Tamper-Indicating Quantum Seal*

Brian P. Williams,† Keith A. Britt, and Travis S. Humble

Quantum Computing Institute, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA
(Received 14 August 2015; revised manuscript received 15 October 2015; published 4 January 2016)

Technical means for identifying when tampering occurs is a critical part of many containment and surveillance technologies. Conventional fiber-optic seals provide methods for monitoring enclosed inventories, but they are vulnerable to spoofing attacks based on classical physics. We address these vulnerabilities with the development of a quantum seal that offers the ability to detect the intercept-resend attack using quantum integrity verification. Our approach represents an application of entanglement to provide guarantees in the authenticity of the seal state by verifying it is transmitted coherently. We implement these ideas using polarization-entangled photon pairs that are verified after passing through a fiber-optic-channel test bed. Using binary-detection theory, we find the probability of detecting inauthentic signals is greater than 0.9999 with a false-alarm chance of 10^{-9} for a 10-s sampling interval. In addition, we show how the Hong-Ou-Mandel effect concurrently provides a tight bound on redirection attack, in which tampering modifies the shape of the seal. Our measurements limit the tolerable path-length change to submillimeter disturbances. These tamper-indicating features of the quantum seal offer unprecedented security for unattended monitoring systems.

DOI: 10.1103/PhysRevApplied.5.014001

I. INTRODUCTION

Tamper-indicating optical seals are widely used for verifying the integrity of enclosed systems, including storage containers, physical perimeters, and fiber networks [1–4]. Fiber-optic seals have proven especially useful for actively surveying large areas or inventories due to the extended transmission range and flexible layout of fiber [5,6]. These seals operate as optical-continuity sensors that confirm transmission of an encoded light pulse from source to receiver with tampering indicated by either the absence of the light or an error in the received encoding.

In the classical setting, detection of tampering requires the failure of the intruder to accurately replicate the original transmission. This is typically accomplished with "secret" information that is hidden from the intruder, for example, the optical modulation sequence used to transmit pulses. This secret information, however, is vulnerable to discovery by the intruder using conventional signal-detection methods. Thus, in principle, an attacker is able to perfectly replicate the optical signal using *a priori* knowledge, and the classical variant of an optical seal is vulnerable to an intercept-resend spoofing attack. In this case, the intruder has the ability to recover information, such as the frequency, bandwidth, and modulation, that describes the classical state of the light. An exact duplicate of the transmitted signal can then be replicated by the attacker and injected into the fiber, thus, spoofing the downstream sensor.

By contrast, cloning quantum information is prohibited by the linearity of quantum mechanics [7,8]. Attempts to clone quantum information, even optimally, necessarily introduce noise into the resulting state and its subsequent observables [9]. These guarantees of the no-cloning theorem are well known from quantum key distribution (QKD), where nonlocal correlations inherent to quantum states are used to secure correlated measurement outcomes between users [10]. A QKD eavesdropper's attempt to clone transmitted quantum states introduces additional noise into the observed results that reveal her presence to the users [11–13]. In the context of QKD, added noise manifests as larger bit-error rates in the raw measurements, and theoretical considerations have set upper limits on the security of these systems.

We report how the no-cloning theorem can be applied to the development of tamper-indicating seals. In particular, we close the intercept-resend vulnerability for optical seals by using entangled quantum states to monitor signal continuity, and we demonstrate how the intercept-resend attack can be detected by monitoring the entanglement between a pair of transmitted photons. Because entanglement between the photon pair can be generated only at the authenticated transmitter, any attempt to spoof the receiver with a replicated photon is immediately detected. We formalize detection of tampering in terms of a statistical estimate of the entanglement and show how entanglement

†williamsbp@ornl.gov

distinguishes between an authentic seal state and a potential tampered seal. We implement these ideas using spectrally and polarization-entangled photon pairs as part of a quantum signal-detection system. Our results find a probability of detection for inauthentic signals greater than 0.999 99 at a false-alarm rate of one in ten for a 10-s sampling interval.

We also present tight bounds on an intruder's ability to spoof the seal using a second type of attack based on redirection of the signal path. The latter vulnerability arises when the intruder changes the path length of the optical signal, perhaps when rerouting around the intended enclosure. Conventional approaches to detect this attack rely on anomalies in the signal time of arrival, which is limited by the time-stamping electronics. We employ the Hong-Ou-Mandel effect between energy-degenerate entangled photons to detect submillimeter-path-length changes. Finally, we present a prototype implementation and experimental results that validate detection of these various tampering methods with estimations of the transmitted entanglement.

Entanglement has been proposed previously to offer an advantage for various forms of tamper detection. This includes our earlier efforts to demonstrate intrusion detection by monitoring the free-space optical transmission of entangled states as a kind of a quantum tripwire [14]. Those experiments used a sensing configuration in which the polarization entanglement between two photons transmitted to different measurement receivers was quantified. This system was subsequently improved with the development of nonlocal polarization interferometry, which offers greater sensitivity to the transmitted state while providing more efficient sampling [15]. Similar research for perimeter monitoring has applied the idea of interaction-free measurement to create an invisible quantum fence, in which the intruder is unable to detect the quantum signal state with very high probability [16]. There have also been previous uses of entanglement verification applied to remote sensing, where the quantum statistics of a reflected signal are used to authenticate the results of an imaging system [17].

The paper is organized as follows. In Sec. II, we present our model for the quantum seal, and we formalize the problem of tamper detection using binary-detection theory. In Sec. III, we detail the experimental implementation of the seal including the entangled photon-pair source, entanglement detection, and Hong-Ou-Mandel interference measurements. Additionally, the results of our experimental studies to characterize seal performance in term of observed entanglement statistics and acquisition times are given in this section. We conclude our presentation in Sec. IV.

II. THEORETICAL MODEL

A schematic diagram of a quantum-seal prototype is presented in Fig. 1. It consists of a secure enclave that generates and detects a quantum signal state and an unsecure area that corresponds with the system to be monitored. The quantum signal state is a pair of photons prepared in a polarization-entangled Bell state by cw pumping of type-II spontaneous parametric downconversion (SPDC). These photons are coupled into active and reference fibers, where the active fiber traverses the unsecure area, and the reference fiber remains inside the secure enclave.

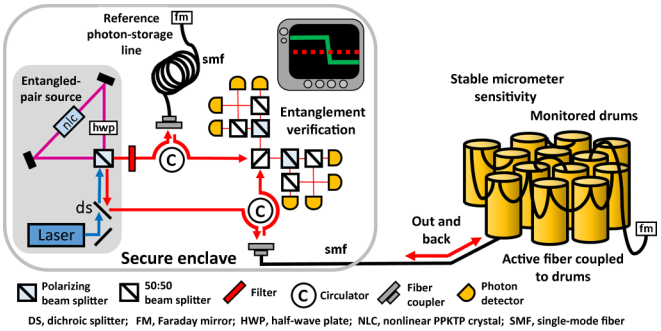

FIG. 1. A schematic of a tamper-indicating quantum-optical seal showing four major components: (a) an entangled-photon source, (b) reference and active fiber-optic links, (c) an entanglement-verification measurement, and (d) a monitoring system that process time-stamped single-photon detections.

The footprint of the active fiber is configured to monitor access to an enclosure, for example, the inventory of closed containers shown in Fig. 1. The reference fiber is colocated with the transmitter and effectively represents a photon-storage loop. Both fibers terminate at a Faraday mirror that reflects the photons and corrects for any polarization scrambling prior to the return trip. After reflection, each photon is routed by a circulator to one of the input ports of the BSA shown in Fig. 2. The photons are subsequently detected, and the resulting information-output port and polarization enables partial discrimination of the Bell states and entanglement detection.

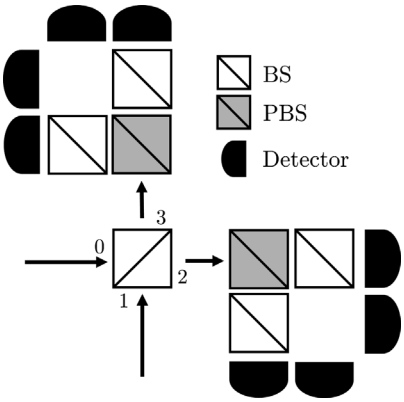

FIG. 2. A Bell-state analyzer (BSA) consists of two modes labeled 0 and 1 input to a symmetric beam splitter, whose output modes 2 and 3 direct to a pair of polarization analyzers and single-photon detectors. A beam splitter after the polarization analyzer allow probabilistic detection of each coincidence type.

A. Entanglement detection

The BSA shown in Fig. 2 supports partial discrimination between the polarization-encoded Bell states [18,19],

$$|\Psi^{\pm}\rangle = (|H_0V_1\rangle \pm |V_0H_1\rangle)/\sqrt{2},$$
$$|\Phi^{\pm}\rangle = (|H_0H_1\rangle \pm |V_0V_1\rangle)/\sqrt{2},$$

where H_i and V_i label horizontally and vertically polarized photons in spatial mode i. The states Ψ^+ and Ψ^- have distinct detection signatures that allow deterministic identification, whereas the $\Phi^{\pm}$ states are not distinguishable amongst themselves but are distinguishable from $\Psi^{\pm}$ [20]. Moreover, consider an arbitrary two-photon pure state

$$|\theta\rangle = a|H_0,H_1\rangle + b|H_0,V_1\rangle + c|V_0,H_1\rangle + d|V_0,V_1\rangle$$
$$= (a\hat{h}_0^{\dagger}\hat{h}_1^{\dagger} + b\hat{h}_0^{\dagger}\hat{v}_1^{\dagger} + c\hat{v}_0^{\dagger}\hat{h}_1^{\dagger} + d\hat{v}_0^{\dagger}\hat{v}_1^{\dagger})|0\rangle, \quad (1)$$

where the photons are temporally indistinguishable, operator $\hat{q}_i^{\dagger}\hat{r}_s^{\dagger}$ creates $q,\ r \in \{h,v\}$ polarization photons in spatial modes $i,\ s \in \{0,1,2,3\}$, $(1+\delta_{qr}\delta_{is})^{-1/2}\hat{q}_i^{\dagger}\hat{r}_s^{\dagger}|0\rangle = |Q_iR_s\rangle$, and $[\hat{q}_i,\hat{r}_s^{\dagger}] = \delta_{qr}\delta_{is}$ holds. We calculate the expected detection signature for this state in the BSA by defining the operator transforms under the symmetric beam splitter as [23,24]

$$\hat{h}_0^{\dagger} \overset{\text{BS}}{\to} (\hat{h}_2^{\dagger} + i\hat{h}_3^{\dagger})/\sqrt{2}, \qquad \hat{h}_1^{\dagger} \overset{\text{BS}}{\to} (i\hat{h}_2^{\dagger} + \hat{h}_3^{\dagger})/\sqrt{2}, \quad (2)$$

$$\hat{v}_0^{\dagger} \overset{\text{BS}}{\to} (\hat{v}_2^{\dagger} - i\hat{v}_3^{\dagger})/\sqrt{2}, \qquad \hat{v}_1^{\dagger} \overset{\text{BS}}{\to} (-i\hat{v}_2^{\dagger} + \hat{v}_3^{\dagger})/\sqrt{2}, \quad (3)$$

where $h_0^{\dagger}$ is the creation operator for $|H_0\rangle$, etc. The corresponding post-beam-splitter state is

$$|\theta'\rangle = (1/2)[ia(\hat{h}_2^{\dagger 2} + \hat{h}_3^{\dagger 2}) - id(\hat{v}_2^{\dagger 2} + \hat{v}_3^{\dagger 2}) + i(b-c)\hat{h}_2^{\dagger}\hat{v}_2^{\dagger}$$
$$- i(b-c)\hat{h}_3^{\dagger}\hat{v}_3^{\dagger} + (b+c)\hat{h}_2^{\dagger}\hat{v}_3^{\dagger} + (b+c)\hat{v}_2^{\dagger}\hat{h}_3^{\dagger}]|0\rangle, \quad (4)$$

and the complete set of detection probabilities is

$$P_{h_2h_2} = P_{h_3h_3} = |a|^2/2, \quad (5)$$

$$P_{v_2v_2} = P_{v_3v_3} = |d|^2/2, \quad (6)$$

$$P_{h_2v_3} = P_{h_3v_2} = [|b|^2 + |c|^2 + (b^*c + bc^*)]/4, \quad (7)$$

$$P_{h_2v_2} = P_{h_3v_3} = [|b|^2 + |c|^2 - (b^*c + bc^*)]/4. \quad (8)$$

As required, the sum over all probabilities is unity. Coincidence probabilities involving different polarizations are related to the overlap of the input state in Eq. (1) with $\Psi^{\pm}$, i.e.,

$$P_{h_2v_3} + P_{h_3v_2} = |\langle\theta|\Psi^+\rangle|^2, \quad (9)$$

$$P_{h_2v_2} + P_{h_3v_3} = |\langle\theta|\Psi^-\rangle|^2. \quad (10)$$

We use the observed BSA detection statistics to distinguish the Bell state prepared by the secure enclave from any other possible signal state. We define the polarization-correlation parameter

$$\mathcal{E} \equiv P_{h_2v_3} + P_{h_3v_2} - P_{h_2v_2} - P_{h_3v_3}, \quad (11)$$

which is positive (negative) when orthogonal polarizations at different (same) ports are most probable. For the monochromatic pure state of Eq. (1),

$$\mathcal{E} = b^*c + bc^*. \quad (12)$$

The utility of $\mathcal{E}$ is that it places tight lower bounds on the strength of the correlations expected from the received states. For example, consider the separable state

$$|\theta_s\rangle = (\cos\alpha\hat{h}_0^{\dagger} + e^{iA}\sin\alpha\hat{v}_0^{\dagger})(\cos\beta\hat{h}_1^{\dagger} + e^{iB}\sin\beta\hat{v}_1^{\dagger})|0\rangle \quad (13)$$

for which

$$a = \cos\alpha\cos\beta, \qquad b = e^{iB}\cos\alpha\sin\beta, \quad (14)$$

$$c = e^{iA}\sin\alpha\cos\beta, \qquad d = e^{i(A+B)}\sin\alpha\sin\beta \quad (15)$$

in Eq. (1) with phases $\alpha,\ \beta,\ A,\ B \in [0,2\pi]$. This restricted state leads to the correlation parameter

$$\mathcal{E}_s = \sin 2\alpha \sin 2\beta \cos(A-B)/2 \quad (16)$$

that is strictly bounded as

$$-1/2 \le \mathcal{E}_s \le 1/2. \quad (17)$$

More generally, any separable mixture

$$\rho_s = \sum_k w_k |\theta_s^k\rangle\langle\theta_s^k|$$

with $w_k \ge 0$ and $|\theta_k>$ the kth pure state also satisfies this bound, since

$$\left|\sum_k w_k \mathcal{E}_s^k\right| \le \sum_k w_k/2 = 1/2. \quad (18)$$

By comparison, the entangled states Ψ^+ and Ψ^- have $\mathcal{E} = 1$ and $\mathcal{E} = -1$, respectively, while the cross-correlation parameter vanishes for the $\Phi^{(\pm)}$ states. Thus, $\mathcal{E} > 1/2$ indicates an entangled state, but $\mathcal{E}$ is not an entanglement metric. The sharp distinction in the parameter $\mathcal{E}$ permits us to classify an arbitrary input state as either Ψ-like entangled or not.

The analysis above neglects the finite temporal duration of each single-photon wave packet in favor of a simplified monochromatic representation of the polarized states. In order to accurately model the time of arrival for each

photon, we represent the Bell state generated by the source as a multimode entangled photon pair

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\int d\omega \int d\omega' f(\omega,\omega') \times [\hat{h}_0^\dagger(\omega)\hat{v}_1^\dagger(\omega') + \hat{v}_0^\dagger(\omega)\hat{h}_1^\dagger(\omega')]|0\rangle, \quad (19)$$

where $f(\omega,\omega')$ is the joint spectral amplitude of the photon pair, and $\hat{j}_i^\dagger(\omega)$ creates a single $j \in \{h,v\}$ polarization photon in spatial mode $i \in \{0,1,2,3\}$ with frequency ω. For these continuous operators, the commutation relation is

$$[\hat{j}_i(\omega), \hat{\ell}_s^\dagger(\omega')] = \delta_{j\ell}\delta_{is}\delta(\omega-\omega'). \quad (20)$$

The symmetric beam-splitter relations are the same as in the single-frequency case, Eqs. (2) and (3), and instead of the state given in Eq. (4), we have the post-beam-splitter state

$$\begin{aligned}|\theta_{\Psi^+}\rangle = \frac{1}{2\sqrt{2}}\int d\omega \int d\omega' f(\omega,\omega') e^{i\omega' t_d} \\ \times (-i[\hat{h}_2^\dagger(\omega)\hat{v}_2^\dagger(\omega') - \hat{v}_2^\dagger(\omega)\hat{h}_2^\dagger(\omega')] \\ - i[\hat{v}_3^\dagger(\omega)\hat{h}_3^\dagger(\omega') - \hat{h}_3^\dagger(\omega)\hat{v}_3^\dagger(\omega')] \\ + [\hat{h}_2^\dagger(\omega)\hat{v}_3^\dagger(\omega') + \hat{h}_2^\dagger(\omega')\hat{v}_3^\dagger(\omega)] \\ + [\hat{v}_2^\dagger(\omega')\hat{h}_3^\dagger(\omega) + \hat{v}_2^\dagger(\omega)\hat{h}_3^\dagger(\omega')])|0\rangle,\end{aligned}$$

where t_d is the potential delay between the reference and active-photon arrival times. This delay arises when the path length of the active photon is shortened ($t_d < 0$) or lengthened ($t_d > 0$). The multimode detection probabilities are now given as

$$P_{j_i\ell_s} = \int_T d\tau |\langle 0|\hat{j}_i(t)\hat{\ell}_s(t+\tau)|\Psi^{+'}\rangle|^2, \quad (21)$$

where

$$\hat{j_i(t)} = \frac{1}{\sqrt{2\pi}}\int d\omega \hat{j}_i(\omega)e^{-i\omega t}. \quad (22)$$

The joint spectral amplitude for a cw-pumped type-II SPDC source is modeled as

$$f(\omega,\omega') = \delta(\omega+\omega'-\omega_p)\mathrm{sinc}(\Delta kL/2), \quad (23)$$

where the longitudinal wave-vector mismatch Δk depends on the group velocity for the ordinary and extraordinary optical axes [25,26]. In this regime, the detection probabilities become

$$P_{h_2v_2} = P_{h_3v_3} = \frac{1}{4}[1- \wedge (2t_d/\Delta t)], \quad (24)$$

$$P_{h_2v_3} = P_{v_2h_3} = \frac{1}{4}[1+ \wedge (2t_d/\Delta t)], \quad (25)$$

where Δt is the propagation delay between ordinary and extraordinary photons traveling the full length of the nonlinear crystal [26],

$$\wedge(x) = \begin{cases} 1-|x| & \text{if } |x| \le 1, \\ 0 & \text{otherwise.}\end{cases} \quad (26)$$

These results converge to the monochromatic case when the delay $t_d = 0$, whereas if tampering delays the photon in the active fiber but preserves the polarization entanglement, then the delay adds temporal distinguishability to the photons. For the multimode case with maximal polarization entanglement and temporal distinguishability, the cross-correlation parameter behaves as

$$\mathcal{E}_{\mathrm{PE}} = \wedge(2t_d/\Delta t). \quad (27)$$

Therefore, delays greater than a fraction of Δt are detected even if the polarization entanglement is preserved. For our optical implementation, $\Delta t \approx 8$ ps and a one-way path-length difference greater than 300 μm results in $|\mathcal{E}| \le 1/2$. As one might expect, it can be shown that an arbitrary polarization multimode pure state has a correlation dependent on both the degree of polarization entanglement and temporal distinguishability,

$$\mathcal{E}_{\mathrm{MM}} = \wedge(2t_d/\Delta t)(bc^* + b^*c). \quad (28)$$

For $t_d/\Delta t \ll 1$, we recover the monochromatic result presented in Eq. (12). The entanglement dependency removes the possibility that the state may be spoofed, while the temporal sensitivity limits the adversary's ability to attack by redirection. In Fig. 3, the temporal and phase space of the parameter $\mathcal{E}$ is represented graphically.

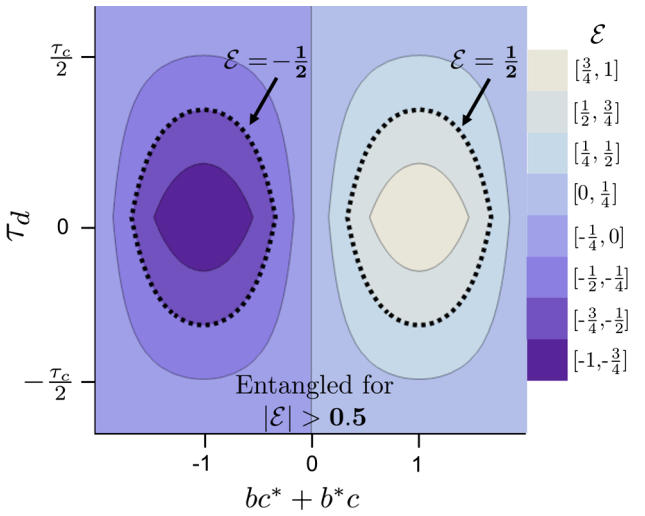

FIG. 3. A contour plot of the entanglement parameter $\mathcal{E}$ presented in Eq. (28) with respect to the pure-state coefficients $bc^* + b^*c$ and time delay t_d. The parameter $\mathcal{E}$ has extremal values when the input state is maximally polarized, and there is no relative delay between the photons.

B. Entanglement-parameter estimation

We detect entanglement by estimating $\mathcal{E}$ from the correlated polarizations measured by the BSA. Because of the symmetry of the BSA, the coincident probabilities in Eqs. (5)–(8) satisfy

$$P_{h_2h_3} = P_{v_2v_3} = p_{sd}/2, \tag{29}$$

$$P_{h_2h_2} = P_{h_3h_3} = P_{v_2v_2} = P_{v_3v_3} = p_{ss}/4, \tag{30}$$

$$P_{h_2v_2} = P_{h_3v_3} = p_{ds}/2, \tag{31}$$

$$P_{h_2v_3} = P_{v_2h_3} = p_{dd}/2, \tag{32}$$

where subscripts s and d denote detections as being same or different, respectively, in the polarization and output mode. We estimate $\mathcal{E}$ from these four parameters.

We estimate the set of coincident probabilities $\mathcal{P} = \{p_{sd}, p_{ss}, p_{ds}, p_{dd}\}$ from the experimentally observed coincidence counts $c_{ij} \forall i, j \in \{s, d\}$. However, the relative frequency of these measured rates does not directly correspond to the probabilities due to several technical limits. First, the SPDC source described in Sec. III is known to result in registering accidental coincidences between photons from different entangled pairs and to a lesser degree photon–dark count coincidences. These so-called "accidentals" are rare but add a contribution c_{acc} to the observed coincidences. Second, the efficiencies for each joint two-photon pathway are typically different. Our first correction removes contributions from accidental coincidences and eliminates joint efficiency asymmetries with the formula

$$c_i' = \frac{\eta_{\min}}{\eta_i}(c_i - c_{\text{acc}}), \tag{33}$$

where $i \in \{h_2h_3, v_2v_3, h_2h_2, v_2v_2, h_2v_2, h_3v_3, h_2v_3, v_2h_3\}$, c_i is the raw coincidence count, $\eta_i \in [0, 1]$ is the joint pathway efficiency for coincidence i, and $\eta_{\min}$ is the least of these joint pathway efficiencies. Since $\eta_{\min}/\eta_i \leq 1$, normalization typically increases the uncertainty in the entanglement estimate. We sum all coincidences that belong to the same coincidence type, ss, sd, ds, or dd,

$$k_{sd} = c'_{h_2h_3} + c'_{v_2v_3}, \tag{34}$$

$$k_{ss} = c'_{h_2h_2} + c'_{v_2v_2}, \tag{35}$$

$$k_{ds} = c'_{h_2v_2} + c'_{h_3v_3}, \tag{36}$$

$$k_{dd} = c'_{h_2v_3} + c'_{h_3v_2} \tag{37}$$

to obtain coincidence type totals $\kappa = \{k_{sd}, k_{ss}, k_{ds}, k_{dd}\}$.

The last technicality is that our experimental prototype monitors statistics in only one arm of the BSA, which reduces the number of observed same-port same-polarization coincidences by a factor of 0.5 relative to the expected value. Comparing Eqs. (30) and (35), we see that monitoring only one port for same-port same-polarization coincidences results in the absence of corrected counts $c_{h_3h_3}$ and $c_{v_3v_3}$ from Eq. (35). Additionally, we use nonphoton number-resolving detectors, which reduces the recorded number of events by an additional factor of 0.5 for these same-port same-polarization events. The joint efficiencies given above are determined relative to the actual number of photons in a given pathway. Thus, the joint efficiencies given above do not account for the losses relevant to same-port same-polarization coincidence events. In principle, we can determine joint efficiencies that will account for these events, but it will greatly increase the uncertainty in our parameter. Instead, we maximize the certainty of our parameter estimation by including these known losses directly into the model. This is done by averaging over all possible values of the true number of same-port same-polarization events n_{ss}. The resulting probability distribution for $\mathcal{P}$ given normalized-coincidence-type totals κ is

$$P(\mathcal{P}|\kappa) = \frac{p_{sd}^{k_{sd}} p_{ds}^{k_{ds}} p_{dd}^{k_{dd}} \sum_{n_{ss}=k_{ss}}^{\infty} \binom{n_{ss}}{k_{ss}} \left(\frac{p_{ss}}{4}\right)^{n_{ss}}}{P(\kappa)}. \tag{38}$$

$P(\kappa)$ is the numerator integrated over all possible values of coincident probabilities p_{sd}, p_{ss}, p_{ds}, and p_{dd}.

Given the set of normalized coincidences totals κ, we estimate $\mathcal{E}$ as the mean

$$\mathcal{E}_\kappa = \int P(\mathcal{P}|\kappa)(p_{dd} - p_{ds}) d\mathcal{P}, \tag{39}$$

which yields

$$\mathcal{E}_\kappa = \frac{(k_{dd} - k_{ds})_2\tilde{F}_1(1 + k_{ss}, 1 + k_{ss}; 5 + n; \frac{1}{4})}{{}_2\tilde{F}_1(1 + k_{ss}, 1 + k_{ss}; 4 + n; \frac{1}{4})}, \tag{40}$$

where $n = k_{sd} + k_{ss} + k_{ds} + k_{dd}$, and ${}_2\tilde{F}_1(a; b; c)$ is the regularized hypergeometric function. We similarly calculate $(\mathcal{E}^2)_\kappa$ to derive the variance $\sigma_\kappa^2 = (\mathcal{E}^2)_\kappa - (\mathcal{E}_\kappa)^2$ in the estimate.

C. Tamper detection

Under normal operation, the quantum seal transmits polarization-entangled states through the active and reference fibers, and the BSA measurements yield an estimate for the entanglement parameter $\mathcal{E}$. When the estimate $\mathcal{E}_\kappa$ exceeds the bound of $1/2$, then the seal confirms that the received photon pairs are entangled. This use of quantum integrity verification certifies that the seal is unmolested. Moreover, the presence of entanglement is doubly indicative, as it confirms that the photon injected into the active fiber is both the same photon retrieved from the active fiber

and that the path-length difference between the reference and active fiber links is much smaller than the single-photon coherence length.

By contrast, quantum integrity verification fails when the estimate $\mathcal{E}_\kappa$ lies below the threshold value of $1/2$. This occurs in the presence of tampering due to either a temporal shift in the photon time of arrival or a loss of entanglement between the photons from the intercept-resend attack. However, verification may also fail because of technical noise during transmission and measurement, e.g., decoherence of the entangled state. Therefore, it is necessary to quantify the probability to accurately detect tampering as well as the rate at which detection fails.

We formalize the tamper detection problem as a binary decision in which the estimate of $\mathcal{E}$ decides between two possible hypotheses [27]. Under the positive hypothesis H_1, tampering is indicated when the entanglement estimate $\mathcal{E}_k$ is below a detection threshold defined as ϵ. Under the null hypothesis H_0, the transmitted entanglement is preserved, and the estimate exceeds the threshold ϵ. We gain greater confidence in our decision by choosing $\epsilon > 1/2$ but at the expense of a higher probability of a false-alarm rate, i.e., classifying entangled states as being inauthentic.

We characterize normal operation of the seal by an average entanglement parameter $\mathcal{E}_1$ and its corresponding variance σ^2. The nominal value $\mathcal{E}_1$ characterizes the amount of entanglement expected from the system in the absence of tampering. This value also characterizes the quality of the transmission and includes effects due to environmental decoherence. We also define the expectation value in the presence of tampering as $|\mathcal{E}_0| \leq 1/2$, which follows from the known theoretical limitations of the entanglement parameter, and we assume that the variance is the same as under normal operation, σ_κ. Given an estimate $\mathcal{E}_\kappa$, our task is to decide whether tampering has occurred

$$H_0\colon\ \mathcal{E}_\kappa = \mathcal{E}_0 + e \leq \epsilon \tag{41}$$

or not

$$H_1\colon\ \mathcal{E}_\kappa = \mathcal{E}_1 + e > \epsilon. \tag{42}$$

In both hypotheses, e represents a zero-mean Gaussian random variable with average variance σ_κ^2, while the detection threshold ϵ will depend on the implementation. For example, the threshold value should be chosen to limit the number of false alarms as well as to limit the possibility of successful spoofing. The probability distribution for $\mathcal{E}_\kappa$ under each hypothesis is closely approximated by the Gaussian

$$P(\mathcal{E}_\kappa|\mathcal{E}_i,\sigma_\kappa) \approx \frac{1}{\sqrt{2\pi\sigma_\kappa^2}} \exp\left[-\frac{(\mathcal{E}_\kappa - \mathcal{E}_i)^2}{2\sigma_\kappa^2}\right], \tag{43}$$

where $i \in \{0,1\}$.

The discrimination of two constant signals in the presence of Gaussian noise is a well-known problem in binary-detection theory [27]. The probability to detect tampering is given as

$$P_D = \frac{1}{2}\mathrm{erfc}\left(\frac{\mathcal{E}_0 - \epsilon}{\sqrt{2}\sigma_\kappa}\right), \tag{44}$$

where

$$\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-z^2} dz \tag{45}$$

is the complementary error function. The corresponding probability for spoofing is

$$P_S = 1 - P_D, \tag{46}$$

while the probability of a false alarm in which an authentic signal is misidentified as spoofed, is

$$P_{\mathrm{FAR}} = \frac{1}{2}\mathrm{erfc}\left(\frac{\mathcal{E}_1 - \epsilon}{\sqrt{2}\sigma_\kappa}\right). \tag{47}$$

The probability of detection and false alarm characterize operation of the seal for a given threshold ϵ, and the parametric dependence of P_D and P_{FAR} are presented by the receiver operating characteristic curve in Fig. 4. Therefore, the operation of the seal can be tuned by selecting a detection threshold ϵ that provides a desired probability of detection or false-alarm rate.

It is apparent from Fig. 4 that tampering can be detected with very high probability when the normal operating value

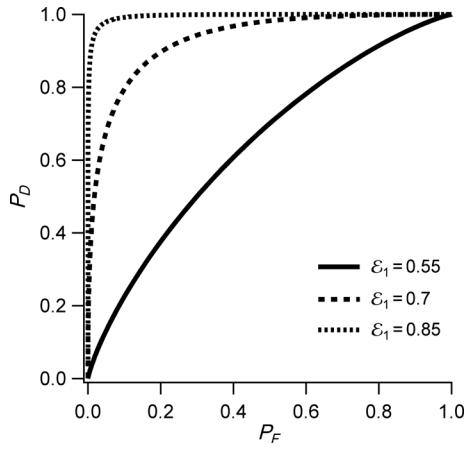

FIG. 4. The receiver operating characteristic curves display a parametric plot of the probability of detection P_D versus the false-alarm rate P_{FAR}. Assuming that tampering yields $\mathcal{E}_0 = 1/2$ with uncertainty $\sigma = 0.1$, we plot the behavior for baseline entanglement values of $\mathcal{E}_1 = 0.55$, 0.7, and 0.85. Our experimental prototype exhibits much smaller uncertainty and higher baseline entanglement.

$\mathcal{E}_1$ is close to the theoretical maximum of ± 1. This detectability is due to the sharp transition separating authentic and spoofed signal as represented by the bounds in Eq. (17), which may be violated by many orders of standard deviation when transmitting the $\Psi^{\pm}$ entangled state. Note that it is also possible that during the time T required to estimate $\mathcal{E}$ that an intruder may inject an unentangled state for some duration $t < T$. The presence of the injected state prepares a mixture of actual and spoofed states with the entanglement estimated as

$$\mathcal{E}(t,T) = \frac{t}{T}\mathcal{E}_0 + \frac{(T-t)}{T}\mathcal{E}_1. \tag{48}$$

Intrusions are indicated when $\mathcal{E}(t,T) < \epsilon$, i.e., for

$$t > \frac{(\mathcal{E}_1 - \epsilon)}{(\mathcal{E}_1 - \mathcal{E}_0)}T.$$

Since $\mathcal{E}_0$ may be at most $1/2$ and $\mathcal{E}_1$ is a constant of the system, the duration for this short-time spoofing decreases linearly with the threshold ϵ. Moreover, the probability of detection increases nonlinearly with ϵ, as seen in Eq. (45), and short-time attacks can be detected with high probability at a relatively low false-alarm rate using only moderate increases in the detection threshold. Short-time attacks may also be mitigated by decreasing the duration T used for estimating the entanglement.

While entanglement excludes spoofing the measurement apparatus with a cloned state, a savvy adversary may attempt to redirect the active photon away from the tamper seal in order to access the surveyed area. The estimated entanglement in this scenario behaves normally when the optical path length of the redirected photon is exactly matched. We address this vulnerability in our implementation by making the entanglement estimate sensitive to submillimeter disturbances in the expected path length. Such tolerances can be adjusted to fit application-specific requirements, for example, by broadening the spectral bandwidth of the photon states emitted from the source. This temporal shaping retains the entanglement required for tamper detection and increases the sensitivity to the redirection attack.

Depending on the length of the optical fiber used and the location of deployment, variations in the ambient temperature may alter the active and reference fiber path lengths. Fibers exposed to different ambient conditions may experience a change in path length ΔL (m) that is proportional to the initial fiber length L_0 (m) and temperature change ΔT (°C),

$$\Delta L = \frac{\alpha L_0}{m°\mathrm{C}}\Delta T, \tag{49}$$

with the thermal expansion coefficient $\alpha = 10^{-6}$ being a high estimate [28]. Consider the example of $L_0 = 1$ km for each of the active and reference fibers and a temperature differential $\Delta T = \pm 10\,°\mathrm{C}$. This temperature change produces a round-trip path-length change of $\Delta L = \pm 20$ mm. This change is large enough to distinguish the active and reference photons temporally, while also small enough to be compensated by simple adjustments to the reference path length. For example, a free-space coupler mounted on a translatable stage can be used to regulate the path length alongside environmental monitoring.

The expected changes in path length due to time of day and weather patterns are relatively slow and very distinct from the sudden unexpected changes in path length that result from tampering. The quantum seal is sensitive to effects on the time scale T, and this includes sudden changes in environmental conditions such as pressure on the fiber or a rapid rise in temperature. The seal does not discriminate between intentional and unintentional acts that modify decoherence in the transmission channel. However, our theoretical account of stochastic fluctuations on the estimate demonstrate that the probability of detection remains high even for a moderate value of σ_κ; cf. Eq. (44).

We also examine the attack in which an intruder replaces the active link with an exact replica. This replacement attack may be technically challenging, but it is, nonetheless, physically possible. Implementing the attack requires first characterizing the active fiber link, then severing the original transmission channel and joining the replica fiber to both the transmitter and receiver, and finally coupling the photon into the replica link. These steps are easily detectable as they modify the physical properties of the fiber and break the continuity of transmission. Alternatively, the seal system can be depowered so that optical continuity is broken at the source. A blackout event again indicates tampering, and when power returns to the system, a system calibration procedure that includes checking the fiber installation reveals evidence of the replacement attack.

III. EXPERIMENTAL IMPLEMENTATION

In this section, we detail the experimental implementation of the quantum seal modeled in Sec. II and Fig. 1. A schematic of the experimental layout is shown in Fig. 5, in which the entangled light source is based on cw pumping of type-II SPDC in a nonlinear optical PPKTP (periodically polled potassium titanyl phosphate) crystal within a Sagnac loop. This configuration generates a polarization-entangled-pair state Ψ^+ [29]. The narrow-band pump laser operates at 405 nm and a power of approximately 1 mW. At this power, the source generates approximately 1.2×10^6 photon pairs per second. The nonlinear PPKTP crystal is 30 mm in length and phase matched to produce near-degenerate-energy collinear photon pairs with orthogonal polarizations. These photons have a central wavelength centered at 810 nm with a 0.5-nm bandwidth.

The entangled light source transmits each photon of the entangled pair to separate polarization-phase-maintaining

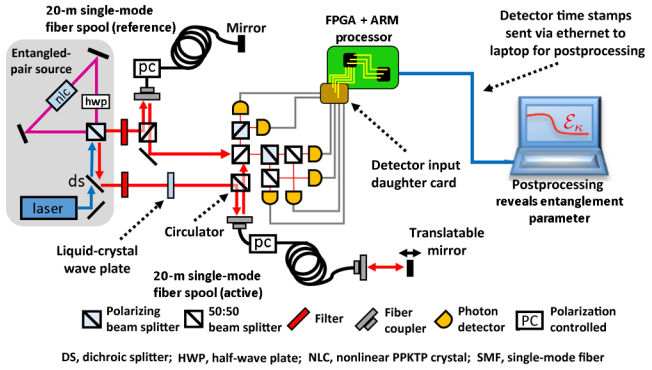

FIG. 5. The experimental schematic for our prototype tamper-indicating quantum seal showing its four major components: (a) a polarization-entangled photon source, (b) 20-m single-mode fiber-optic channels for the reference and active links, (c) polarization-entanglement verification based on a Bell-state analyzer, and (d) time-stamping electronics integrated with a processor to transmit observed coincidences to a host computer for parameter estimation.

circulators. For convenience, we use lossy, but easily configured, symmetric beam splitters as circulators. As opposed to more elaborate setups, this reduces the overall photon-pair collection efficiency by 90% and represents the dominant loss mechanism. Whereas this setup is sufficient for our proof-of-principle demonstration, future tamper seals will benefit from using more efficient dual polarization-phase-preserving optical circulators. Following the circulators, one photon is output to the active fiber, while the other is routed to the reference fiber. We use 20-m single-mode fibers for both the active and reference links with polarization controllers to correct for polarization rotation that occurs during the fiber round trip. Polarization entanglement is reduced or lost completely without this correction. We include an optical delay stage at the terminal of the active fiber in order to implement redirection attacks.

Once the active and reference photons complete the round trip through the respective fibers, they are routed to a Bell-state analyzer consisting of symmetric beam splitters, polarization beam splitters, and single-photon detectors. Our BSA is modeled after the design shown in Fig. 2, but we do not monitor the full set of possible coincidences. This is due to the symmetry expected for the detection probabilities given by Eqs. (5)–(8). This inobservance comes at the expense of a reduced data-set size and correspondingly greater uncertainty in the parameter estimate but reduces the number of single-photon detectors needed. We use Perkin-Elmer (now Excelitas) SPCM devices which have an efficiency of 0.4 at a photon wavelength of 810 nm. Because of pathway efficiencies ranging from $5\text{–}6 \times 10^{-3}$, we observe single-photon counts/s in the range of $2\text{–}6 \times 10^{3}$ counts/s and average coincidence rates in the range of 0–15 counts/s.

We measure the photon time of arrival by monitoring the output signal from the detector array. Photon detection triggers a detector to output a 25-ns transistor-transistor logic (TTL) pulse that is then time stamped and logged according to a detector identifier. We implement time stamping by sending the TTL pulses to a FPGA (field-programmable gate array) configured with a custom daughter card that connects up to eight coaxial cables to input pins. We reported previously on the use of FPGAs for performing single-photon detection, in which we time stamp each TTL pulse against the FPGA clock and store the resulting data alongside the input channel identifier [30]. In the current implementation, we use a ZedBoard system on a chip composed from a FPGA and Acorn RISC Machine (ARM) processor [31]. We operate the FPGA using a 10-ns clock cycle for the detection system. Stored time-stamp data are then aggregated and packetized by custom software running on the ARM processor within the Xillinux operating system [32]. These packets are then transmitted over ethernet using the user datagram protocol to a host computer where the entanglement parameter is estimated [33].

We experimentally detect tampering by estimating $\mathcal{E}$ using the prototype quantum seal. The results are shown in Fig. 6, where the dependence of $\mathcal{E}_\kappa$ is plotted against tuning of the entanglement in the input state and the relative difference between the active and reference paths. These

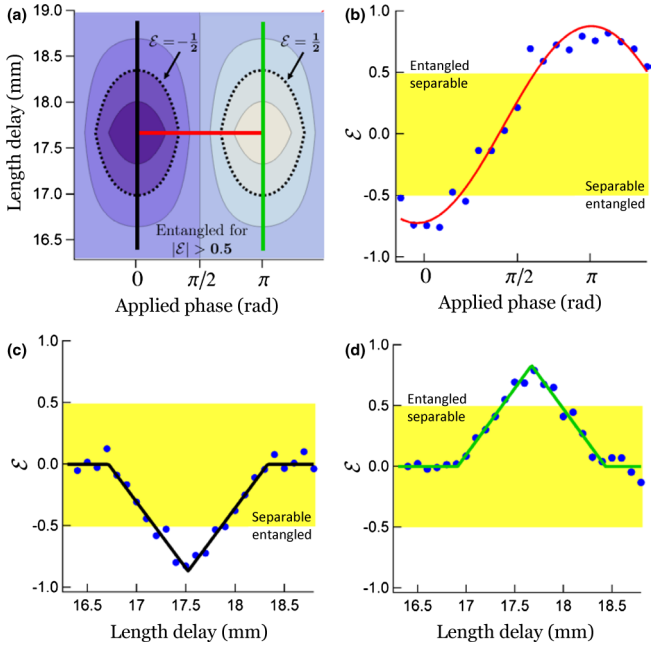

FIG. 6. (a) This contour plots the theoretical value of parameter $\mathcal{E}$ versus phase and path-length delay (mm). Red, black, and green dotted lines indicate the range over which the experimental data in plots (b)–(d) are taken. (b) Experimental values for $\mathcal{E}$ as the phase of the polarization-entangled state is modulated with a liquid-crystal wave plate. At 0 and π phase, the Ψ^- and Ψ^+ states are obtained, respectively. (c) Experimental values for $\mathcal{E}$ in the state Ψ^- as the active photon's path length is increased. (d) Experimental values for $\mathcal{E}$ in state Ψ^+ as the active photon's path length is increased.

plots correspond to modifying the delay and phase parameters of Eq. (28). Assuming the source generates the Ψ^+ Bell state, the entanglement parameter is

$$\mathcal{E} = \wedge\,(2t_d/\tau_c)\cos(\phi+\pi), \tag{50}$$

which clearly depends on the optical delay t_d and the relative phase ϕ. Settings of $\phi = 0$ and $\phi = \pi$ correspond to the Bell states Ψ^- and Ψ^+, respectively. By adjusting the phase ϕ, we tune the state that returns to the detector from being authentic to inauthentic. This tuning was accomplished experimentally by modulating, changing the applied voltage, a liquid-crystal wave plate in the active photon path as seen in Fig. 5. The temporal delay t_d is adjusted by translating the reflection mirror at the end of the active fiber.

The experimentally estimated entanglement parameter is shown in Fig. 6, where a maximum value of $|\mathcal{E}_\kappa| \approx 0.8$ is obtained. This statistically significant estimate is well above the separable bound of 0.5 and a clear signature of entanglement as nominal behavior. Figure 6(b) shows how the estimate varies as the phase of the prepared state is varied, and the detected state is rotated from Ψ^+ to Ψ^-. In addition, Figs. 6(c) and 6(d) show how submillimeter-path-length delays lead to decreases in the estimated entanglement.

For the system demonstrated here, each entanglement estimate $\mathcal{E}_\kappa$ is calculated from coincidences collected during a 10-s sampling window interval. For this sampling interval, we observe combined raw coincident counts of $c_i \in \{0, 400\}$ with corresponding standard deviation $\sigma_\kappa = 0.03$–0.04. Using these experimentally measured parameters, the detection theory presented in Sec. II yields greater than 0.9999 probability of detecting inauthentic signals with a false-alarm chance of 10^{-9} when using a 10-s sampling interval. Longer sampling windows lead to even lower false-alarm rates.

Several factors contribute to reduction in the entanglement estimate from a maximal value of 1. Foremost is the imperfect correction offered by the polarization controllers, which are subject to drift during acquisition time. The use of Faraday rotators at the fiber terminals can provide better correction for this type of system noise. Interfaces between the optical fibers and free-space optics also degrade the entanglement with unwanted reflections causing photon pairs to become temporally distinguishable and polarization uncorrected. These degradations resulted in unwanted coincidence events that do not participate in Hong-Ou-Mandel interference. Future improvements to the seal design should make use of more stable Faraday mirrors to overcome the need to correct the polarization, and angled optical-fiber connectors to eliminate the unwanted reflections.

IV. CONCLUSIONS

We report on the design, operation, and implementation of a tamper-indicating quantum seal. Our approach is based on transmitting polarization-entangled photon-pair states over optical fibers and monitoring the received entanglement in near real time. We estimate the received entanglement from measured coincidences in a Bell-state analyzer. We show that the entanglement parameter $\mathcal{E}$ is sufficient to discriminate between the entangled states transmitted by the seal and those states that are modified by an intruder.

We also present a detailed theoretical model accounting for the seal operation including its physics and an analysis of its performance in terms of binary-detection theory. We also provide a detailed experimental implementation of the major subsystems, including an entangled photon-pair source based on cw-pumped SPDC and a Bell-state analyzer based on two-photon interferometric time-of-arrival measurements. We integrate these subsystems with an entanglement-monitoring system, and we report the performance of this seal implementation in terms of the generated entanglement, acquisition time, state phase, and temporal delay as they relate to entanglement-detection sensitivity. Based on these results, we conclude that the seal detects spoofed states with a probability $(P_D > 0.9999)$ at a very low false-alarm rate $(P_F \ll 10^{-9})$ for a 10-s time interval. In conclusion, the tamper-indicating quantum seal presented here offers unprecedented surety in the detection of intrusion against fiber-optical seal systems. Applications in containment and surveillance technologies, as well as telecommunications security and fiber-based sensors, are likely to benefit from the adaption of these ideas.

ACKNOWLEDGMENTS

This work is supported by the Defense Threat Reduction Agency. This manuscript is authored by UT-Battelle, LLC, under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy.

[1] A. Chtcherbakov, P. Swart, and S. Spammer, in *Proceedings of the IEEE International Symposium on Industrial Electronics, ISIE '98, 1998* (IEEE, New York, 1998), Vol. 1, pp. 267–270.

[2] B. Griffiths, in *Proceedings of Institute of Electrical and Electronics Engineers 29th Annual 1995 International Carnahan Conference on Security Technology, 1995* (IEEE, New York, 1995), pp. 325–330.

[3] J. Juarez, E. Maier, K. N. Choi, and H. Taylor, Distributed fiber-optic intrusion sensor system, J. Lightwave Technol. **23**, 2081 (2005).

[4] M. Szustakowski and M. Zyczkowski, Fiber optic sensors for perimeter security with intruder localisation, Proc. SPIE Int. Soc. Opt. Eng. **5954**, 59540C (2005).

[5] P. R. V. Horton and I. G. Waddoups, Sandia National Laboratory Technical Report No. SAND95-2279, 1995; http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/27/032/27032416.pdf.

[6] R. G. Johnston, Tamper detection for safeguards and treaty monitoring: Fantasies, realities, and potentials, Nonprolif. Rev. **8**, 102 (2001).
[7] D. Dieks, Communication by EPR devices, Phys. Lett. **92A**, 271 (1982).
[8] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature (London) **299**, 802 (1982).
[9] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, Quantum cloning, Rev. Mod. Phys. **77**, 1225 (2005).
[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[11] K. Bartkiewicz, K. Lemr, A. Černoch, J. Soubusta, and A. Miranowicz, Experimental Eavesdropping Based on Optimal Quantum Cloning, Phys. Rev. Lett. **110**, 173601 (2013).
[12] N. Lütkenhaus, Security against eavesdropping in quantum cryptography, Phys. Rev. A **54**, 97 (1996).
[13] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).
[14] T. S. Humble, R. S. Bennink, W. P. Grice, and I. J. Owens, Sensing intruders using entanglement: A photonic quantum fence, Proc. SPIE Int. Soc. Opt. Eng. **7342**, 73420H (2009).
[15] B. P. Williams, T. S. Humble, and W. P. Grice, Nonlocal polarization interferometer for entanglement detection, Phys. Rev. A **90**, 042121 (2014).
[16] P. M. Anisimov, D. J. Lum, S. B. McCracken, H. Lee, and J. P. Dowling, An invisible quantum tripwire, New J. Phys. **12**, 083012 (2010).
[17] M. Malik, O. S. Magaña-Loaiza, and R. W. Boyd, Quantum-secured imaging, Appl. Phys. Lett. **101**, 241103 (2012).
[18] S. L. Braunstein and A. Mann, Measurement of the Bell operator and quantum teleportation, Phys. Rev. A **51**, R1727 (1995).
[19] H. Weinfurter, Experimental Bell-state analysis, Europhys. Lett. **25**, 559 (1994).
[20] A complete BSA is possible using linear optics and hyper-entanglement [21–23].
[21] M. Barbieri, G. Vallone, P. Mataloni, and F. De Martini, Complete and deterministic discrimination of polarization Bell states assisted by momentum entanglement, Phys. Rev. A **75**, 042317 (2007).
[22] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Beating the channel capacity limit for linear photonic superdense coding, Nat. Phys. **4**, 282 (2008).
[23] C. Schuck, G. Huber, C. Kurtsiefer, and H. Weinfurter, Complete Deterministic Linear Optics Bell State Analysis, Phys. Rev. Lett. **96**, 190501 (2006).
[24] Z.-Y. J. Ou, *Multi-Photon Quantum Interference* (Springer, New York, 2007).
[25] W. P. Grice and I. A. Walmsley, Spectral information and distinguishability in type-ii down-conversion with a broadband pump, Phys. Rev. A **56**, 1627 (1997).
[26] A. Sergienko, Y. Shih, and M. Rubin, Experimental evaluation of a two-photon wave packet in type-ii parametric downconversion, J. Opt. Soc. Am. B **12**, 859 (1995).
[27] H. van Trees, *Detection, Estimation, and Modulation Theory, Part I* (Wiley-Interscience, New York, 2001).
[28] P. K. Bachmann, D. Wiechert, and T. Meeuwsen, Thermal expansion coefficients of doped and undoped silica prepared by means of PCVD, J. Mater. Sci. **23**, 2584 (1988).
[29] T. Kim, M. Fiorentino, and F. N. C. Wong, Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer, Phys. Rev. A **73**, 012316 (2006).
[30] R. C. Pooser, D. D. Earl, P. G. Evans, B. Williams, J. Schaake, and T. S. Humble, FPGS-based gating and logic for multichannel single photon counting, J. Mod. Opt. **59**, 1500 (2012).
[31] http://www.zedboard.org.
[32] http://www.xillybus.com.
[33] T. S. Humble and R. J. Sadlier, Software-defined quantum communication systems, Opt. Eng. **53**, 086103 (2014).