Proceedings of the INMM & ESARDA Joint Annual Meeting
August 23-26 & August 30-September 1, 2021, Virtual Meeting

FIBER-OPTIC QUANTUM SEAL

Junji Urayama, Constantin Brif, Daniel B. S. Soh, and Mohan Sarovar

Sandia National Laboratories, Albuquerque, NM 87185 and Livermore, CA 94550, USA

ABSTRACT

We report on our development of the fiber-optic quantum seal (FOQS) which will provide high-sensitivity detection capabilities for tamper events at bulk storage facilities to enhance safeguards verification efforts. Long-term verification of critical assets in storage facilities for the containment and surveillance mission area must provide material accountancy with assurance of security and continuity of knowledge. As a part of this effort, future monitoring systems may incorporate networked sensors to perform status checks on individual or collection of containers. FOQS enhances current practices by making use of quantum optical probes to enable channel integrity checks and sensor data authentication. Encoded light pulses in the fiber channels will monitor for intrusions while decoding of these pulses will provide data authentication. FOQS consists of an interferometric quantum transceiver which transmits randomly encoded packets of photons over a fiber loop used to seal a container. These photon packets return to the receiver to be decoded for amplitude and phase information. Comparisons of the transmit and receive signals allow for the characterization of the channel. If the comparison shows high degree of correlation, channel integrity and authentication are deemed true, while a lack of correlation triggers an intrusion alarm. The key advantage that FOQS has is that the quantum probes are governed by the uncertainty principle which prevents the intruder from attacking the channel without leaving a trace. This trace will be used to detect the attack attempt. Experimental work will be discussed for the seal development, and theoretical analysis for enhanced security will be presented in the hypothesis-test framework. *SNL is managed and operated by NTESS under DOE NNSA contract DE-NA0003525. SAND2021-9167 C.*

INTRODUCTION

Fiber-optic seals play an important role in the monitoring of critical assets for international safeguards. In particular, fiber-optic seals serve as tamper-indicating sensors for the monitoring of inventoried materials and provide integrity checks of items such as storage containers and physical spaces. Tamper checks are made by sensing the disturbances from external stimuli on optical pulses traveling down a fiber-optic loop. Tamper attempts result in changes to the optical probes often in the form of amplitude and/or phase changes which can be used to trigger alarms. Due to the configurable nature of the optical fiber, these seals can be arranged as small-scale local seals for container monitoring or as large-scale distributed seals for large physical spaces (see Figure 1). With evidence for a growing list of sophisticated attacks on fiber channels for optical links, the sensitivity of the sensor making up the seal must be high and ensure integrity checks of the channel. In the operations of a fiber-optic seal, encoded signal pulses are transmitted to a receiver and decoded for pulse analysis. If the comparison of the transmitted and received pulse stream shows high degree of fidelity, the seal is deemed secure. Given that sophisticated attacks could involve very small changes to the pulse characteristics such as through evanescent coupling, pulse re-routing, and pulse injection, the sensitivity of the seal is of utmost importance.

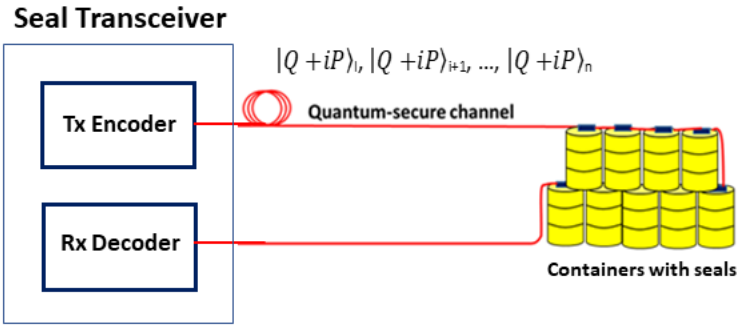

Figure 1. Diagram of a fiber-optic seal transceiver. The seal consists of a transmitting encoder which sends light pulses through the fiber channel and a receiving decoder. Changes induced on the light pulses are analyzed to determine tamper levels. The optical fiber is routed around the important asset for monitoring.

In this paper, we provide an update of our ongoing work for the development of the fiber-optic quantum seal. The main objective for this project is to enhance the sensitivity level of the fiber-optic seal to detect sophisticated data-falsification attacks. This class of attacks includes the intercept-and-resend of the sensor data to falsify seal signals. The quantum version of the fiber-optic seal makes use of laws of quantum mechanics to prevent adversaries from counterfeiting the encoded probe signals [1]. Such attempts by an adversary could create a hole in the seal which could be used to breach security.

This novel quantum seal provides capabilities for data-falsification attacks by leveraging the Uncertainty Principle and the No Cloning Theorem from quantum mechanics. These concepts prevent an intruder from fully characterizing the properties of the quantum probe pulses without leaving a trace and in fact prevent the intruder from copying the quantum probes with high fidelity. The trace that the intruder would leave is increased noise at the decoder which can be used to detect the presence of an attack. The approach taken in this effort is the use of coherent states as the quantum probes in the prepare-and-measure scheme [2]. Here, laser pulses are prepared in coherent states with normally distributed random values for their two quadratures. These pulses are transmitted over the seal fiber channel and then measured on the receiver package using balanced coherent detection. The matching of the transmitted and received quadrature measurements is used to assess the security status of the seal. We describe in the following sections the progress on the experimental development work and the theoretical and numerical analysis work used to determine the tamper state under the hypothesis-test framework.

EXPERIMENT

The experimental implementation of the fiber-optic quantum seal makes use of continuous-variable quadrature measurements to estimate the quadrature values of the encoded stream of coherent states [2]. The basic components of both the transmitter and receiver are depicted in Figure 2. The transmitter consists of a narrow-line laser which is modulated with an amplitude (AM) and phase modulator (PM). The modulators control the amplitude and phase of the light pulses to assign orthogonal quadrature values, *Q* and *P*, for the coherent states. These pulses are sent down the seal fiber channel and combined with the split-off local oscillator for quadrature measurement at the balanced detectors (BD). The local oscillator enables coherent detection and provides the reference phase against which phase measurements are taken. The balanced coherent detection is performed in the shot-noise limit enabling high sensitivities to excess noise imparted by the intruder.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.

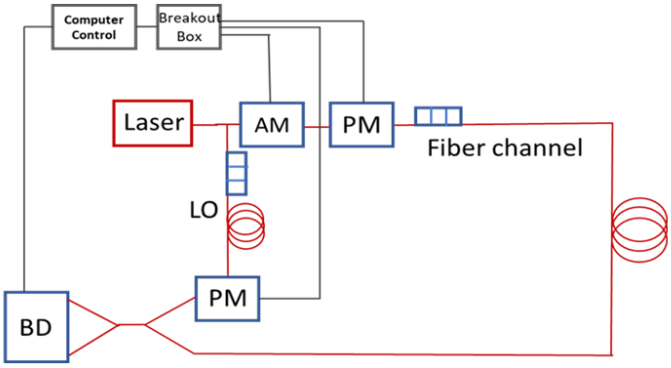

Figure 2. Schematic of the experimental setup for the fiber-optic quantum seal. The transmitter consists of a narrow-line laser with amplitude (AM) and phase modulators (PM) used for encoding. The local oscillator used for coherent detection is split off from the transmitter laser and combined with the signal beam at the balance detector (BD) for quadrature measurements.

The procedure for the seal operation is as follows. The transmitter assigns the Q and P quadrature values randomly from a Gaussian distribution which has a distribution variance of V_A. After these coherent states traverse the seal fiber channel, the receiver makes a coherent measurement of one of the quadratures per pulse. In principle, this measured quadrature value can be calibrated and compared with the encoded value. Due to challenging phase jitters observed in interferometric measurements in the optical domain, fixed reference pulses are also transmitted along with signal pulses to estimate the random phase rotations suffered along the fiber path. The phase changes measured with the reference pulses allow for phase compensation which establishes common reference frames for phase measurements at transmit and receive.

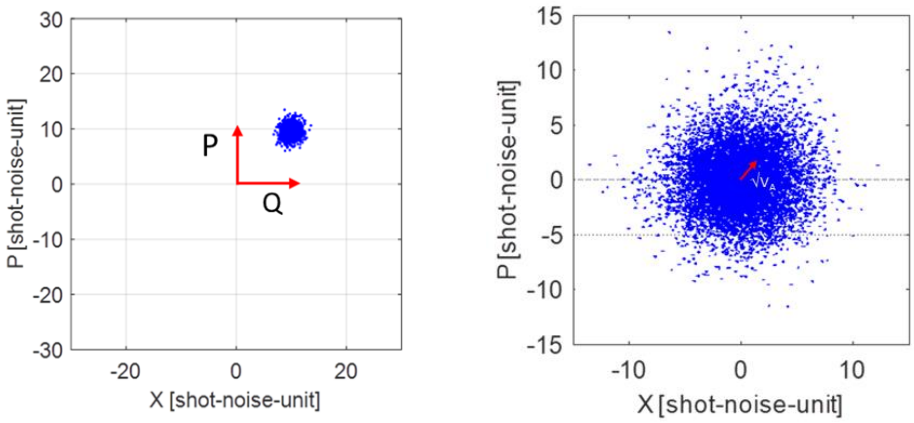

Figure 3. Plots of measured quadrature values in phase space over a sequence of signal pulses. Both for a discrete point (left) and Gaussian distribution (right) of states, the controls for modulation and measurements via the reference pulses produce good reconstruction of the transmitted states.

With these procedures and controls in place, arbitrary coherent states can be generated, transmitted, and detected using coherent detection. Recent results point to adequate quantum state control for reconstruction as shown in Figure 3. On the left of this figure is a plot of the measured quadratures over 500 pulses with Q and P each having a value of 10 shot noise units (SNU). This reconstruction of a discrete point in phase space shows a mean value as assigned at the transmitter and shows shot-noise fluctuations about the mean value as expected. Similar device controls are demonstrated on the right figure with a reconstruction of states generated with a Gaussian distribution with a variance, V_A. The quality of the Gaussian distribution is a

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.

feature required for data analysis, as will be shown below in the analysis section, thus steps need to be taken to stabilize the acquisitions.

The acquired data for transmit and receive were overlayed in the left plot of Figure 4. Accounting for channel losses and detector efficiency, the overlay shows a reasonable match between the two sets of data. In addition, the shape of Gaussian distributions looks reasonable as depicted in the histograms on the middle and right plots for the *Q* and *P* quadratures respectively. Preliminary numbers on point-to-point correlations between the transmit and receive signals show good matching. This matching is achieved at the shot-noise-level resolution. The next steps for the experiments will be on the stabilization of the seal components for consistent performance. The results thereafter will be used in the analysis for seal status. As will be shown in the next section, the array of data points for the $Q_{A,B}$ and $P_{A,B}$ quadratures will be assessed quantitatively to determine whether the assigned quadratures at A (Alice, transmitter) correlate well with those measured at B (Bob, receiver). This assessment feeds into hypothesis testing which is used to determine the status of the seal for binary decision making.

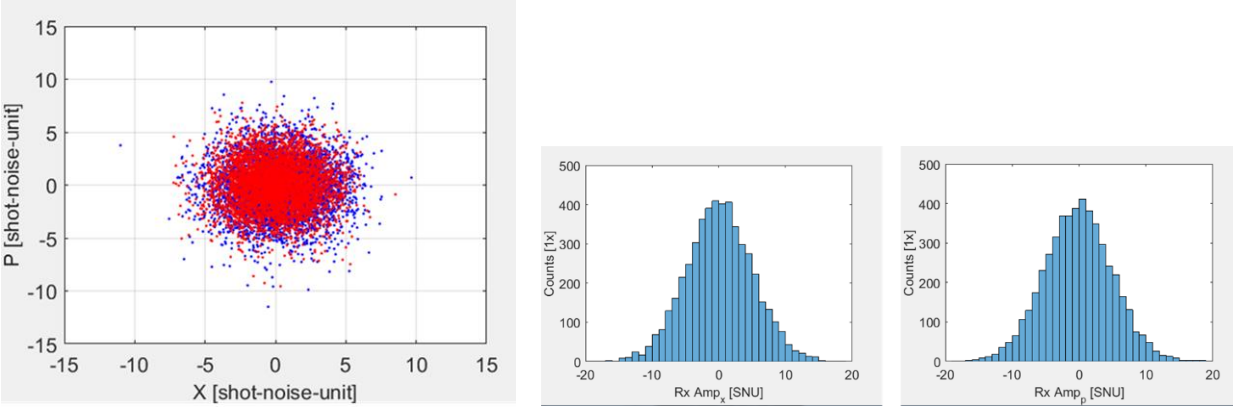

Figure 4 Left: Overlapped plot of Gaussian distribution of transmitted states (red) and received states (blue). Overlap shows good matching in the absence of external disturbance. Histogram of the Gaussian distribution taken as counts along the x-axis (middle) and y-axis (right) to show quality of the distribution for the Q and P quadratures.

THEORETICAL ANALYSIS

To mathematically describe the quantum seal operation, we assume that the channel, with or without tampering, is represented by a lossy, noisy passive Gaussian process that models channel transmittance, channel excess noise, detection inefficiency, and electronic detector noise. Under this assumption, $\langle Q_A \rangle = \langle P_A \rangle = \langle Q_B \rangle = \langle P_B \rangle = 0$, and properties of Alice's and Bob's observables are completely described by their second moments. Therefore, it is convenient to use the covariance matrix γ_{AB} whose elements are expectation values $\langle O_i O_j \rangle$ where $\mathbf{O} = \{Q_A, P_A, Q_B, P_B\}$ [8]. The respective covariance matrix is [2][6]:

$$\gamma_{AB} = \begin{pmatrix} V_A I_{2\times 2} & \sqrt{T\eta} V_A I_{2\times 2} \\ \sqrt{T\eta} V_A I_{2\times 2} & T\eta(V_A + 1 + \xi) I_{2\times 2} \end{pmatrix}. \quad (1)$$

Here, $I_{2\times 2}$ is the 2×2 identity matrix, T is the channel transmittance, η is the detector efficiency (so the overall effective transmittance is $T_{\text{eff}} = T\eta$), ξ is the channel noise (referred to the input of the channel), and V_A is the variance of Alice's Gaussian modulation of the signal pulse. The noise can be modeled as a sum of three terms [8][6]:

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.

$$\xi = \frac{1 - T\eta}{T\eta} + \frac{V_{\mathrm{el}}}{T\eta} + \varepsilon, \tag{2}$$

where the first term is the loss-induced vacuum noise, the second term is the contribution of the detector electronic noise with the variance V_{el}, and ε is the excess noise in the channel. In the unperturbed channel, we set $\varepsilon = \varepsilon_{\mathrm{ch}}$, and in the presence of tampering, $\varepsilon = \varepsilon_{\mathrm{ch}} + \varepsilon_{\mathrm{in}}$, where $\varepsilon_{\mathrm{in}}$ is the additional excess noise due to the actions of the intruder.

We assume that during a session, Alice prepares and sends $2n$ pulses. On a randomly selected subset of n received pulses Bob performs homodyne measurements of the Q_B quadrature, and on the remaining subset of n pulses Bob performs homodyne measurements of the P_B quadrature. These measurements result in two sets of values: $\mathbf{q}_B = \{q_{B1}, q_{B2}, \dots, q_{Bn}\}$ and $\mathbf{p}_B = \{p_{B1}, p_{B2}, \dots, p_{Bn}\}$. Each value q_{Bi} $(i = 1,2, \dots, n)$ has one-to-one correspondence with the value q_{Ai} of the respective pulse generated by Alice, and analogously for p_{Bi} and p_{Ai}. Using these sets of values, Alice and Bob generate two other sets: $\mathbf{x} = \{x_1, x_2, \dots, x_n\}$ and $\mathbf{y} = \{y_1, y_2, \dots, y_n\}$, where $x_i = q_{Bi} - q_{Ai}$ and $y_i = p_{Bi} - p_{Ai}$. Formally, these sets of values correspond to measurements of the observables

$$X = Q_B - Q_A, \quad Y = P_B - P_A. \tag{3}$$

Obviously, $\langle X \rangle = \langle Y \rangle = 0$, and second moments are obtained using Eq. (1):

$$\langle X^2 \rangle = \langle Y^2 \rangle = V_{\mathrm{diff}} = V_A + T\eta(V_A + 1 + \xi) - 2\sqrt{T\eta}V_A, \quad \langle XY \rangle = \langle YX \rangle = 0. \tag{4}$$

For the sake of generality, we set $n = n_1$ for the calibration session and $n = n_2$ for any of the monitoring sessions.

As seen from Eqs. (4) and (2), a tampering attempt will change the statistics of the sets **x** and **y** due to an increase in the excess noise value ε. This change can be detected using a statistical hypothesis test that compares the sets $(\mathbf{x}_{\mathrm{mon}}, \mathbf{y}_{\mathrm{mon}})$ obtained in each monitoring session to the sets $(\mathbf{x}_{\mathrm{cal}}, \mathbf{y}_{\mathrm{cal}})$ obtained in the calibration session. Specifically, we study the utility of three types of statistical tests: the Kolmogorov–Smirnov (KS) test, the Anderson–Darling (AD) test, and the covariance matrix (CM) test.

Each test compares the sets of values $(\mathbf{x}_{\mathrm{mon}}, \mathbf{y}_{\mathrm{mon}})$ and $(\mathbf{x}_{\mathrm{cal}}, \mathbf{y}_{\mathrm{cal}})$ to determine whether they came from the same statistical distribution or different statistical distributions. Formally, this is done by formulating two complementary hypotheses:

1. H_0: values in the sets $(\mathbf{x}_{\mathrm{mon}}, \mathbf{y}_{\mathrm{mon}})$ and $(\mathbf{x}_{\mathrm{cal}}, \mathbf{y}_{\mathrm{cal}})$ came from the same statistical distribution.
2. H_1: values in the sets $(\mathbf{x}_{\mathrm{mon}}, \mathbf{y}_{\mathrm{mon}})$ and $(\mathbf{x}_{\mathrm{cal}}, \mathbf{y}_{\mathrm{cal}})$ came from different statistical distributions.

Each test generates a quantity p known as the p-value, which is the probability of obtaining test results at least as extreme as the results actually observed, under the assumption that the null hypothesis (H_0) is correct. The p-value is compared against a pre-defined threshold value α, which is referred to as the *level of significance*, such that the null hypothesis is accepted if $p \geq \alpha$ and rejected if $p < \alpha$. In terms of tamper detection, if the null hypothesis is accepted, then we conclude that the channel was not perturbed, indicating that no tampering happened. Conversely, if the null hypothesis is rejected, then we conclude that the channel's properties changed after the calibration was performed, indicating that a tampering attempt did happen.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.

The covariance matrix elements for the $(\mathbf{x}, \mathbf{y})$ data set are obtained from Eq. (4), specifically,

$$\gamma_{xy} = \begin{pmatrix} \sigma_x^2 & \rho_{xy}\sigma_x\sigma_y \\ \rho_{xy}\sigma_x\sigma_y & \sigma_y^2 \end{pmatrix} = \begin{pmatrix} V_{\text{diff}} & 0 \\ 0 & V_{\text{diff}} \end{pmatrix}, \tag{5}$$

where σ_x and σ_y are standard deviations for the sets **x** and **y**, respectively, and ρ_{xy} is the correlation coefficient between **x** and **y**. If the channel parameters change, this will affect the covariance matrix elements in Eq. (5). Assuming that the channel is described by a Gaussian process whether tampering is absent or present, the covariance matrix elements can be used to test the null hypothesis H_0 described above. Specifically, the CM test [11] uses a vector of five statistical moments:

$$\theta = \left(\mu_x, \mu_y, \sigma_x, \rho_{xy}, \sigma_y\right)^{\mathsf{T}}, \tag{6}$$

where μ_x and μ_y are mean values for the sets **x** and **y**, respectively. For the coherent-state quantum seal implemented as described here, $\mu_x = \mu_y = 0$, $\rho_{xy} = 0$, and $\sigma_x = \sigma_y = \sqrt{V_{\text{diff}}}$.

As described in [11], the CM test determines whether two data sets $(\mathbf{x}_1, \mathbf{y}_1)$ and $(\mathbf{x}_2, \mathbf{y}_2)$ came from the same normal distribution by determining whether respective vectors θ_1 and θ_2 are statistically different.

The KS statistic [5][10] quantifies a distance between the empirical distribution function of the sample and the cumulative distribution function of the reference distribution, or between the empirical distribution functions of two samples. The null distribution of this statistic is calculated under the null hypothesis that the sample is drawn from the reference distribution (in the one-sample case) or that the samples are drawn from the same distribution (in the two-sample case). In the two-sample case, the distribution considered under the null hypothesis has to be a continuous distribution but is otherwise unrestricted.

The KS test is based on computing the empirical distribution function F_n for a set $\{Z_i\}$ of n independent and identically distributed (i.i.d.) observations, specifically, $F_n(z) = \frac{1}{n}\sum_{i=1}^{n} I_{[-\infty,z]}(Z_i)$, where $I_{[-\infty,z]}(Z_i)$ is the indicator function, equal to 1 if $Z_i \leq x$ and equal to 0 otherwise. In the two-sample case, which is relevant for the quantum seal operation, the KS statistic is $D_{n_1,n_2} = \sup_z \left|F_{n_1}(z) - F_{n_2}(z)\right|$, where F_{n_1} and F_{n_2} are the empirical distribution functions of the first and the second sample, respectively, and sup is the supremum function. We compute the p-value numerically using the routine scipy.stats.ks_2samp, which follows the analysis in [4]. Since we have to compare two-dimensional samples $(\mathbf{x}_1, \mathbf{y}_1)$ and $(\mathbf{x}_2, \mathbf{y}_2)$, we use the KS test performed for various pairs of one-dimensional samples: $\mathbf{x}_1$ and $\mathbf{x}_2$ (denoted on plots below as KS-X), $\mathbf{y}_1$ and $\mathbf{y}_2$ (denoted as KS-Y), $\mathbf{z}_1$ and $\mathbf{z}_2$, where $\mathbf{z} = \{x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n\}$ is the concatenated set of all quadrature measurements (denoted as KS-XY).

The AD statistic [3] quantifies a distance between the empirical distribution function of the sample and the cumulative distribution function of the reference distribution, or between the empirical distribution functions of multiple (two or more) samples. The version of the AD test for multiple (two or more) samples, in which the distribution function does not have to be specified, was developed in [9], and we use its numerical implementation by the routine scipy.stats.anderson_ksamp to compute the p-value. Since we have to compare two-dimensional samples $(\mathbf{x}_1, \mathbf{y}_1)$ and $(\mathbf{x}_2, \mathbf{y}_2)$, we use the AD test performed for various pairs of one-dimensional

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.

samples: $\mathbf{x}_1$ and $\mathbf{x}_2$ (denoted on plots below as AD-X), $\mathbf{y}_1$ and $\mathbf{y}_2$ (denoted as AD-Y), $\mathbf{z}_1$ and $\mathbf{z}_2$ (denoted as AD-XY), as well as the foursome of one-dimensional samples: $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{y}_1$, and $\mathbf{y}_2$ (denoted as AD-4).

We used numerical simulations to evaluate the performance of the statistical tests described above and investigate the dependence of the tamper detection sensitivity on various parameters of the quantum seal setup. In each simulation, we generated two two-dimensional samples of random numbers: $(\mathbf{x}_1, \mathbf{y}_1)$ and $(\mathbf{x}_2, \mathbf{y}_2)$, where each of the samples $\mathbf{x}_1$ and $\mathbf{y}_1$ was of size n_1, each of the samples $\mathbf{x}_2$ and $\mathbf{y}_2$ was of size n_2, and all samples came from normal distributions that correspond to the covariance matrix in Eq. (5). Specifically, the performance of the statistical tests was evaluated on two cases:

Case 1: Both two-dimensional samples are randomly generated from the same normal distribution: $\mu_1 = \mu_2 = 0$, $\sigma_1 = \sigma_2 = \sqrt{V_{\text{diff}}(\varepsilon = \varepsilon_{\text{ch}})}$, where we explicitly denoted the dependence of the variance V_{diff} on the excess noise. This case corresponds to no tampering, and therefore each trial in which the null hypothesis was accepted ($p \geq \alpha$) corresponded to a *true negative*, while each trial in which the null hypothesis was rejected ($p < \alpha$) corresponded to a *false positive*. A measure of performance is the false positive rate (FPR), given by the ratio of false positive counts to the total number of trials.

Case 2: Each two-dimensional sample is randomly generated from a different normal distribution: $\mu_1 = \mu_2 = 0$, $\sigma_i = \sqrt{V_{\text{diff}}(\varepsilon_i)}$, for $i = 1,2$, where $\varepsilon_1 = \varepsilon_{\text{ch}}$ and $\varepsilon_2 = \varepsilon_{\text{ch}} + \varepsilon_{\text{in}}$. This case corresponds to a tampering event, where the intruder adds the excess noise ε_{in}, and therefore each trial in which the null hypothesis was accepted ($p \geq \alpha$) corresponded to a *false negative*, while each trial in which the null hypothesis was rejected ($p < \alpha$) corresponded to a *true positive*. A measure of performance is the false negative rate (FNR), given by the ratio of false negative counts to the total number of trials.

If the adversary employs the "intercept and resend" attack (i.e., they divert the light from the seal fiber using adiabatic optical signal rerouting, perform a heterodyne measurement, and resend the estimated state instead of the original light), they add one shot noise unit (SNU) of excess noise (i.e., $\varepsilon_{\text{in}} = 1$ SNU). However, if the adversary does not attempt to remove the seal fiber and just tries to learn about the system, they might divert and replace only a portion of the light. In this scenario, they will add a smaller amount of excess noise, and, generally, $0 < \varepsilon_{\text{in}} \leq 1$ (conservatively, we do not consider a careless intruder that would add classical noise resulting in $\varepsilon_{\text{in}} > 1$). Therefore, we investigate the dependence of the FNR on ε_{in}, for various values of quantum seal parameters (variance of Alice's Gaussian modulation of the signal pulse, V_A, overall effective transmittance of the channel, T_{eff}, unperturbed channel excess noise, ε_{ch}, significance level, α, calibration sample size, n_1, and ratio of monitoring and calibration sample sizes, n_2/n_1). In all simulations we set $V_{\text{el}} = 0.01$ SNU.

Figure 5 shows FPR values obtained in Case 1 versus the sample size n_1 (with $n_2 = 0.9n_1$) and Figure 6 shows FNR values obtained in Case 2 versus the additional excess noise due to the intruder, ε_{in}. Different subplots correspond to various values of V_A and T_{eff}. Each curve corresponds to a particular statistical test, including the CM test, three variants of the KS test (KS-X, KS-Y, KS-XY), and four variants of the AD test (AD-X, AD-Y, AD-XY, AD-4). Each of the FPR and FNR values is obtained from 10000 trials.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.

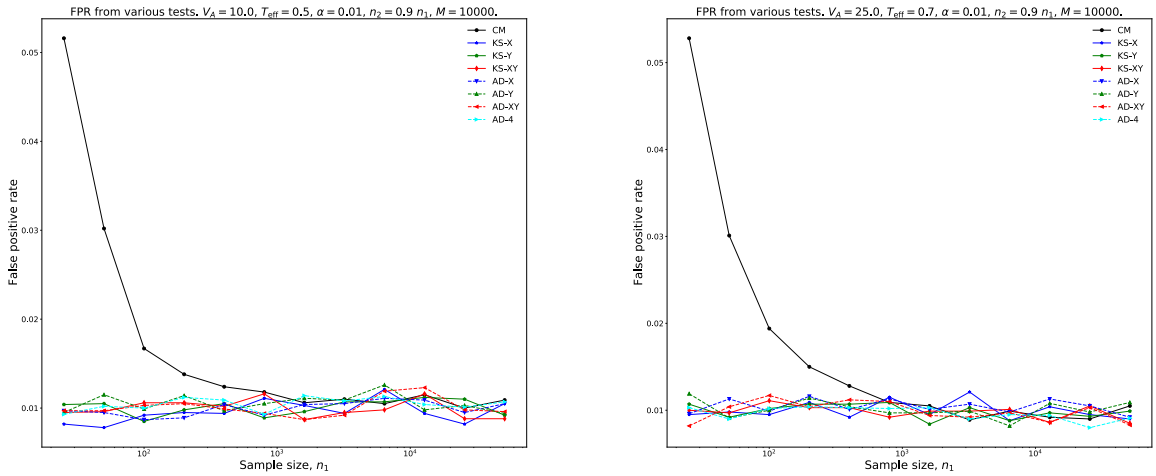

Figure 5. Performance comparison of different statistical tests, including the CM test and various variants of the KS and AD tests. Each subplot shows FPR values obtained from 10000 trials in Case 1, versus the sample size n_1, for $\alpha = 0.01$, $n_2 = 0.9n_1$, $\varepsilon_{ch} = 0.01\ SNU$, and various values of V_A and T_{eff}. (left) $V_A = 10.0\ SNU, T_{eff} = 0.5$. (right) $V_A = 25.0\ SNU, T_{eff} = 0.7$.

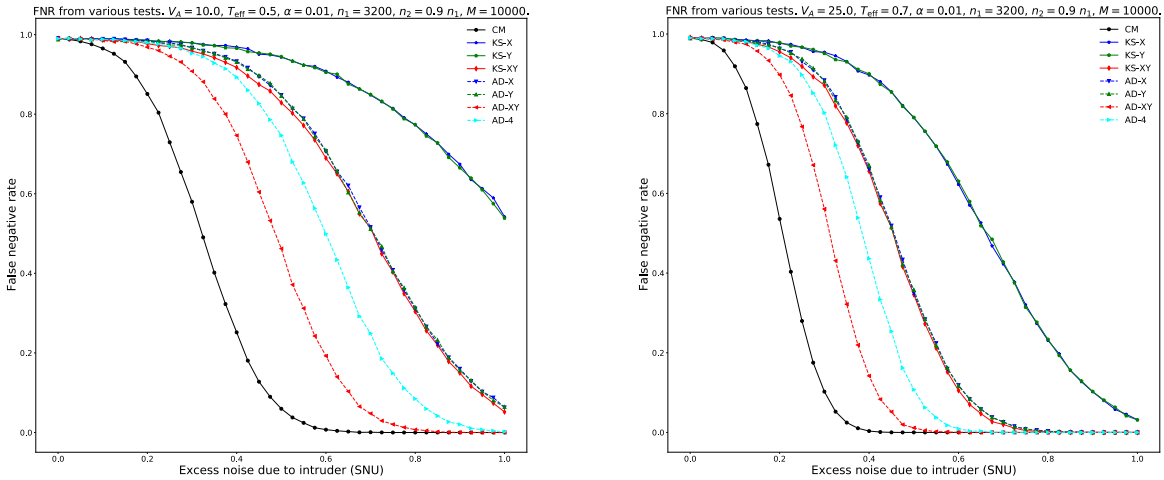

Figure 6. Performance comparison of different statistical tests, including the CM test and various variants of the KS and AD tests. Each subplot shows FNR values obtained from 10000 trials in Case 2, versus ε_{in}, for $\alpha = 0.01$, $n_1 = 3200$, $n_2 = 0.9n_1$, $\varepsilon_{ch} = 0.01\ SNU$, and various values of V_A and T_{eff}. (left) $V_A = 10.0\ SNU, T_{eff} = 0.5$. (right) $V_A = 25.0\ SNU, T_{eff} = 0.7$.

The FPR values in Figure 5 are around the value of the significance level, $\alpha = 0.01$, except for larger values obtained with the CM test for $n_1 \lesssim 1000$. The FNR values in Figure 6 for all tests decrease as ε_{in} increases (ultimately converging to zero for sufficiently large ε_{in}), however, the CM test produces the best (lowest) FNR values, with the AD-XY test being the second best. Overall, if sufficiently large sample size is used so that all tests achieve FPR $\approx \alpha$, the CM test is superior to all other tests since it achieves lowest FNR values for any given combination of the seal parameters, while also being most efficient in terms of the computation time.

We study the FNR obtained in Case 2 using the CM test in more detail, focusing on the effects of various quantum seal parameters. In Figure 7, the FNR is plotted versus ε_{in} for various V_A values, various T_{eff} values, various ε_{ch} values, various α values, various n_1 values, and various n_2/n_1 values. For all these parameter combinations, the obtained FPR is close to the value of α.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.

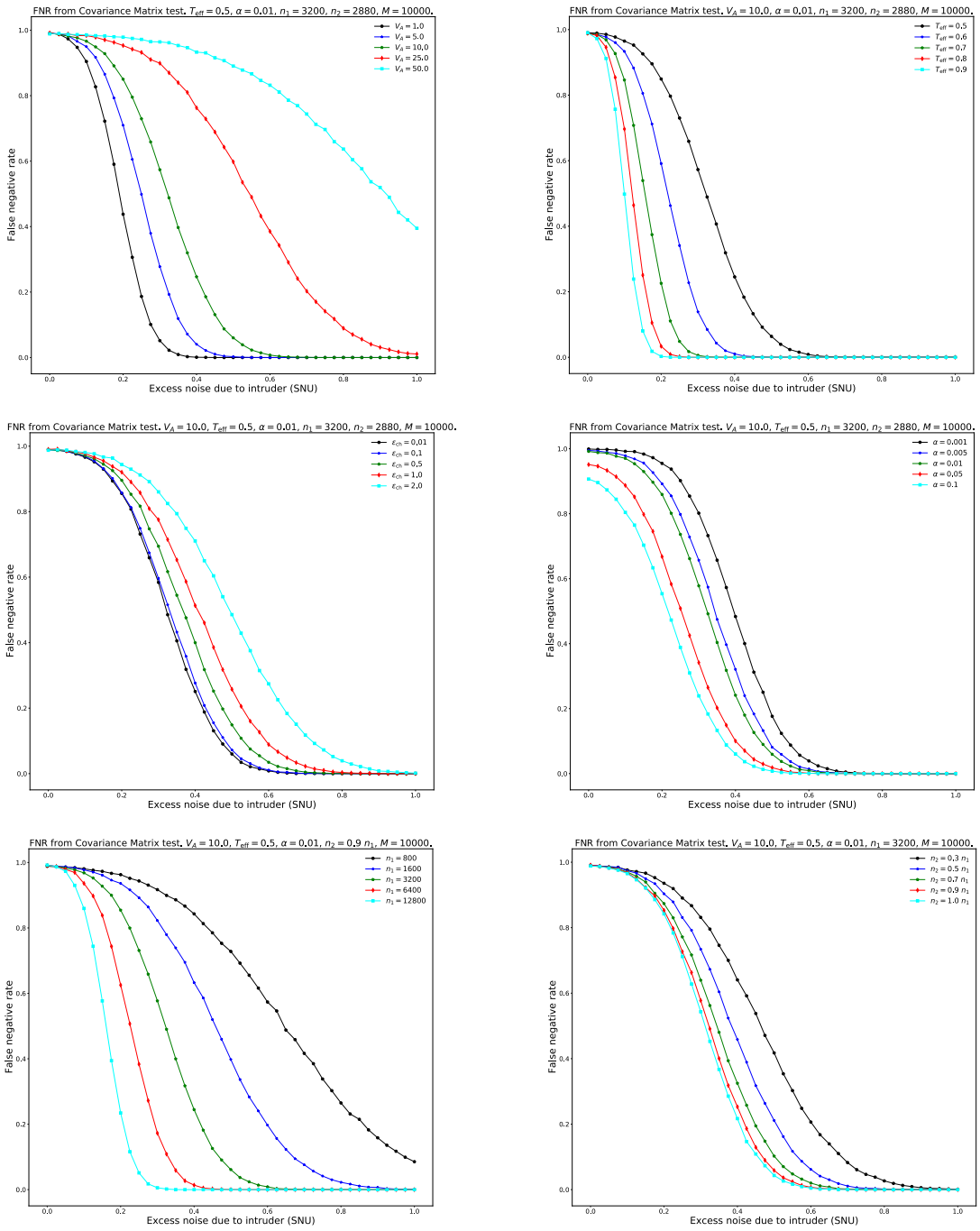

Figure 7. FNR values obtained from 10000 trials in Case 2 using the CM test, versus ε_{in}, for: (top left) various V_A values, (top right) various T_{eff} values, (middle left) various ε_{ch} values, (middle right) various α values, (bottom left) various n_1 values, and (bottom right) various n_2/n_1 values.

Based on the results shown in Figure 7, we can choose sensible values for the quantum seal parameters. Obviously, the smaller is the unperturbed value of the variance $V_{\text{diff}}(\varepsilon)$, the larger is its relative change due to the additional excess noise, and the easier is the tamper detection. For T_{eff} close to one, V_{diff} grows very slowly with V_A, and therefore values of V_A as large as 50 SNU to 100 SNU can be used. However, for lower effective transmittance, e.g., T_{eff} about 0.5, it is

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.

advisable to keep V_A at values about 10 SNU. Ideally, it is preferable to maximize the detector efficiency and minimize the channel loss in order to achieve T_{eff} above 0.5, as well as decrease the existing excess noise in the channel to the level $\varepsilon_{\text{ch}} \leq 0.1$. The sample size for the calibration session, n_1, of about 3000 seems to be reasonable, although using a larger value of n_1 (e.g., about 10^4) would improve the seal sensitivity. The sample size for a monitoring session, n_2, should be preferably not less than $0.5n_1$.

CONCLUSIONS

Controls for the experimental implementation of the fiber-optic quantum seal have been established for generation and shot-noise limited measurements of coherent states used as quantum probes for the seal. Challenges still exist in targeted modulation of these quantum probes for intruder detection. Next steps will include optimizations of the operating points for the seal based on the sensitivity analysis obtained in the theory effort.

Based on the theoretical analysis, the CM test achieves much lower FNR values compared to other tests, and therefore it should be used in practice. Also, using the CM test is most numerically efficient. Computation for hypothesis testing can be fast enough to make it possible to operate a quantum seal at rates of 1 kHz to 10 kHz. We can rely on the obtained theoretical results to choose sensible values of quantum seal parameters for a practical system. The smaller is the unperturbed value of the variance V_{diff}, the larger is its relative change due to the additional excess noise, and the easier is the tamper detection. Specific recommendations regarding optimal parameter values are listed in the text.

REFERENCES

[1] Williams, B. P., K. A. Britt, and T. S. Humble. 2016. "Tamper-Indicating Quantum Seal." *Phys. Rev. Applied* 5 (January): 014001. https://doi.org/10.1103/PhysRevApplied.5.014001.

[2] Soh, D. B. S., C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar. 2015. "Self-Referenced Continuous-Variable Quantum Key Distribution Protocol." *Phys. Rev. X* 5 (October): 041010. https://doi.org/10.1103/PhysRevX.5.041010.

[3] Anderson, T. W., and D. A. Darling. 1952. "Asymptotic Theory of Certain 'Goodness of Fit' Criteria Based on Stochastic Processes." *Ann. Math. Statist.* 23 (2): 193–212. https://doi.org/10.1214/aoms/1177729437.

[4] Hodges, J. L. 1958. "The Significance Probability of the Smirnov Two-Sample Test." *Ark. Mat.* 3 (5): 469–86. https://doi.org/10.1007/BF02589501.

[5] Kolmogorov, A. 1933. "Sulla Determinazione Empirica Di Una Legge Di Distribuzione." *Giorn. Ist. Ital. Attuar.* 4: 83–91.

[6] Laudenbach, F., C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel. 2018. "Continuous-Variable Quantum Key Distribution with Gaussian Modulation—the Theory of Practical Implementations." *Adv. Quantum Technol.* 1 (1): 1800011. https://doi.org/10.1002/qute.201800011.

[7] Sarovar, M., D. Farley, D. B. S. Soh, R. Camacho, and C. Brif. 2019. "Secure Fiber Optic Seals Enabled by Quantum Optical Communication Concepts." https://www.freepatentsonline.com/10341015.html.

[8] Scarani, V., H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. 2009. "The Security of Practical Quantum Key Distribution." *Rev. Mod. Phys.* 81 (September): 1301–50. https://doi.org/10.1103/RevModPhys.81.1301.

[9] Scholz, F. W., and M. A. Stephens. 1987. "K-Sample Anderson–Darling Tests." *J. Am. Stat. Assoc.* 82 (399): 918–24. https://doi.org/10.1080/01621459.1987.10478517.

[10] Smirnov, N. 1948. "Table for Estimating the Goodness of Fit of Empirical Distributions." *Ann. Math. Statist.* 19: 279–81. https://doi.org/10.1214/aoms/1177730256.

[11] Sullivan, J. H., Z. G. Stoumbos, R. L. Mason, and J. C. Young. 2007. "Step-down Analysis for Changes in the Covariance Matrix and Other Parameters." *J. Qual. Technol.* 39 (1): 66–84. https://doi.org/10.1080/00224065.2007.11917674.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No. 2021-9167 C.