INTRUSION DETECTION WITH QUANTUM MECHANICS: A PHOTONIC QUANTUM FENCE

T. S. Humble*, R. S. Bennink, and W. P. Grice
Oak Ridge National Laboratory
Oak Ridge, Tennessee, 37831

I. J. Owens
Los Alamos National Laboratory
Los Alamos, New Mexico, 87545

ABSTRACT

We describe the use of quantum-mechanically entangled photons for sensing intrusions across a physical perimeter. Our approach to intrusion detection uses the no-cloning principle of quantum information science as protection against an intruder's ability to spoof a sensor receiver using a 'classical' intercept-resend attack. We explore the bounds on detection using quantum detection and estimation theory, and we experimentally demonstrate the underlying principle of entanglement-based detection using the visibility derived from polarization-correlation measurements. no-cloning principle ensures that an adversary cannot replicate the transmitted signal, while the nonlocal correlations established by entanglement reveal any attempts at deception. We propose implementing this idea using polarization-entangled biphoton states, and we present an experimental demonstration of how the polarization-correlation visibility readily identifies intrusion attempts. We further characterize the performance of a hypothetical sensor based on these visibility measurements as well as on the direct detection of the entangled quantum state. We conclude by summarizing these results and suggesting applications for this new application of QIS.

1. INTRODUCTION

Quantum information science (QIS) underlies a new paradigm for processing information in which the quantum mechanical nature of the physical substrate is taken into account. By drawing on uniquely quantum mechanical features, novel approaches to information processing can be developed, e.g., quantum computing and quantum key distribution (QKD). Some of the most remarkable examples include quantum teleportation for the non-local transfer of information, quantum algorithms for accelerating the time-to-solution of select problems, and quantum sensing strategies for resolving signals with a precision limited by the Heisenberg uncertainty principle.

In this report, we describe the adaptation of quantum information to sensing intrusions across a physical perimeter. Specifically, we suggest that a 'quantum fence' based on the transmission of entangled photon pairs provides a unique capability for sensing when an intruder attempts to spoof a receiver using an intercept-resend attack. Underlying our proposal is the no-cloning principle, a tenet of QIS that prohibits perfect cloning of an arbitrary quantum state (Wootters and Zurek, 1982). As discussed below, the

2. POLARIZATION-ENTANGLED STATES

In this section, we review some properties of polarization-entangled photon pairs. In particular, we introduce the polarization-correlation visibility as a measure of the entanglement carried by a biphoton polarization state, and we discuss how entangled states can be discriminated from unentangled states based on this measure.

2.1 Single-mode, polarization-entangled biphotons

The simplest example using polarization-entangled photons to detect intrusions considers a photon-pair source that outputs single-mode, entangled states of the form

$$|\varphi_{PG}\rangle = \frac{1}{\sqrt{2}}\left(|h_P, v_G\rangle + |v_P, h_G\rangle\right), \qquad (1)$$

where the horizontally and vertically polarized states of photon j are denoted $|h_j\rangle$ and $|v_j\rangle$, respectively. The indices P and G refer to the patrol and guard photons shown in Fig. 1, where the patrol photon traverses the monitored boundary while the guard photon remains in a secure location, perhaps near the source. Note that

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intrusion Detection With Quantum Mechanics: A Photonic Quantum Fence	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Oak Ridge National Laboratory Oak Ridge, Tennessee, 37831**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002187. Proceedings of the Army Science Conference (26th) Held in Orlando, Florida on 1-4 December 2008, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**6**	

the entangled state in Eq. (1) differs from the unentangled state

$$|h_P, v_G\rangle = |h_P\rangle \otimes |v_G\rangle \quad (2)$$

in that the latter can be factorized as a product of single-photon polarization states while the former cannot. A key element in our detection strategy is the ability to discern between entangled and unentangled states.

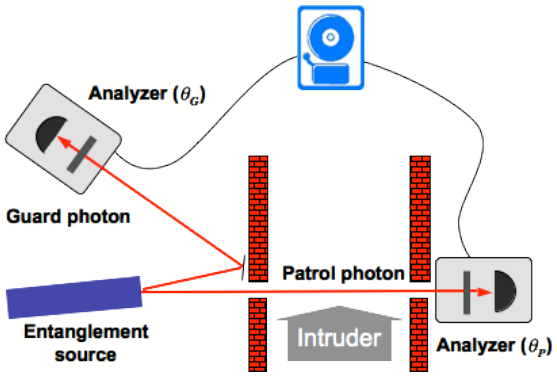

Fig. 1 A schematic implementation of a photonic quantum fence to monitor intrusions along a corridor. Polarization analyzers for the patrol and guard photons provide measurement data to an alarm system that validates the entanglement between the transmitted photon pairs using the visibility. If the expected entanglement is absent, then the alarm sounds.

Experimentally, the amount of polarization entanglement carried by a biphoton state can be detected from polarization-correlation measurements and quantified in terms of the correlation visibility. The polarizations correlations are obtained from an ensemble of identically prepared states using a pair of polarization analyzers, i.e., polarization detectors variably rotated with respect to one another. For the j^{th} photon, the analyzer measurement can be modeled using the rotated creation operator

$$a_j^\dagger(\theta_j) = h_j^\dagger \cos\theta_j + v_j^\dagger \sin\theta_j, \quad j = P, G. \quad (3)$$

The probability that both photons are detected is

$$P_{PG}(\theta_P, \theta_G) = \langle a_P(\theta_p), a_G(\theta_G) | \rho_{PG} | a_P(\theta_p), a_G(\theta_G) \rangle \quad (4)$$

where ρ_{PG} is the density operator of the pair. The probability to detect one photon at the j^{th} analyzer is

$$P_j(\theta_j) = \langle a_j(\theta_j) | \rho_j | a_j(\theta_j) \rangle \quad (5)$$

with ρ_j the single-photon density operator obtained by tracing out the unmeasured photon. For the maximally polarization-entangled state of Eq. (1), the single-photon detection probabilities are

$$P_j(\theta_j) = 1/2, \quad (6)$$

for $j = P, G$, while the joint detection probability is

$$P_{PG}(\theta_P, \theta_G) = \frac{1}{2}\sin^2(\theta_P + \theta_G). \quad (7)$$

This yields a conditional joint detection probability

$$P_{PG}^C(\theta_P, \theta_G) = P_{PG}(\theta_P, \theta_G)/P_G(\theta_G) = \sin^2(\theta_P + \theta_G). \quad (8)$$

Compelling evidence for quantum entanglement arises when a similar conditional probability is measured after the incoming photons undergo a change in basis. In particular, inserting a half-wave plate into the path of each photon performs the unitary transformations

$$U_j^{\lambda/2} |h_j\rangle = \frac{1}{\sqrt{2}}\left(|h_j\rangle + |v_j\rangle\right) \quad (9)$$

and

$$U_j^{\lambda/2} |v_j\rangle = \frac{1}{\sqrt{2}}\left(|h_j\rangle - |v_j\rangle\right). \quad (10)$$

Remarkably, the resulting conditional joint detection probability remains sinusoidal for the case of entangled states (albeit phase-shifted relative to Eq. (8)). In contrast to an entangled state, neither the unentangled state in Eq. (1) nor any unentangled state, demonstrates a similar behavior for the correlation measurement, e.g., when the two photons exist in a classical mixture described by the density matrix

$$\rho = \left[|h_1, v_2\rangle\langle h_1, v_2| + |v_1, h_2\rangle\langle v_1, h_2|\right]/2. \quad (11)$$

This state corresponds to a mixture of correlated polarizations. In the *h*-*v* basis, the mixed state yields a sinusoidal conditional joint detection probability identical to Eq. (8). However, changing the basis of the incoming photons according to Eqs. (9) and (10), the sinusoidal variation is replaced by a flat distribution representing a lack of coherence between detections. Thus, experimentally acquired polarization-correlation measurements can be used to identify whether entanglement is present in an ensemble of identically prepared biphoton states.

2.2 Identifying polarization-entangled biphotons

A convenient and compact figure of merit for characterizing the entanglement carried by a pair of photons is the visibility *V*, which is defined in terms of the maximal and minimal values of the conditional joint detection probability as

$$V = (P_{\max}^C - P_{\min}^C)/(P_{\max}^C + P_{\min}^C), \quad (12)$$

The extremal values are determined experimentally by measuring the conditional detection probability as a function of the polarization-analyzer angles, cf. Eq. (8). A maximally polarization-entangled state yields unit visibility in either basis, while an unentangled state yields a vanishing visibility in at least one basis. Furthermore, the visibility serves as a quantifying

measure of the polarization entanglement, with a higher visibility indicating greater entanglement. This approach to quantifying visibility has traditionally been useful for estimating the losses in bench-top quantum optical setups, where visibilities above 99% are routinely observed.

At the heart of the quantum fence is the ability to validate that the entangled biphoton states are reliably transmitted. This includes the secured transmission of the guard photon, as well as the potentially compromised transmission of the patrol photon along the monitored perimeter. Under normal conditions, the polarization analyzers register correlations indicative of the presence of entanglement. The certainty of this can be quantified using the visibility. On the other hand, if an intruder interacts with the patrol photon, then the entanglement with the guard photon is destroyed and the visibility measured by the receivers vanishes. The interaction can arise from either unintentional destruction of the photon (absorption, scattering) or an intentional attempt by the intruder to replace the patrol photon with a doppelganger. In subsequent sections we discuss the reliability with which these distinctions can be made.

3. QUANTUM DETECTION THEORY

As described in Sec. 2, polarization entanglement can be quantified by performing a series of measurements on an ensemble of identically prepared system, e.g., by measuring the visibility using polarization-correlation measurements taken with different analyzer settings. However, this approach to quantifying entanglement is not direct detection. In fact, a direct measure (detection) of entanglement is not possible because entanglement is regarded as an amplitude-level descriptor of the quantum state and is, therefore, not a physical observable. From the standpoint of sensor development, however, a pertinent question is how well a sensor can directly discriminate between an entangled state and an unentangled state (perhaps with some error). As described below, we formulate this question within the context of quantum detection theory and find that for certain scenarios the entangled and unentangled states can be discriminated.

3.1 Quantum binary decision problem

We consider a binary decision problem, in which a single measurement results is used to identify which of two hypotheses is most likely. Quantum detection theory for the binary decision problem considers hypothesis H_0 to assert that the quantum state of an observed system is ρ_0 and hypothesis H_1 to assert that the quantum state is ρ_1. The binary decision problem devises a decision rule to optimize selection of the correct hypothesis based on the outcome of a detection operator, i.e., we define a decision rule (strategy) with respect to a detection operator Π such that

$$\text{for } \langle \Pi \rangle = 1 \text{, choose } H_1$$
$$\text{for } \langle \Pi \rangle = 0 \text{, choose } H_0 \tag{13}$$

The accuracy of the decision rule is characterized by the probability for detection

$$Q_d = \mathrm{Tr}[\Pi \rho_1] \tag{14}$$

and the false alarm rate

$$Q_0 = \mathrm{Tr}[\Pi \rho_0]\,. \tag{15}$$

In determining the optimal detection operator Π, we employ the Neyman-Pearson criterion, for which the detection scheme is designed to give a fixed false alarm rate Q_0 (and does not require *a priori* probabilities about the intruder's intentions). These considerations lead to the quantum detector equation

$$Q_d - \lambda Q_0 = \mathrm{Tr}[\Pi(\rho_1 - \lambda \rho_0)]\,, \tag{16}$$

which is maximized with respect to the detection operator. Employing the eigenstates of the difference operator

$$(\rho_1 - \lambda \rho_0)|\eta_k\rangle = \eta_k |\eta_k\rangle\,, \tag{17}$$

the optimal detection is defined in terms of the matrix elements

$$\langle \eta_k | \Pi | \eta_k \rangle = \begin{cases} 1 & \text{if } \eta_k \geq 0 \\ 0 & \text{otherwise} \end{cases}. \tag{18}$$

As a result, the optimal detection operator is

$$\Pi = \sum_k^{\eta_k \geq 0} |\eta_k\rangle\langle\eta_k|\,, \tag{19}$$

which yields a detection probability

$$Q_d = \sum_k^{\eta_k \geq 0} \langle \eta_k | \rho_1 | \eta_k \rangle \tag{20}$$

and a false alarm rate

$$Q_0 = \sum_k^{\eta_k \geq 0} \langle \eta_k | \rho_0 | \eta_k \rangle\,. \tag{21}$$

3.2 Biphoton pure states

As an applicable example of the binary decision problem, consider the biphoton pure states

$$\rho_k = |\varphi_k\rangle\langle\varphi_k|\,. \tag{22}$$

where the normalized pure states are defined as

$$|\varphi_k\rangle = a_k |h_1, v_2\rangle + b_k |v_1, h_2\rangle\,, \tag{23}$$

and $|a_k|^2 + |b_k|^2 = 1$ for k = 1, 2. It is straightforward to show that the eigenvalues of the difference operator are

$$\eta_k = a - (-1)^k R \tag{24}$$

with $a = (1-\lambda)/2$ and $R^2 = a^2 + \lambda q$, where

$$q = 1 - \left|\langle \varphi_0 | \varphi_1 \rangle\right|^2 \tag{25}$$

measures the distinguishability of the two pure states. Hence, the optimal detection operator is

$$\Pi = |\eta_1\rangle\langle\eta_1| \tag{26}$$

with the eigenstate given up to a phase factor by

$$|a_1|^2 = \frac{|1-\eta_1|^2}{2R(\eta_1 - q)} \text{ and } |b_1|^2 = \frac{|1-q|^2}{2R(\eta_1 - q)}. \tag{27}$$

Using these results, we obtain the detection probability and false alarm rate for discriminating between two pure states as

$$Q_d = \frac{\eta_1 + \lambda q}{2R} \tag{28}$$

and

$$Q_0 = \frac{(\eta_1 - q)}{2R}, \tag{29}$$

respectively. Helstrom has shown that by eliminating the dependence on the threshold λ this set of equations can be expressed more compactly as (Helstrom, 1976)

$0 \le Q_0 \le 1 - q$

$$Q_d = \left(\sqrt{Q_0(1-q)} + \sqrt{(1-Q_0)q}\right)^2 \tag{30}$$

and

$1 - q \le Q_0 \le 1$

$$Q_d = 1. \tag{31}$$

The results of this analysis yield the receiver operating characteristic (ROC) curves shown in Fig. 2. The curves are parameterized by the value of q. Note that as the value of q approaches 1, the states are quantum mechanically more distinguishable and the performance of the sensor improves, as indicated by the ROC curve. As a specific example, when the first state is equivalent to the entangled state in Eq. (1) and the second state is equivalent to the unentangled state in Eq. (2) then the quantity q equals ½ and we see that Q_d = ½ for Q_0 = 0 and Q_d = 1 for Q_0 = ½.

3.3 Direct discrimination of mixed states

The solution to the quantum binary detection problem depends on the two states being discriminated against. For the case that the unentangled biphoton state ρ_0 is given the mixed polarization state in Eq. (11), a straightforward solution of the eigenvalue problem yields an optimal detection operator that is identical to the entangled biphoton density matrix ρ_1, i.e., $\Pi=\rho_1$. It is important to note that this result is independent of the threshold λ. Consequently, the detection probability Q_d = 1 and the false alarm rate Q_0 = ½ can not be improved upon by lowering the threshold for detection. This result arises because the correlations exhibited by the entangled state cannot be distinguished from classical correlations through direct detection.

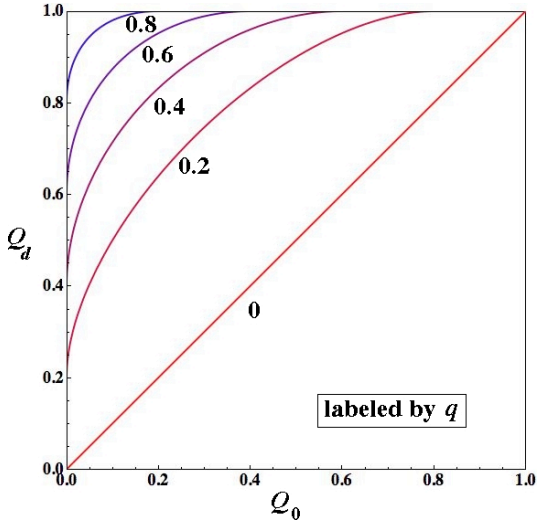

Figure 2. The ROC curve for discriminating between two pure states. The curves are parameterized by the value of q, which measures the orthogonality of the quantum states. When q = 0, the states are identical and the probability for detection Q_d equals the false alarm rate Q_0. As q approaches unity, the states become more quantum mechanically distinct and the detection strategy improves.

This last example emphasizes that entanglement is not a physical observable and that a sensing strategy based on direct detection of the quantum state is not a useful means to identify the presence of an active intruder. However, the density matrices ρ_1 and ρ_0 lead to distinctively different results for the polarization-correlation visibility, cf. Sec. 2, and we discuss using this metric for detection next.

3.4 Using visibility to discriminate states

In this section, we formulate the binary decision problem using the polarization-correlation visibility. As noted previously, the visibility is unity for a pure, entangled biphoton state and vanishes for an unentangled state (in at least one basis). We expect experimental noise to blur this distinction. Moreover, the accuracy of the visibility measurement should be strongly dependent on the number of biphoton states

that are sampled. We consider two hypotheses for the i^{th} sample s_i,

$$H_0: s_i = V_0 + n \quad \text{and} \quad H_1: s_i = V_1 + n, \tag{32}$$

where $V_0 = 0$ and $V_1 = 1$ are the expected visibilities for the unentangled and entangled photon pairs, and n denotes a zero-mean Gaussian random noise variable of variance σ^2. For M measurements, this leads to the log likelihood ratio test

$$\sum_{i=1}^{N} \tilde{s}_i \underset{H_0}{\overset{H_1}{>\!<}} \frac{\ln \lambda}{d} + \frac{d}{2} \tag{33}$$

where $\tilde{s}_i = s_i / \sigma M^{1/2}$ is the normalized sample data, λ is the threshold and $d = M^{1/2}\Delta V/\sigma$ is the normalized value of $\Delta V = V_1 - V_0$.

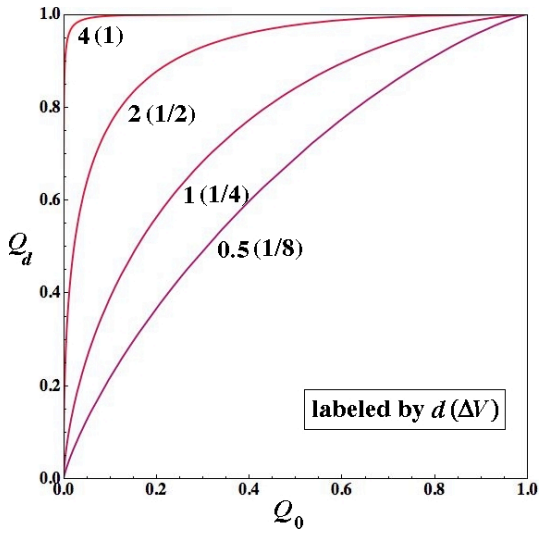

Figure 3. The ROC curve using the polarization-correlation visibility. The curves are parameterized by the dimensionless displacement $d = M^{1/2}\Delta V/\sigma$. For $\sigma = 1/4$ and $M^{1/2} = 1$, the visibility offset is in parentheses.

Discriminating between two signals values in additive Gaussian noise leads to well known results for the detection and false alarm probabilities (Van Trees, 2001)

$$Q_d = erfc(x_1) \quad \text{and} \quad Q_0 = erfc(x_0) \tag{34}$$

where the complementary error function is defined as

$$erfc(y) \equiv (2\pi)^{-1/2} \int_y^{\infty} \exp[-x^2/2]\,dx \tag{35}$$

and the lower limits

$$x_0 = (\ln \lambda)/d + d/2 \quad \text{and} \quad x_1 = (\ln \lambda)/d - d/2 \tag{36}$$

are given in terms of the threshold and the displacement.

The associated ROC curve is shown in Fig. 3 for different values of visibility. Note that this detection strategy succeeds in discriminating entangled states from classical mixed states. This detection strategy does not require that the underlying quantum states be known. Rather, this strategy determines whether the guard-patrol photon pair was entangled. As noted above, only when an intruder has not interacted with the transmitted patrol photon will a high visibility be obtained.

3.5 Experimental test for tampering

We have experimentally tested the idea that the visibility can indicate that an intrusion has occurred using the setup shown in Fig. 4. In the experiment, the entangled photon pairs are generated using spontaneous parametric down conversion in a nonlinear optical crystal (BBO). The guard and patrol photons are sent to separate detectors where their polarizations correlations are analyzed using a high-speed rotatable polarizer to enact a change of basis. The outcomes of the individual polarization analyzers are monitored for coincident detections, which are used to calculate the conditional correlation as a function of the analyzer angles. The maximum and minimum of this detection probability is then used to calculate the visibility V.

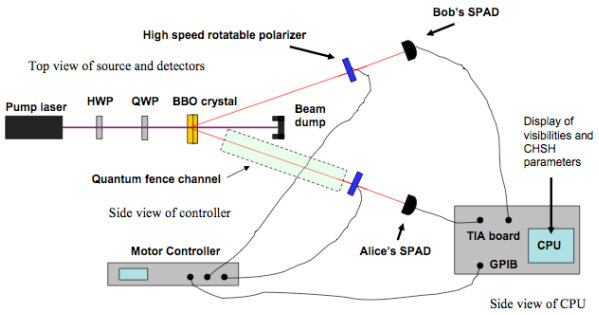

Figure 4. The experimental setup used to generate the polarization entangled photon pairs and calculate the polarization-correlation visibility.

We have validated that the visibility can be used to identify when an intrusion has taken place by examining the visibility acquired under both normal and abnormal (intrusion) conditions. The results of these experiments are shown in Fig. 5, where different scans are acquired under different tampering conditions. Scans 1, 2, and 3 give the visibility under normal conditions, while scans 4, 5, and 6 give the visibilities under different types of tampering. As expected, the visibility under normal conditions is high (above 90%), while the visibilities after tampering are considerably lower. In scan 4, a phase plate inserted into the path of the patrol photon randomizes the

overall polarization state and leads to a reduction in the correlations. In scan 5, the patrol photon is completely blocked, though stray light (noise) leads to a nonvanishing visibility. In scan 6, the polarization correlations between guard and patrol photons corresponding to different photon pair states are analyzed. This simulation of an intercept-resend attack most closely resembles an intrusion scenario. Notably, the visibility from this scan is much less than the visibility in the nominal case.

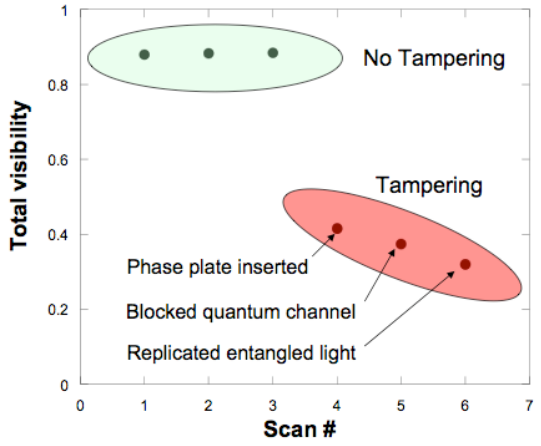

Figure 5. Experimentally acquired polarization-correlation visibility measurements under different intrusion conditions. Scans 1, 2, and 3 are visibility measurements in the absence of any tampering with the entangled photon pair, while scans 4, 5, and 6 each correspond to a different case of tampering: 4 – rotating the polarization of one photon, 5 – fully blocking transmission of one photon, and 6 – the visibility for photons that are unentangled.

The experimental results presented in Fig. 5 exemplify the argument that the visibility will drastically change when an entangled pair of photons is replaced by an unentangled pair. Moreover, the change in visibility with respect to scan is indicative of how the sensing strategy could be formulated, i.e., the difference in visibility from one scan to the next could be used to identify when transmission changes from a normal and to an abnormal cases. In this example, the sensor would be characterized by the ROC curve shown in Fig. 3 for the value of $\Delta V = 0.6$. While the experimental setup in Fig. 4 has not been optimized for sensor performance, the distinction between the visibility in the tampering and no tampering cases clearly demonstrates the proof-of-principle.

CONCLUSIONS

We have reported on the detection of intrusions across a physical boundary using polarization-entangled biphoton states. The 'quantum fence' offers a unique means for assessing the authenticity of a transmitted signal (the patrol photon) by checking if the patrol photon remains entangled with a securely transmitted guard photon. Because the no-cloning principle prohibits an intruder from duplicating the entangled state, any attempts at spoofing the sensor receiver, as well as blatant intrusions, can be identified using the quantum fence.

The unique capability offered by the quantum fence is the ability to verify the authenticity of a transmitted signal. This capability should prove useful in applications where the integrity of the signal is of absolute importance, e.g., surveillance and reconnaissance. The idea of deploying the quantum fence to monitor a physical boundary, e.g., a perimeter, needs only slight modification to also incorporate monitoring of locks and seals (containment and surveillance technologies), as well as communication systems (detecting eavesdroppers on fiber networks). Research continues into the types of physical systems that could be utilized for these different tasks, but the development of a photonic quantum fence is, now, the most promising.

ACKNOWLEDGEMENTS

The submitted manuscript has been authored by a contractor of the U.S. Government under Contract No. DE-AC05-00OR22725. Accordingly, the U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes. This material is based on work supported by the Defense Advanced Research Projects Agency.

REFERENCES

W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, **299**, 802-803 (1982).

C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York, 1976.

H. L. Van Trees, *Detection, Estimation, and Modulation Theory*, Wiley, New York, 2001.