SAND2022-8533C

Proceedings of the INMM 63rd Annual Meeting
July 24-28, 2022

FIBER-OPTIC QUANTUM SEAL FOR SAFEGUARDS

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 new results on our development of the fiber-optic quantum seal (FOQS) which will provide high-sensitivity tamper detection capabilities at nuclear facilities to enhance safeguards verification efforts. Long-term verification of critical assets in storage facilities for containment and surveillance must provide material accountancy with continuity of knowledge. As a part of this effort, FOQC will enhance current practices by making use of quantum optical probes to enable fiber-channel integrity checks and sensor data authentication. FOQS consists of an interferometric quantum transceiver which transmits randomly encoded packets of photons over an optical fiber loop used to seal a container. These photon packets return to the receiver to be decoded for field quadrature 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 of the FOQS is that the quantum probes are governed by the uncertainty principle which prevents the intruder from attacking the channel without leaving a trace. We present new results obtained in years two and three of this project, including improvements in the experimental system, automated numerical analysis of obtained experimental data, and extended theoretical analysis of the FOQS sensitivity under realistic conditions. These capabilities increase seal sensitivity and enables detection of data falsification attacks. *SNL is managed and operated by NTESS under DOE NNSA contract DE-NA0003525. SAND2022-XXXX C.*

INTRODUCTION

Nuclear safeguards rely on tamper-indicating seals to maintain continuity of knowledge of monitored items and equipment at nuclear facilities. Such measures are required to prevent diversion of nuclear materials especially in the presence of an increasing number of potential sophisticated attacks. Fiber-optic seals already play an important role in this domain serving as tamper-indicating sensors and integrity checks of critical assets against intrusions. These capabilities are often derived from the tracking of changes to optical pulses transmitted over a fiber channel (Figure 1). If significant changes are observed in the pulse properties, an alarm is tripped.

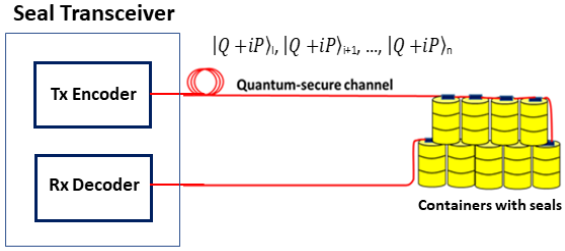

Figure 1. Diagram of a general fiber-optic seal transceiver for monitoring assets. The seal consists of a transmitting encoder which sends light pulses through the fiber channel and a receiving decoder. Changes induced on the light pulses are analyzed to determine tamper status.

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. 2022-XXXX C.

Enhanced sensor sensitivity is a desired property of the seal to detect man-in-the-middle tamper attacks. Given that these attacks could impart very small changes to the pulse characteristics, the seal sensitivity and the associated data analysis must produce high probability of detection with low false alarms. In this paper, we outline the proof-of-concept results of the fiber-optic quantum seal which enhances sensor sensitivity and enables a novel detection capability against data falsification for thwarting intercept-and-resend attacks.

A quantum seal provides capabilities for detecting data-falsification attacks by leveraging the Uncertainty Principle and the No Cloning Theorem from quantum mechanics [1]. These concepts prevent an intruder from fully characterizing the properties of the quantum probe pulses and copying the quantum probes with high fidelity. Any tamper attempt introduces noise to the measured quantities of the quantum probe thereby signaling the presence of the intruder. The approach taken in this effort is the use of coherent states as the quantum probes in the prepare-and-measure scheme [2]. 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 at 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 below the experimental results and the theoretical and numerical analysis used to determine the tamper state under the hypothesis-test framework.

EXPERIMENT

The proof-of-concept experimental implementation of the fiber-optic quantum seal makes use of continuous-variable measurements to estimate the quadrature values of the stream of coherent states [2]. The basic components of the seal transceiver are depicted in Figure 2. The transmitter consists of a narrow-line laser modulated with an amplitude (AM) and phase modulator (PM). The modulators are used to assign orthogonal quadrature values, Q and P, for the coherent states. These pulses are attenuated (Attn.), delivered down the seal fiber channel, and combined with the split-off local oscillator for quadrature measurement at the balanced detectors (BD). The balanced coherent detection is performed in the shot-noise limit enabling high sensitivities to excess noise imparted by tamper attempts.

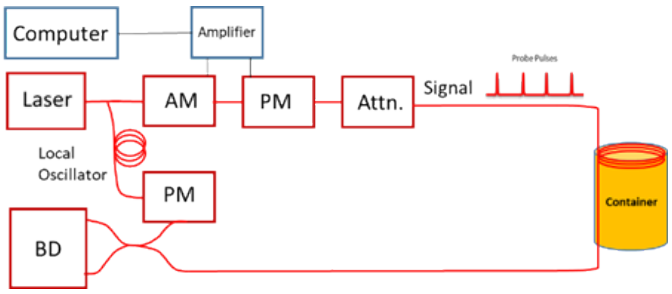

Figure 2. Schematic of the experimental setup for the fiber-optic quantum seal. The transmitter consists of a narrow-line laser with amplitude (AM) and phase modulators (PM) used for encoding. The local oscillator is split off from the transmitter laser and combined with the signal beam at the balance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

The procedure for the seal operation begins with the assignment of random Q and P quadrature values from a Gaussian distribution of variance, V_A. These coherent states are transmitted through the seal fiber channel, and one of the quadratures is measured per probe pulse. Interleaved among the probe pulses are reference pulses to enable phase compensation to overcome phase jitter observed between the probe and local oscillator pulses in the

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. 2022-XXXX C.

interferometer. The compensated phase allows for calibrated quadrature measurements for comparison at transmit and receive.

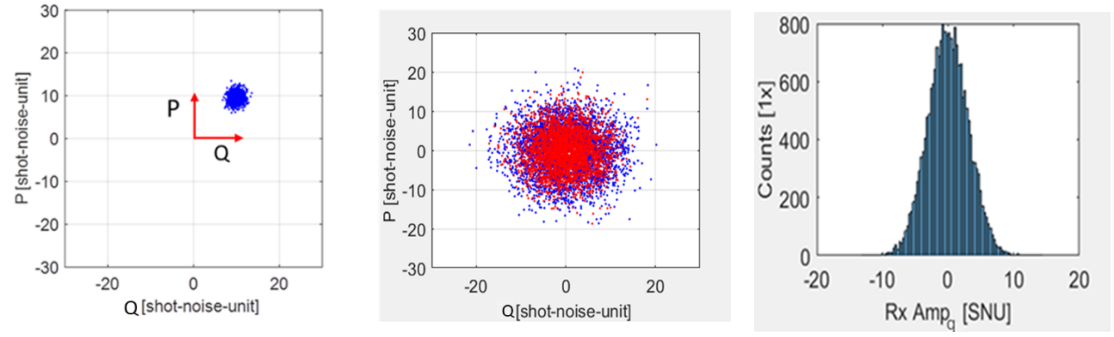

Figure 3. Plots of measured quadrature values in phase space over a sequence of signal pulses. Left: Depiction of measurements of a coherent state in phase space. Middle: Good overlap of Gaussian distribution of transmitted states (red) and received states (blue). This plot shows the results from a seal with no tamper. Right: Typical histogram of the measured Gaussian-distributed Q quadratures.

With these calibrations and controls in place, arbitrary coherent states are generated and detected. On the left plot in Figure 3 is a reconstruction of a coherent state in phase space with Q and P quadratures each having a value of 10 shot noise units (SNU). The spread in the 500 data points about the mean value reflects the shot noise. The measurements are extended to a Gaussian distribution of states as shown in the middle figure. These states are used for seal monitoring, and this particular result shows the "No Tamper" seal state indicated by the good matching between the red and blue points. Here, externally induced excess noise did not disturb the coherent state distribution. In the opposite case, tamper-induced excess noise produces the "Tamper" seal state with mismatching distributions. The plot on the right of the same figure shows a typical histogram of the Gaussian-distributed quadratures representing the high-fidelity control and measurement of the coherent states.

To test the seal response to the "Tamper" state, excess noise was injected using the transmitter modulators in a controlled way. The resulting data distributions are shown in Figure 4. On the left plot is the overlapped distribution of the transmitted states (red) and the received states (blue). As the added-noise standard deviation, $\sqrt{V_n}$, is only 0.6 SNU, the two distributions still appear to match. In spite of this, the hypothesis analysis as described below distinguishes this tamper event. In the right phase-space plot, a non-tampered, calibration data set (red) is overlapped with a tampered, monitoring data set (blue). The latter set has again 0.6 SNU excess noise inserted. The data points are represented by variables X and Y which capture the differences in the Q and P quadratures respectively for the transmit and receive states (see analysis section). Although the red and blue distributions appear similar, the second moment of these distributions gives away the difference. In the inset of the right plot in Figure 4, the standard deviation of the calibration and monitoring data sets are listed for X and Y. The difference in the standard deviation is approximately 0.2 SNU, and this difference directly contributes to the conclusion on the tamper state of the seal. The detection and discrimination of distribution changes with sub-shot-noise resolution points to the high sensitivity of the seal. The quantitative assessment for the binary tamper status of the quantum seal is determined with the hypothesis-test analysis as described in the next section.

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. 2022-XXXX C.

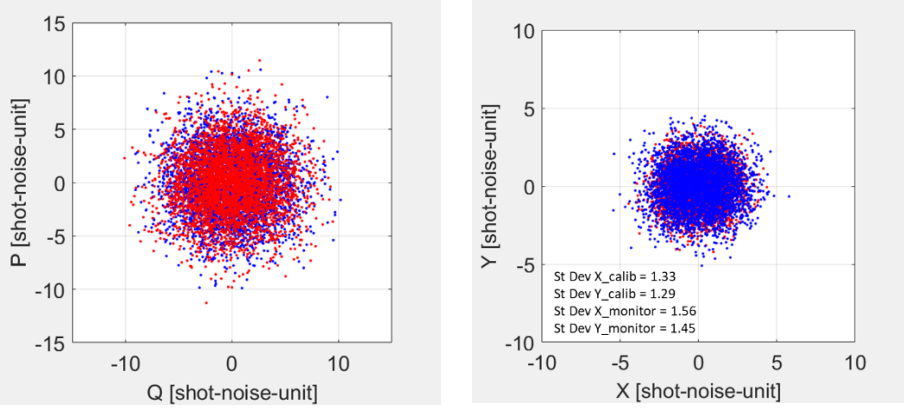

Figure 4 Left: Overlapped Gaussian distribution of transmitted states (red) and received states (blue). Excess noise is added to create the "Tamper" seal state. Excess noise amounts to only 0.6 SNU, but analysis can distinguish this tamper event. Right: Overlap of calibration data set (red) and monitoring data set (blue) plotted using X and Y data representation (see analysis section below). Excess noise is again 0.6 SNU, and the difference in the second moment of the X and Y distributions (see inset) for the calibration and monitoring sets trips the alarm for the tamper state.

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]:

$$\xi = \frac{1 - T\eta}{T\eta} + \frac{V_{\text{el}}}{T\eta} + \varepsilon, \quad (2)$$

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 $\varepsilon = \varepsilon_{\text{ch}}$, and in the presence of tampering, $\varepsilon = \varepsilon_{\text{ch}} + \varepsilon_{\text{in}}$, where ε_{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: $\mathbf{q}_B = \{q_{B1}, q_{B2}, \ldots, q_{Bn}\}$ and $\mathbf{p}_B = \{p_{B1}, p_{B2}, \ldots, p_{Bn}\}$. Each value q_{Bi} $(i = 1,2,\ldots,n)$ 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: $\mathbf{x} = \{x_1, x_2, \ldots, x_n\}$ and $\mathbf{y} = \{y_1, y_2, \ldots, y_n\}$, where $x_i = q_{Bi}$

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. 2022-XXXX C.

$-q_{Ai}$ 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):

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

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 $(\mathbf{x}_{\text{mon}},\mathbf{y}_{\text{mon}})$ obtained in each monitoring session to the sets $(\mathbf{x}_{\text{cal}},\mathbf{y}_{\text{cal}})$ obtained in the calibration session. Specifically, we consider the use 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 $(\mathbf{x}_{\text{mon}},\mathbf{y}_{\text{mon}})$ and $(\mathbf{x}_{\text{cal}},\mathbf{y}_{\text{cal}})$ 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 $(\mathbf{x}_{\text{mon}},\mathbf{y}_{\text{mon}})$ and $(\mathbf{x}_{\text{cal}},\mathbf{y}_{\text{cal}})$ came from the same statistical distribution.
2. H_1: values in the sets $(\mathbf{x}_{\text{mon}},\mathbf{y}_{\text{mon}})$ and $(\mathbf{x}_{\text{cal}},\mathbf{y}_{\text{cal}})$ 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.

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:

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

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. 2022-XXXX C.

where μ_x and μ_y are mean values for the sets $\mathbf{x}$ and $\mathbf{y}$, 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] and the AD statistic [3] quantify 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. For the KS test, 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 as KS-X), $\mathbf{y}_1$ and $\mathbf{y}_2$ (denoted as KS-Y), $\mathbf{z}_1$ and $\mathbf{z}_2$, where $\mathbf{z} = \{x_1,x_2,...,x_n,y_1,y_2,...,y_n\}$ is the concatenated set of all quadrature measurements (denoted as KS-XY). For the AD test, we use a version developed in [9] for multiple (two or more) samples, and employ 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 samples: $\mathbf{x}_1$ and $\mathbf{x}_2$ (denoted 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.

In what follows, we use a convention in which values of V_A, V_{el}, ε_{ch}, and ε_{in} are all measured in shot noise units (SNU). For simplicity, we omit "SNU" when citing values of these quantities.

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. 2022-XXXX C.

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 SNU of excess noise (i.e., $\varepsilon_{\text{in}} = 1$). 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 FOQS parameters. In all simulations, we set $V_{\text{el}} = 0.01$.

Figure 5 shows FPR values obtained in Case 1 versus the sample size n_1 (with $n_2 = 0.9n_1$) and FNR values obtained in Case 2 versus the additional excess noise due to the intruder, ε_{in}. 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.

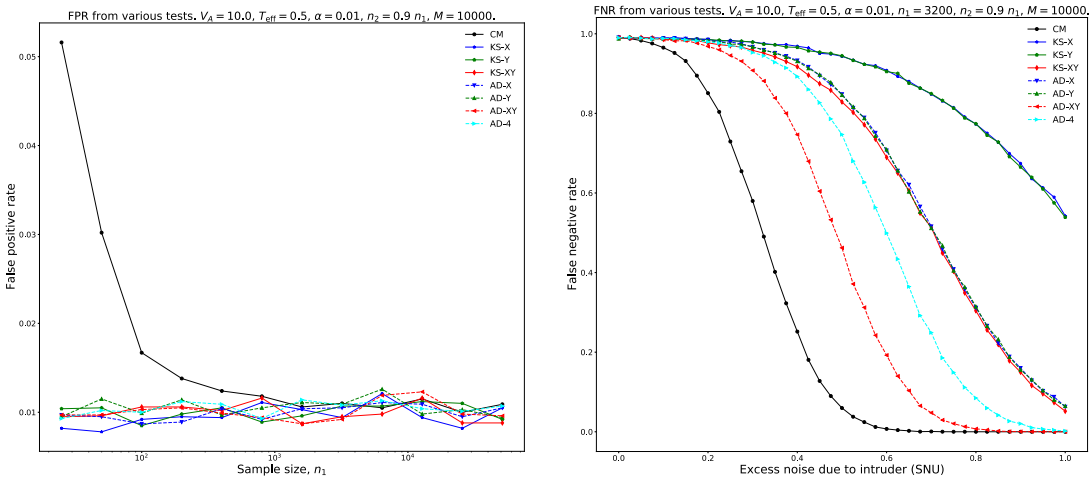

Figure 5. Performance comparison of different statistical tests, including the CM test and various variants of KS and AD tests. (left) FPR values obtained from 10000 trials in Case 1, versus n_1,and (right) FNR values for $n_1 = 3200$ obtained from 10000 trials in Case 2, versus ε_{in}. In both plots, FOQS parameter values are $V_A = 10.0, T_{eff} = 0.5, \alpha = 0.01, n_2 = 0.9n_1, \varepsilon_{ch} = 0.01$.

Based on the performed analysis, the CM test achieves much lower FNR values compared to other tests whose performance we studied, and therefore it should be used in practice (except in the regime when the sample size is small, $n_1 < 1000$, which should be avoided). We also studied the FNR obtained in Case 2 using the CM test in more detail, focusing on the effects of various FOQS parameters. Based on this analysis, we can choose sensible values for these parameters. 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. Therefore, it is advisable: (1) maximizing detector efficiency and minimizing channel loss in order to achieve $T_{\text{eff}} \geq 0.5$; (2) for $T_{\text{eff}} \approx 0.5$ keeping V_A at values about 10 (larger V_A values can be used if T_{eff} is closer to 1); (3) decreasing existing excess noise in the channel to the level of $\varepsilon_{\text{ch}} \leq 0.1$; (4) keeping sample size for calibration session at $n_1 \geq 3000$ and sample size for monitoring session at $n_2 \geq 0.5n_1$.

The analysis above assumed that, in the absence of tampering, both samples arise *from the same normal distribution*. However, in reality, due to experimental imperfections, *two distributions*

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. 2022-XXXX C.

will not be exactly the same. We incorporated experimental imperfections using a model, in which the actual value of V_A in every session differs from its nominal value due to the presence of random fluctuations. Specifically, for the *i*th session, the sample of random numbers $(\mathbf{x}_i,\mathbf{y}_i)$ comes from the normal distribution $\mathcal{N}(0,\sigma_i^2)$, where $\sigma_i = \sqrt{V_{\rm diff}(\varepsilon_i)}$, $V_{\rm diff}(\varepsilon_i) = V_A + T\eta$ $(V_A + 1 + \xi(\varepsilon_i)) - 2\sqrt{T\eta}V_A$, $V_A = V_A^{(0)}(1+\zeta)^2$, where $V_A^{(0)}$ is the nominal value of V_A, and ζ is a random variable, whose value comes from the normal distribution $\mathcal{N}\left(0,\sigma_{\rm noise}^2\right)$. FPR and FNR values now depend on how large is the noise variance $\sigma_{\rm noise}^2$ (in the *ideal case*, $\sigma_{\rm noise}^2 = 0$, we recover previous results). For example, the noise standard deviation value $\sigma_{\rm noise} = 0.01$ can be thought of as causing 1% spread in the values of $\sqrt{V_A}$, and so on.

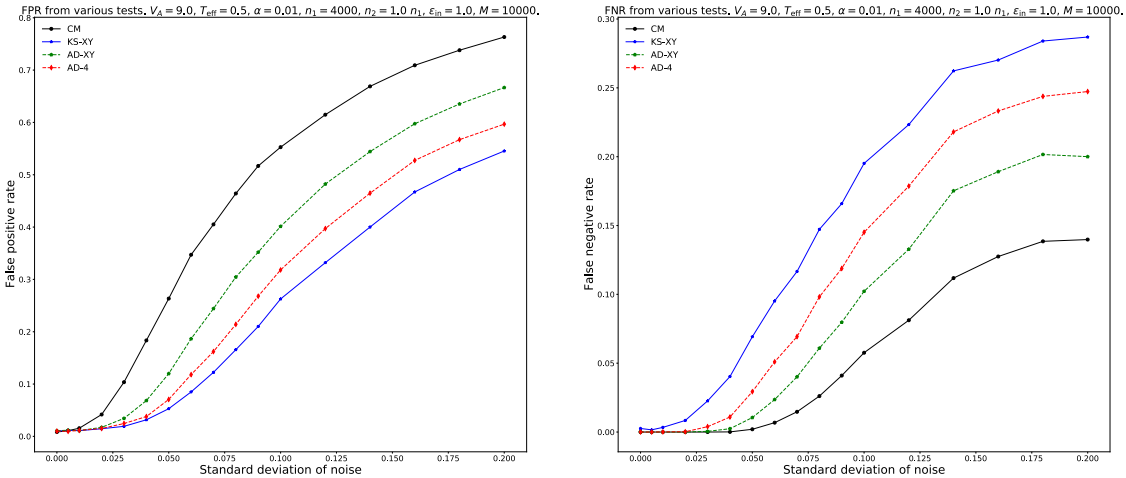

Figure 6. Performance comparison of CM, KS-XY, AD-XY, and AD-4 tests, for simulations of the FOQS model with experimental imperfections. FPR values (left) and FNR values (right) obtained from 10000 trials in Case 1 and Case 2, respectively, versus σ_{noise}. *In both plots, FOQS parameter values are* $V_A = 9.0, T_{eff} = 0.5, \alpha = 0.01,\ n_1 = n_2 = 4000, \varepsilon_{in} = 1.0, \varepsilon_{ch} = 0.01$.

Figure 6 shows FPR and FNR vs $\sigma_{\rm noise}$, for different statistical tests. The smaller is $V_A^{(0)}$, the larger is the interval of $\sigma_{\rm noise}$ values over which the FPR stays at FPR $\approx \alpha$. Since the CM test is most sensitive one, it exhibits the largest increase of FPR due to V_A fluctuations. The smaller is $V_A^{(0)}$, the larger is the interval of $\sigma_{\rm noise}$ values over which the FNR stays at FNR $= 0$. Since the CM test is most sensitive one, it exhibits the smallest increase of FNR due to V_A fluctuations.

ANALYSIS OF EXPERIMENTAL DATA

We developed software tools for automated analysis of experimental data. Analyses have been performed for two types of experiments:

Type 1: Experiments with no excess noise added, $\varepsilon_{\rm in} = 0$, in any of the sessions, to simulate normal FOQS operation in the absence of tampering. These data are used to estimate the FPR. We refer to a set of sessions that includes one calibration session and a number of monitoring sessions (compared against that calibration session) as a *session-set*.

Type 2: Experiments with some excess noise added, $\varepsilon_{\rm in} > 0$, in monitoring sessions, to simulate FOQS operation in the presence of tampering. These data are used to estimate the FNR as a function of the variance of the added noise, $V_{\rm n} \equiv \varepsilon_{\rm in}$. For this type, a session-set consists of one calibration session with $V_{\rm n} = 0$ and a number of monitoring sessions with $V_{\rm n} > 0$.

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. 2022-XXXX C.

Since an intruder with perfect capabilities can always keep $\langle X \rangle$ and $\langle Y \rangle$ values unchanged, we subtract mean values from experimental samples of Q_A,P_A,Q_B, and P_B values for each session, in order to keep $\langle X \rangle = \langle Y \rangle = 0$. This enables us to eliminate the effect of experimental jitter in $\langle X \rangle$ and $\langle Y \rangle$ values, without providing any information to the intruder that they would not already have in the ideal case.

Experiments in dataset	Sessions per experiment	Total number of sessions in dataset	FPR for different session-set sizes		
			5	10	20
6-17	20	240	0.0052	0.0046	0.0088
21-40	20	400	0.0188	0.0167	0.0105

Table 1. FPR values obtained using the CM test with $\alpha = 0.01$ from two experimental datasets of Type 1 with $n_1 = n_2 = 3200$ and $\sqrt{V_A} = 3.0$. Each experiment includes 20 sessions which can be divided into session-sets of different size: four session-sets of size 5; two session-sets of size 10; one session-set of size 20.

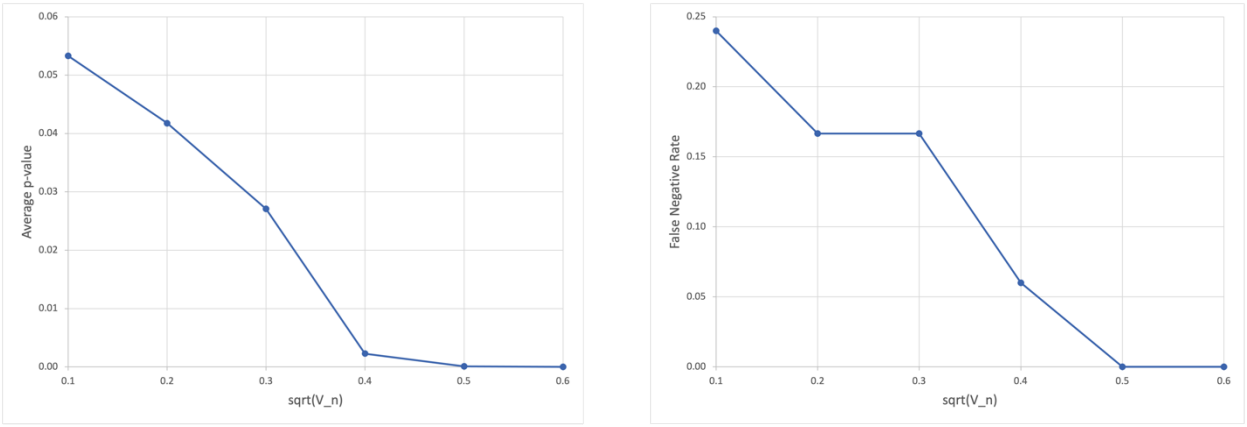

Figure 7. Average p-values (left) and FNR values (right), plotted versus $\sqrt{V_n}$, obtained using the CM test with $\alpha = 0.01$ from an experimental dataset of Type 2 with 150 session-sets, $n_1 = n_2 = 4000$, and $\sqrt{V_A} = 3.0$. Each session-set consists of one calibration session with $V_n = 0$ and six monitoring sessions with $\sqrt{V_n} = 0.1,\ldots,0.6$.

Table 1 shows FPR values obtained using the CM test with $\alpha = 0.01$ from two experimental datasets of Type 1. These FPR values are on the order of α, which is in a good agreement with theoretical predictions, given statistical errors of FPR estimation from a small sample of values (from 12 to 80 values, depending on the session-set size). Figure 7 shows average p-values and FNR values plotted versus $\sqrt{\mathrm{V_n}}$, obtained using the CM test with $\alpha = 0.01$ from an experimental dataset of Type 2 with 150 session-sets. Importantly, we observe FNR $= 0$ for $\sqrt{\mathrm{V_n}} \geq 0.5$. This combination of results show conclusive tamper-state determination in the sub-shot-noise regime using the quantitative hypothesis-test for FOQS.

CONCLUSIONS

A proof-of-concept fiber-optic quantum seal has been developed and demonstrated. Implementation effort for system control and stability has established high-fidelity encoding of

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. 2022-XXXX C.

coherent states as quantum probes and shot-noise level resolution of probe quadratures. These capabilities enabled detection of tamper-induced excess noise changes below a shot noise unit. The resulting seal sensitivity has significant impact on seal performance as the sophisticated man-in-the-middle data falsification attack becomes detectable.

We have developed a theoretical model of the FOQS employing weak coherent states of light. A tampering attempt results in added excess noise in the channel, which is detected by using statistical hypothesis testing. We have performed a numerical analysis to quantify the FOQS performance with different statistical tests and sensitivity with respect to various practical parameters. We have also extended the numerical analysis to include the effect of experimental imperfections (random fluctuations of V_A). We have developed software tools for automated analysis of experimental data. The capability to perform on-line analysis of measured data is critical for transforming the experimental FOQS system into a practical tool. The performed analysis of experimental data is a proof-of-principle demonstration of this capability.

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.

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

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. 2022-XXXX C.