 are sent have the same contribution of the false image. In this case $V(\rho_3, \rho_4, \theta) \neq V(\rho_3', \rho_4', \theta)$ allowing for more efficient detection of the jamming and application of the recovery protocol.

Without constraints on ρ_i^E, ϕ and r the problem (10) is trivial as d reaches zero for instance for $r = 0$. Therefore, in order to select an optimal strategy of jamming detection it is reasonable to calculate (10) assuming a non-trivial constraint. We chose to optimize d keeping the level of jamming[5] defined as follows

$$V_L = \max_j \; V(\rho_j, \rho_j', \theta) \tag{11}$$

fixed. This quantity estimates how much an image is different from a correct one assuming that jamming occurs.

Finally, formula (10) allows us to calculate probability of jamming detection numerically. It is plotted in Fig. 2. During the minimization the intruder's states ρ_1^E and ρ_2^E are assumed to be pure, single-qubit states from

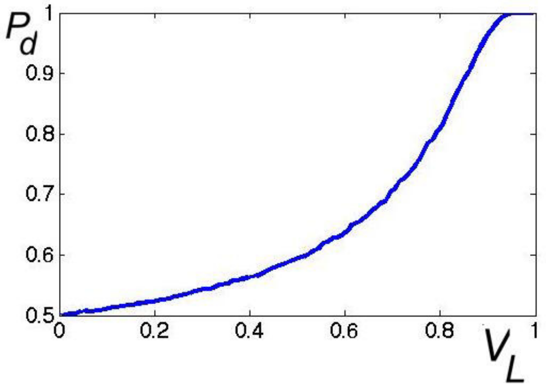

Figure 2. Jamming detection probability based on the hypotheses testing scheme with the variance of measured visibility equal to $\sigma = 0.1$.

the one parameter family $\alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle$ with $0 \leq \alpha \leq 1$. We observe that for small levels of jamming the probability of detection is not significant. In this region the intruder can take more advantage of the knowledge about states from the legitimate source.

4. IMAGE RECOVERY BY WEIGHTED DIFFERENCE

In this section we show an example of correct image recovery if photons with partially distinguishable polarisation states from the set ρ_1 - ρ_4 given in (2) - (5) respectively are chosen by the legitimate imagers. In this example we assume that the intruder intercepts and resends photons at rate $r = 1/2$. The intercepted photons are measured by an analyser that allows states ρ_3 to pass. States ρ_4 are blocked by the analyser, but states ρ_1 and ρ_2 pass with probability 1/2. If a photon passes the analyser the intruder resends a photon carrying false information with polarisation $\rho_1^E = \rho_3$, otherwise the polarisation state $\rho_2^E = \rho_2$ is resent. The legitimate imagers take four pictures using the four states. To introduce controlled distinction between the pictures an analyser directed along the polarisation axis of ρ_1 is applied. The images are formed by the states partially corrupted by the intruder according to (9). Finally, the legitimate imager has freedom to chose which images are taken into account as intrusion detection and image reconstruction protocol is delivered. Fig. 3 shows the situation if images related to ρ_1 and ρ_2 are chosen. The upper left picture shows the image corresponding to ρ_1. The probability that the photons from the legitimate source pass the analyser is 1/2. The intensity of the correct contribution is proportional to this value. The brightness of the false image is proportional to the probability of passing the analyser by the false image bearing photons, i.e. 1/8 in this case. The upper right picture of Fig. 3 shows the situation if the legitimate imager switches the state from ρ_1 to ρ_2. The correct contribution disappears while the false image has brightness proportional to 1/4. As we recognise the false contribution we take a weighted difference of the two images with a weight such that the false part disappears. In consequence, we obtain only the correct contribution. It is shown in the lower right quarter of fig. 3. Finally, for comparison, the image without jamming is shown in the lower right corner. This demonstrates the recovery protocol.

5. CONCLUSIONS

In this paper we apply a correct image recovery protocol for partially jammed images recently established in[5] to a particular problem of imaging by photons with different, partially distinguishable states of polarisation. Naturally, legitimate imagers who prepare the states possess more knowledge about them than can be extracted from any measurement. Therefore, there exists an informational advantage that is a source of security against jamming. We estimate the probability of jamming detection based only on intensities of images corresponding to different states as a function of jamming level. This probability is evidently lower for small amounts of jamming than the counterpart for indistinguishable states analysed in.[5] The reason is that, having some partial information about which states have been chosen by imagers, the intruder imitates the correct signal. In this case for small levels of invasions it is easy to misconstrue the intrusion as experimental inaccuracy. However, as

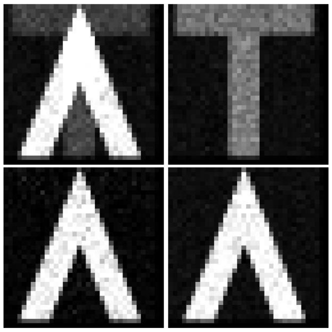

Figure 3. The upper left image shows the mixture of the correct (Λ-shape) and the false (T-shape) image obtained using states (2) and (3) respectively. The upper right image shows the false image. In this case, the correct part disappears because the legitimate states (3) are blocked by a polariser. The lower left image shows the recovered image. For comparison, the lower right image shows the image without jamming.

the knowledge of the intruder is not complete, errors in the imitation of correct states must appear. Therefore, a false contribution to images is created by photons with polarisation states uncorrelated with the actual choices of states carrying correct information. This part can be recognised and a modified version of recovery protocol by[5] can by successfully applied.

We have also shown that intercept-resend jamming in imaging is related to a communication scheme in which messages are represented by images. These scheme can be characterised by perfect security in the sense of,[1] but can possess a Trojan Horse element in the source of light carrying the image. Our protocol implies that if an eavesdropper knows a pattern of some light modulations that look like random noise then any intercept-resend type encryption can be broken if $r > 0$.

In consequence, a perfect cryptographic key

can be created only if the resent light perfectly imitate all the modulations of the signal carrying an unencrypted message, even though the modulations look like random noise. Alternatively, the source should be certified as experienced only perfectly random modulations that is also a nontrivial problem.[10–14, 21]

ACKNOWLEDGMENTS

The work was supported by the QuantIC Project of the UK Engineering and Physical Sciences Research Council (EP/M01326X/1).

REFERENCES

[1] C. E. Shannon, "COMMUNICATION THEORY OF SECRECY SYSTEMS," *Bell Labs Tech. J.* **28**, 656-715 (1949).

[2] A. D. Wyner, "WIRE-TAP CHANNEL," *Bell Syst. Tech. J.*, **54**, 1355-1387 (1975).

[3] I. Csiszàr and J. Körner, "BROADCAST CHANNELS WITH CONFIDENTIAL MESSAGES," *IEEE Trans. Inf. Theory*, **24**, 339-348 (1978).

[4] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "KEY GENERATION FROM WIRELESS CHANNELS: A REVIEW," *IEEE Access*, **4**, 614-626 (2016).

[5] W. Roga, and J. Jeffers, "SECURITY AGAINST JAMMING AND NOISE EXCLUSION IN IMAGING," *Phys. Rev. A* **94**, 032301-032301-6 (2016).

[6] M. Malik, O. S. Magańa-Loaiza, and R. W. Boyd, "QUANTUM-SECURED IMAGING," *Appl. Phys. Lett.* **101**, 241103-241103-4 (2012).

[7] T. S. Humble, R. S. Bennink, W. P. Grice, and I. J. Owens, "INTRUSION DETECTION WITH QUANTUM MECHANICS: A PHOTONIC QUANTUM FENCE," 26. Army Science Conference; Orlando, FL, Dec. 14, 2008 (Oak Ridge National Laboratory, Oak Ridge, TN, 2008).

[8] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, ”EXPERIMENTAL QUANTUM CRYPTOGRAPHY,” *J. Cryptology* **5**, 3-28 (1992).

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, ”QUANTUM CRYPTOGRAPHY,” *Rev. Mod. Phys.* **74**, 145-195 (2002).

[10] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, ”A FAST AND COMPACT QUANTUM RANDOM NUMBER GENERATOR,” *Rev. Sci. Instrum.* **71**, 1675-1680 (2000).

[11] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, ”OPTICAL QUANTUM RANDOM NUMBER GENERATOR,” *J. Mod. Opt.*, **47**, 595-598 (2000).

[12] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, ”A HIGH SPEED, POST-PROCESSING FREE, QUANTUM RANDOM NUMBERGENERATOR,” *Appl. Phys. Lett.* **93**, 031109-031109-3 (2008).

[13] U. Atsushi, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, ”FAST PHYSICAL RANDOM BIT GENERATION WITH CHAOTIC SEMICONDUCTOR LASERS,” *Nature Photon.*, **2**, 728-732 (2008).

[14] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, ”SECURE SELF-CALIBRATING QUANTUM RANDOM-BIT GENERATOR,” *Phys. Rev. A* **75**, 032334-032334-5 (2007).

[15] C. Bennett, and G. Brassard, ”QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING,” in *Proceedings of IEEE International Conference CSSP*, Bangalore, India, p. 175-179 (1984).

[16] T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, ”OPTICAL IMAGING BY MEANS OF TWO-PHOTON QUANTUM ENTANGLEMENT,” *Phys. Rev. A* **52**, R3429-R3432 (1995).

[17] B. I. Erkmen, and J. H. Shapiro, ”GHOST IMAGING: FROM QUANTUM TO CLASSICAL TO COMPUTATIONAL,” *Adv. Opt. Photon.* **2**, 405-450 (2010).

[18] K. W. C. Chan, M. N. O'Sullivan, and R. W. Boyd, ”TWO-COLOR GHOST IMAGING,” *Phys. Rev. A* **79**, 033808-033808-6 (2009).

[19] R. S. Aspden, N. R. Gemmell, P. A. Morris, D. S. Tasca, L. Mertens, M. G. Tanner, R. A. Kirwood, A. Ruggeri, A. Tosi, R. W. Boyd, G. S. Buller, R. H. Hadfield, and M. J. Padgett, ”PHOTON-SPARSE MICROSCOPY: VISIBLE LIGHT IMAGING USING INFRARED ILLUMINATION,” *Optica*, **2**, 1049-1052 (2015).

[20] R. S. Bennink, S. J. Bentley, and R. W. Boyd, ”TWO-PHOTON COINCIDENCE IMAGING WITH A CLASSICAL SOURCE,” *Phys. Rev. Lett.* **89**, 113601-113601-4 (2002).

[21] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, ”RANDOM NUMBERS CERTIFIED BY BELL'S THEOREM,” *Nature*, **464**, 1021-1024 (2010).