Quantum-Secured Single-Pixel Imaging against Jamming Attacks

Jaesung Heo, Junghyun Kim, Taek Jeong, Yong Sup Ihn, Duk Y. Kim, Zaeill Kim, and Yonggi J;
Agency for Defense Development, Daejeon, South Korea
(Dated: September 15, 2022)

We propose a quantum-secured single-pixel imaging method exploiting non-classical correlations of a photon-pair for preventing a possible jamming attack. Our method is based on a single-pixel imaging which exploits spatial correlations between target-illuminating photons and the number of measured photons after a target interaction. To reduce effects of external noises, time-correlation of non-classically correlated photon-pairs is exploited. Simultaneously, security of the imaging method is investigated by analyzing polarization-correlation of the photon-pairs. By photon heralding, our method can obtain an image under an imaging disrupting attack by using strong chaotic light. Also, it is able to detect a deceiving attack based on the polarization-correlation. As a result, images obtained from a proof-of-principle demonstration are provided, and we show that the statistical errors in polarization measurement can reveal a deceiving attack. The proposed method can be developed by adopting matured techniques used in quantum secure communication.

I. INTRODUCTION

Non-classical correlations are the essential source of a quantum advantage in various quantum information protocols. For example, in entanglement-based quantum key distribution (QKD) and quantum-secured imaging, the correlation provides security against a possible eavesdropping attack in the quantum channel, and quantum ghost imaging exploits the correlation for enhancing signal-to-noise ratio (SNR) of an image beyond the classical limit. In the original correlation-based quantum-secured imaging, an attack for deceiving the imaging system can be detected by analyzing non-classical correlation, and SNR of an image is enhanced like QGI. After its first proposal, there was experimental demonstration of the quantum-secured ghost imaging in time-frequency domain.

The first proposal of quantum-secured imaging was based on prepare-and-measure manner, and in the protocol, a photon exploited for the security check simultaneously contributes to the imaging protocol. However, in the correlation-based quantum-secured imaging, the security check and the imaging protocol are sequentially performed, i.e., some photon-pairs are used for the security check, and the others are exploited for the imaging process. Also, for quantum ghost imaging, an electron-multiplying charge-coupled device (EMCCD) has limited range of acceptable noise.

In this article, we propose a quantum-secured single-pixel imaging (QS-SPI) setup and describe its security. Experimental realization will be shown in Sec. III, and finally, it is concluded in Sec. IV.

II. QUANTUM-SECURED SINGLE-PIXEL IMAGING

In SPI, an image is constructed by using a correlation between spatial information of a beam illuminating a target and intensity of the beam measured after interaction with the target. A spatial light modulator (SLM) is used to modulate the spatial profile of the incident beam, and single-pixel detector such as a photodiode is exploited to measure the intensity. A target image can be constructed based on the correlation obtained after several repetitions with various spatial patterns modulated by the SLM. QS-SPI exploits correlations of photon-pairs, so it needs to control or measure signals in a single-photon level. A digital micromirror device (DMD) has higher reflectivity compared to liquid crystal based SLM, thus beneficial for the usage in single-photon regime. Moreover, DMD is independent of the polarization of an incident photon, different from a liquid crystal based SLM. Thus, DMD is exploited for our setup, and the measurement setup consists of photon-pairs. By photon heralding, our method can obtain an image under an imaging disrupting attack by using strong chaotic light. Also, it is able to detect a deceiving attack based on the polarization-correlation. As a result, images obtained from a proof-of-principle demonstration are provided, and we show that the statistical errors in polarization measurement can reveal a deceiving attack. The proposed method can be developed by adopting matured techniques used in quantum secure communication.
FIG. 1. A schematic diagram of QS-SPI. Alice who has the imaging system generates polarization entangled state. One photon in the signal mode of the entangled state is sent to an SLM, and only photon that has allowed position is reflected at the SLM. The photon illuminates a target and is measured by SPCMs after its interaction with the target. The other photon in the idler mode is measured by the other SPCMs. Time-correlation and polarization-correlation of the two modes are analyzed from the detections of the SPCMs.

Let us denote $k$-th spatial pattern as $P(k)$ and its corresponding measured intensity as $I(k)$. Then, spatial correlation function $G$ for constructing an image is calculated from the following equation:

$$G(i,j) = \langle P(k)(i,j)I(k) \rangle - \langle P(k)(i,j) \rangle \langle I(k) \rangle,$$  

where $i$ and $j$ represent the pixel position of 2D image and $\langle \cdot \rangle$ denotes averaging for the whole $N$ patterns. In QS-SPI, the intensity $I(k)$ is obtained from the coincidence counts of the signal and idler modes. Like heralded SPI, an external noise contribution in $I(k)$ is significantly suppressed due to time-correlation of a photon-pair and narrow time window of SPCMs. Thus, QS-SPI is naturally immune to the imaging disrupting attack that strong chaotic light illuminates an imaging system to saturate the sensor.

Fig. 2 shows a schematic diagram of QS-SPI under a possible attack. An enemy, called Eve, tries to deceive the imaging system. Eve modulates the number of photons induced in an image sensor to make the imaging system constructing a fraud image. Simultaneously, when a photon is sent to the sensor, Eve performs an intercept-and-resend attack for the least disturbance of the polarization of the received photon.

A. Method of Image Deceiving Attack

Security analysis method of QKD has been well-established for protecting photon carrying information against eavesdropping, which is directly related to the generation of secret keys. For example, in polarization-based QKD, polarization-encoded information of a photon is critical to secret key. There are many advanced attacks for extracting polarization-encoded information of successively transmitted photons such as collective attack, which exploits demanding technologies including quantum cloning machines[19, 20], quantum memories[21], and collective measurements.[22, 23] However, in SPI, the main purpose of an attack is deceiving an imaging system to construct a fake image rather than eavesdropping secret keys. For this purpose, the meaningful attack is modulating intensity (photon number) of the light induced in the image sensor for fake image formulation. Under this circumstance, intercept-and-resend attack is the probable attack strategy for image deceiving attack.[4]

Fig. 2 shows a schematic diagram of QS-SPI under a possible attack of an enemy called Eve. It is assumed that Eve can exploit all implementations allowed by the laws of physics and all processes of QS-SPI are known to Eve. For the deceiving attack, Eve possesses time-resolved single-photon detectors with polarization control and an on-demand single-photon source with polarization control. Eve intercepts Alice’s signal photon and discriminate its polarization. Since it is not possible to measure a quantum state in conjugate bases simultaneously, disturbance in original photon state is retained and measured to analyze correlations with the signal photon. In the QS-SPI setup, four SPCMs are exploited to measure time-correlation and polarization-correlation.

Security analysis method of QKD has been well-established for protecting photon carrying information against eavesdropping, which is directly related to the generation of secret keys. For example, in polarization-based QKD, polarization-encoded information of a photon is critical to secret key. Therefore, advanced attacks for extracting polarization-encoded information of successively transmitted photons such as collective attack, which exploits demanding technologies including quantum cloning machines[19, 20], quantum memories[21], and collective measurements.[22, 23] However, in SPI, the main purpose of an attack is deceiving an imaging system to construct a fake image rather than eavesdropping secret keys. For this purpose, the meaningful attack is modulating intensity (photon number) of the light induced in the image sensor for fake image formulation. Under this circumstance, intercept-and-resend attack is the probable attack strategy for image deceiving attack.[4]
inevitable. After the polarization measurement, without a delay, the on-demand single-photon source generates a photon with the measured polarization, and the photon is sent to Alice. SPI constructs an image by spatial pattern information and the number of received photons, so Eve should control $n_g/n_m$ according to the DMD pattern to make QS-SPI construct a fraud image, where $n_g$ ($n_m$) is the number of generated (measured) photons of Eve.

As the signal and idler are polarization entangled state, expected polarization of signal is determined when polarization of idler is measured, and only such combination can be detected ideally. However, intercept-and-resend attack leads to detection of signal photons in unexpected polarization, which is what QS-SPI uses to check its security. Details of the security check will be described in the following section.

**B. Security Check in QS-SPI**

Presence of Eve is tested by Alice via measuring photons in mutually unbiased bases (MUBs). One basis, named rectilinear basis, consists of horizontal and vertical polarization, and the other basis, diagonal basis, does diagonal (D) and anti-diagonal (A) polarization. For the two bases, the following relations are satisfied:

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle),$$

and thus, the two bases are MUBs. Alice, who has a QS-SPI system, randomly chooses the measurement basis for the security check. Different from QKD, it is not necessary for the basis choice of signal and idler modes to be independently random, since the measurement setups of the both modes belong to Alice.

Let us define $r_1 := H$, $r_2 := V$, $d_1 := D$, and $d_2 := A$, then the following relations are satisfied:

$$P(X_i, X_j) = \frac{C(X_i, X_j)}{\sum_{i,j=1}^{2} C(X_i, X_j)},$$

where $C(x, y)$ is the coincidence counts of $x$- and $y$-polarized photons in the signal and idler modes, respectively, $P(x, y)$ is the probability of the coincidence count to happen, $X \in \{r,d\}$, and $i, j \in \{1, 2\}$. From Eq. (2), $P(X_i, X_i) = 1/2$ and $P(X_i, X_j) = 0$ for $i \neq j$, indicating that the latter coincidence count is unexpected. Error rate can be defined by the ratio of unexpected coincidence count to all coincidence counts. Since idler photon is unhindered by Eve’s attack, an error rate is defined with respect to polarization of idler. Thus, a polarization error rate when an idler photon is detected on the SPCM corresponding to the polarization $X_i$ is written as following:

$$e_{X_i} = \frac{C(X_i, X_j)}{\sum_{k=1}^{2} C(X_k, X_i)},$$

where $i \neq j$.

In ideal, the error rates are always zero. However, if there is an enemy who tries to disturb the imaging system, the probabilities are affected by enemy’s attack, so Alice can notice the presence of Eve by analyzing the error rates.

Eve possesses its own MUBs for polarization measurement. Let us denote its constitutive polarizations in primed notation, i.e., $H'$, $V'$, $D'$, and $A'$. For the same choice of measurement basis of Alice and Eve, let the angle difference between the two as $\theta$, measured in counterclockwise from one polarization of the Alice to that of the Eve, i.e., angle measured from $H$-polarization to $H'$-polarization in counterclockwise. Then, the angle difference between different bases is $\theta \pm \frac{\pi}{2}$. If idler photon is measured as $H$-polarization in the rectilinear basis by Alice, then Alice’s rectilinear polarization measurement on the signal photon always gives $H$-polarization. If Eve chooses its own rectilinear basis, Eve’s setup measures $H'$-polarization and $V'$-polarization with probabilities $\cos^2 \theta$ and $\sin^2 \theta$, respectively. Regardless of Eve’s result, Alice’s error rate, i.e., detection of $V$-polarized signal, is $\cos^2 \theta \sin^2 \theta$. Thus, the error rate observed by Alice is following:

$$2\cos^2 \theta \sin^2 \theta = \frac{1 - \cos^2 2\theta}{2}. \tag{5}$$

If Eve chooses the other measurement basis, the error rate is calculated by replacing $\theta$ to $\theta \pm \frac{\pi}{4}$:

$$\frac{1 - \sin^2 2\theta}{2}. \tag{6}$$

Since Eve’s basis choice is random, the $H$-polarization error rate is calculated as the following equation:

$$e_H = \frac{1}{2} \left( \frac{1 - \cos^2 2\theta}{2} + \frac{1 - \sin^2 2\theta}{2} \right) = \frac{1}{4}. \tag{7}$$

The result indicates that the criterion error rate for determining the presence of an attack is 25% regardless of the angle difference $\theta$. If the error rate is less (greater) than 25%, the protocol is reliable (compromised).

**III. PROOF-OF-PRINCIPLE DEMONSTRATION**

**A. QS-SPI setup**

Fig. 3 shows setups for proof-of-principle demonstration of QS-SPI. A polarization-entangled state is generated from the Sagnac interferometer with periodically poled potassium titanyl phosphate (ppKTP) crystal. The crystal is pumped by 405 nm continuous wave (CW) laser, generating 810 nm polarization-entangled photon-pairs via type-II SPDC process. The initial state generated from the Sagnac interferometer is $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_V|V\rangle_H + |V\rangle_V|H\rangle_H)$, so to make the state be $|\Phi^+\rangle$, additional phase shifts on the idler mode is given. Fig. 4 shows the results of quantum state tomography of the generated state. The figure shows that $|\Phi^+\rangle$ is well-prepared with its fidelity 98.6%.
FIG. 3. Experimental setups of our QS-SPI. A polarization-entangled photon-pair is generated by the Sagnac interferometer with ppKTP crystal, and polarization of its idler photon is directly detected by SPCMs. The signal photon is reflected by the DMD with post-selection of its position and sent to the target, an alphabet letter "A". After interaction with the target, the photon is counted by SPCMs in selected polarization. Eve's attack is demonstrated by blocking Alice’s signal photon and sending polarization-controlled laser beam with intensity modulation. Accidental coincidence counts in Alice’s TCSPC is occurred by Eve’s light, so the fraud image, an alphabet letter "D", is constructed in Alice’s system. PBS: polarizing beam splitter; QWP (HWP): quarter (half) wave plate; ND filter: neutral density filter.

FIG. 4. The result of quantum state tomography of our source: (a) the real values of the density operator; (b) the imaginary values. These graphs indicate that $|\Phi^+\rangle$ is well-prepared, and its fidelity is 98.6%.

After the generation, the idler mode is detected by SPCMs (Excilites Technologies, SPCM-780-13-FC) in selected polarization. SPCMs are connected to a time-correlated single photon counting (TCSPC) module to record the photon counts with detected time and polarization. The signal photon is sent to the DMD (Vialux GmbH, DLP650LNIR), and the photon is post-selected by a displayed pattern on the DMD. The DMD displays the Hadamard patterns for enhancing image quality with restricted number of shots.$^{[26–29]}$ A $2^n+1 \times 2^n+1$ Hadamard matrix is calculated by the following equation:

$$H_{2n+1} = H_{2n} \otimes H_2,$$

(8)

where

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

(9)

and $\otimes$ denotes tensor product. Hadamard patterns are generated by reshaping each row of the Hadamard matrix $H_{2n}$ into a $2^n \times 2^n$ square matrix. Since the negative pixel value cannot be displayed, two shots are necessary to represent a Hadamard pattern.$^{[18]}$ The first intensity pattern has bright and dark pixels for the matrix elements 1 and -1, respectively, and the other one is its inverse. The resolution of our Hadamard patterns is $32 \times 32$, so the total number of shots becomes 2048.

The spatially post-selected signal photons interact with the target, an alphabet letter "A", and the number of transmitted photons is counted by SPCMs. The four SPCMs are connected to a TCSPC module, and coincidence counts of one SPCM in the signal mode and the other SPCM in the idler mode are analyzed by the TCSPC to construct an image and analyze security. The other coincidence counts such as that of SPCMs in the same mode or of multiple SPCMs are discarded.

In the setup, power of pump laser for generation of the entangled photon-pairs was 5 mW. Single count rates of the signal and idler were $6 \times 10^3$ cps and $8 \times 10^4$ cps, respectively.
when there is no target. Under the same condition, we set the coincidence window as 650 ps, and coincidence count rate of the signal and the idler in the same polarization was 300 cps. The accumulation time of one Hadamard pattern was 3.5 seconds.

B. Demonstration of Eve’s attack

As previously described, Eve’s intercept-and-resend attack exploits on-demand single-photon generator to make a generated photon enter within the coincidence window. However, since the implementation is not feasible with current technologies, we demonstrate a realistic attack with implementable devices.

Since QS-SPI constructs an image based on coincidence counts information, Eve needs to control the coincidence count for deceiving the system. In our deceiving attack, Eve’s 810 nm CW laser illuminates Alice’s receiver to make accidental coincidence counts occur. For the accidental coincidence counts to be dominant, Eve blocks Alice’s signal mode. Instead of polarization control based on the measured information, we fix the polarization of the illumination laser as $H'$, which is set to have approximately 0.10 radian angle difference with $H$ to show the effect of Eve’s misaligned bases. This demonstration provides a simulation of the intercept-and-resend attack, since the statistics of Alice’s polarization measurement in the diagonal basis is similar to those of the intercept-and-resend attack when Alice’s and Eve’s bases are different.

To deceive Alice’s setup, accidental coincidence count rate needs to be similar to the coincidence count rate of the entangled photon-pairs. To achieve this condition, the power of Eve’s laser is determined as follows. The detection probabilities per window on the signal and idler mode SPCMs are $n_E \tau$ and $n_I \tau$, respectively, where $n_E$ is the mean photon number of Eve’s laser and $\tau$ is a coincidence window. In this case, the coincidence probability in the coincidence window is given by the product of the single probabilities, $n_E n_I \tau^2$. Then, the accidental coincidence count rate $n_{\text{acc}}$ can be calculated from the following equation:

$$ n_{\text{acc}} = n_I n_E \tau. $$

To make $n_{\text{acc}} \sim 300$ cps, the coincidence count rate of the entangled photon-pairs, with $n_I = 8 \times 10^4$ cps and $\tau = 650$ ps, we obtain $n_E \sim 5.8 \times 10^6$ cps, which is 1000 times greater than the original signal photon count rate without a target. This photon number corresponds approximately to the 1.41 pW for an 810 nm CW laser. Intensity modulation of Eve’s laser, which is necessary to deceive SPI, is performed by using another DMD. The Eve’s DMD displays the overlapped patterns between Alice’s Hadamard patterns and a fraud image, directly. Then at the end of the protocol, the fraud image, an alphabet letter "D", is constructed by the QS-SPI setup from the accidental coincidence counts induced by Eve.

C. Results

Fig. 5 shows the images obtained under the imaging disrupting attack by the original SPI (left) and by our QS-SPI (right). In the attack, Eve’s laser, of which the power is 1000 times larger than the original signal, illuminates Alice’s receiver to disturb the imaging process. The image obtained by SPI is ruined by the laser, however, due to the time-correlation of a photon-pair, the target image is successfully constructed by QS-SPI.

Fig. 6 shows the obtained images with our QS-SPI setup without an attack (left) and under Eve’s attack (right). In both cases, the images are well-constructed, so Alice cannot notice the presence of the attack from the obtained images. Therefore, to check the security, we analyze average of the four polarization errors given in Eq. (4). When there is no attack, the average error rate is suppressed below 5%, however, under
Eve’s attack, the error rate becomes nearly 50%.

Fig. 7 shows the images and corresponding polarization error rates with their standard deviations. When there is no Eve, all the error rates are suppressed below 5%, so the security of the obtained images is guaranteed. Under Eve’s attack, since Eve’s laser has $H'$-polarization, $H$-polarization error rate is below 5% but $V$-polarization error rate exceeds 95%. In the diagonal basis, $D$-polarization error rate is nearly 40%, and $A$-polarization error rate exceeds 60%. The both error rates in the diagonal basis are larger than 25% in Eq. (7), so Alice can notice that the obtained image is fake.

In theory, $D$-polarization and $A$-polarization error rates with the $H'$-polarized light are given by $\sin^2 (\frac{\pi}{4} - \theta) \approx 0.40$ and $\cos^2 (\frac{\pi}{4} - \theta) \approx 0.60$, respectively, and these values are well-matched with our experimental results.

Note that our attack scenario does not directly simulate the intercept-and-resend attack. There is no basis choice in our setups in Eve’s side, however, in the intercept-and-resend attack, there is a random basis choice step. Since Eve’s correct basis choice does not induce an error in the polarization statistics, the probability of mismatched basis choice, $1/2$, should be considered in the intercept-and-resend attack. Thus, to simulate the intercept-and-resend attack, our error rates in the diagonal basis would be considered to halve. Even we consider these differences, $A$-polarization error is still larger than 25%, so we can expect that Eve’s intercept-and-resend attack also can be noticed with our QS-SPI.

Moreover, in the intercept-and-resend attack, Eve sends both polarizations in the mismatched basis, in this case, $H'$- and $V'$-polarization, however, in our demonstration, only the $H'$-polarized laser illuminates Alice’s receiver. If we modify the setup including a random choice of $H'$- and $V'$-polarized laser, then both error rates in the diagonal basis would become similar.

IV. SUMMARY AND DISCUSSION

In this article, we provide a methodology of quantum-secured single-pixel imaging (QS-SPI) against jamming attacks. By exploiting time-correlation and polarization-correlation, all detected photon-pairs are used for imaging and security checking, simultaneously. QS-SPI is naturally immune to an imaging disrupting attack, an enemy illuminating sensor with strong chaotic light, since it is based on the heralded SPI scheme. A deceiving attack, such as an intercept-and-resend attack can be detected from polarization statistics, since an attack induces errors in the statistics. We demonstrated QS-SPI setup and deceiving attack as well. The attack is able to completely deceiving SPI, however, we showed that QS-SPI can detect the attack by analyzing the statistics. We presented that an intercept-and-resend attack can be simulated from the results of our demonstrated deceiving attack and that QS-SPI can detect the intercept-and-resend attack as well.

To use QS-SPI as an application, implementation of an active random basis choice is very hard. Thus, our active basis choice setups and two SPCMs can be modified to passive ones consisting of a 50:50 beam splitter, phase shifters, and four SPCMs corresponding to four polarization detection. In the modified scheme, the photon-pair detected at SPCMs with mismatched basis should be discarded under our security check. However, if we introduce a security check based on the Bell inequality, especially the Clauser-Horne-Shimony-Holt (CHSH) inequality, then all bases combinations are exploited to check a security and construct an image without discarding photon-pairs. In the security check, the absence of an attack is guaranteed if the polarization statistics violates the Bell inequality, and this security provides a device-independent security.

Since our setup exploited time-correlation of signal and idler photons, time-of-flight information of a signal photon should be measured. Therefore, QS-SPI naturally includes a quantum-secured optical ranging protocol i.e., QS-SPI provides a method to securely acquire a target distance against jamming attacks.

We expect that QS-SPI can be developed with matured techniques exploited in quantum secure communication. For example, six polarization states in three possible MUBs can be used to enhance security or for reference-frame-independent security analysis and various degrees-of-freedoms in a single photon can be used to exploit high-dimensional quantum states or hyper-entangled states. It is expected that our method can be developed to quantum-secured LiDAR with quantum-correlation-based free-space experiment techniques as well.

ACKNOWLEDGMENTS

This work was supported by the Agency for Defense Development Grant funded by the Korean Government.

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

AUTHOR CONTRIBUTIONS

Jaesung Heo: Data curation (lead); Formal analysis (equal); Investigation (lead); Methodology (supporting); Validation (equal); Visualization (equal); Writing – original draft (lead); Writing – review & editing (equal). Junghyun Kim: Conceptualization (supporting); Data curation (supporting); Investigation (supporting); Methodology (supporting); Writing – review & editing (supporting). Taeck Jeong: Conceptualization (supporting); Data curation (supporting); Investigation (supporting); Methodology (supporting); Writing – review & editing (supporting). Yong Sup Ihn: Conceptualization (supporting); Investigation (supporting); Methodology (supporting); Validation (supporting);
FIG. 7. Images obtained by QS-SPI with individual idler polarization. The error rates are given under the images with its standard deviations. (a) When there is no attack, all error rates are suppressed below 5%. (b) Under the attack, since Eve’s laser has $H'$-polarization, $H$-polarization error rate is below 5% but $V$-polarization error rate exceeds 95%. In the diagonal basis, $D$-polarization error rate is nearly 40%, and $A$-polarization error rate exceeds 60%.

Writing – review & editing (supporting). **Duk Y. Kim:** Funding acquisition (equal); Methodology (supporting); Project administration (supporting); Writing – review & editing (supporting). **Zaeill Kim:** Funding acquisition (equal); Methodology (supporting); Project administration (equal); Supervision (supporting); Writing – review & editing (supporting). **Yonggi Jo:** Conceptualization (lead); Data curation (supporting); Formal analysis (equal); Funding acquisition (supporting); Investigation (supporting); Methodology (lead); Project administration (equal); Supervision (lead); Validation (equal); Visualization (equal); Writing – original draft (supporting); Writing – review & editing (equal).

**DATA AVAILABILITY**

The datasets generated and/or analyzed during the current study are not publicly available due to the security policy of the Ministry of National Defense of South Korea but are available from the corresponding author upon reasonable request.
[18] G. M. Gibson, S. D. Johnson, and M. J. Padgett, Opt. Express 28, 28190-28208 (2020).
[19] V. Bužek and M. Hillery, Phys. Rev. A 54, 1844 (1996).
[20] D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. 81, 2598 (1998).
[21] A. I. Lvovsky, B. C. Sanders, and W. Tittel, Nat. Photon. 3, 706–714 (2009).
[22] E. Biham and T. Mor, Phys. Rev. Lett. 79, 4034 (1997).
[23] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007).
[24] T. Kim, M. Fiorentino, and N. C. Wong, Phys. Rev. A 73, 012316 (2006).
[25] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A 64, 052312 (2001).
[26] W. Pratt, J. Kane, and H. Andrews, Proc. IEEE 57, 58–68 (1969).
[27] S. P. Souza, J. Szumowski, C. L. Dumoulin, D. P. Plewes, and G. Glover, J. Comput. Assist. Tomogr. 12, 1026–1030 (1988).
[28] M. F. Duarte, M. A. Davenport, D. Takhar, J. N. Laska, T. Sun, K. F. Kelly, and R. G. Baraniuk, IEEE Signal Process. Mag. 25, 83–91 (2008).
[29] M.-J. Sun, L.-T. Meng, M. P. Edgar, M. J. Padgett, and N. Radwell, Sci. Rep. 7, 3464 (2017).
[30] J. S. Bell, Physics Physique Fizika 1, 195 (1964).
[31] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880–884 (1969).
[32] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, Phys. Rev. Lett. 84, 4733 (2000).
[33] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. 95, 010503 (2005).
[34] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. 97, 120405 (2006).
[35] D. Bruß, Phys. Rev. Lett. 81, 3018 (1998).
[36] A. Laing, V. Scarani, J. G. Rarity, and J. L. O’Brien, Phys. Rev. A 82, 012304 (2010).
[37] N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Phys. Rev. Lett. 88, 127902 (2002).
[38] Y. Jo and W. Son, Phys. Rev. A 94, 052316 (2016).
[39] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B. G. Englert, L. L. Sànchez-Soto, and E. Karimi, Quantum 2, 111 (2018).
[40] Y. Jo, H. S. Park, S.-W. Lee, and W. Son, Entropy 21, 80 (2019).
[41] X.-L. Wang, X.-D. Cai, Z.-E. Su, M.-C. Chen, D. Wu, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Nature 518, 516–519 (2015).
[42] J.-H. Kim, Y. Kim, D.-G. Im, C.-H. Lee, J.-W. Chae, G.Scarcelli, and Y.-H. Kim, Optica 8, 1524–1531 (2021).
[43] D. Kim, D. Lim, K. Park, and Y. S. Ihn, Curr. Appl. Phys. 41, 156–162 (2022).