SAND2016-9501PE

SECANT QKD Grand Challenge

Sandia Enabled Communications and Authentication Network using Quantum Key Distribution

Maturing continuous variable QKD and New Ideas

Scott Bisson, Constantin Brif, David Farley, Matthew Grace, Howard Poston, Mohan Sarovar, Daniel Soh

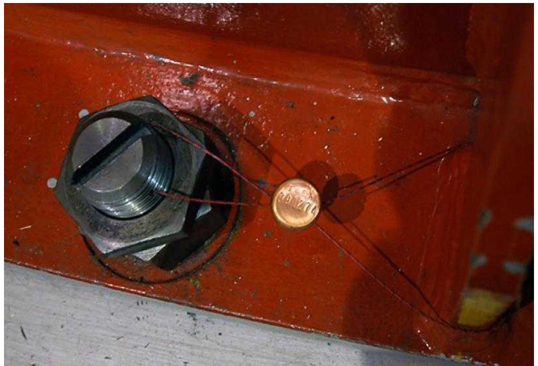
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

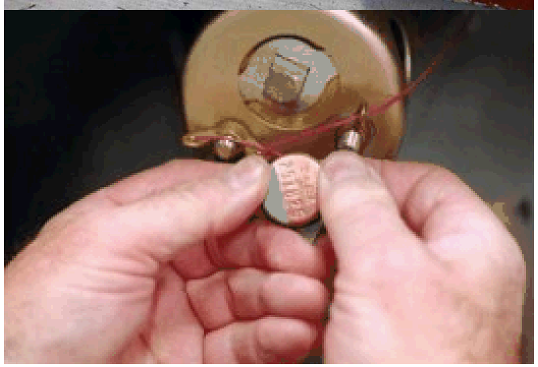
Talk outline

1. On-chip realization of CV-QKD hardware
2. Quantum seal development
3. New Ideas and application of the quantum silicon photonics toolbox
4. Objectives, milestones, deliverables

Quantum seal development

Secure seals





Seals are an important tool for nuclear non-proliferation safeguards (IAEA)

Physical seal (made from plastic, steel etc.). [Picture from Acme seals]

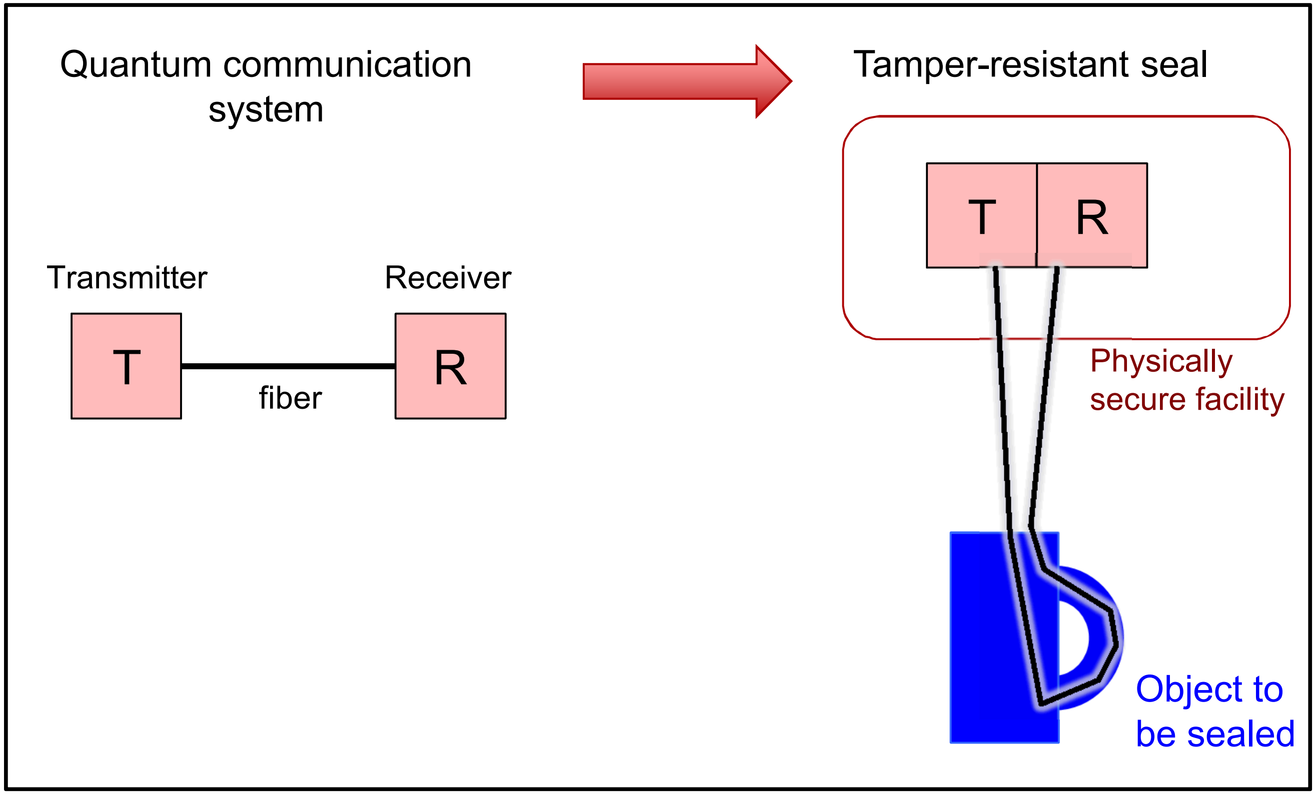
Metal seal with insulating wire (Cobra seal)

Fiber optic seals [Picture from Canberra Industries]

But these seals simply measure light intensity and compare against a fiducial value.

Vulnerable to duplication of laser source and adiabatic tapering in of counterfeit source.

QKD-enabled optical seals



- Calibrate seal (loss, noise, covariance matrix) upon installation.
- QKD performed up to channel estimation. No error correction or production of key necessary.
- Alice and Bob right next to each other, so no classical "communication" necessary

QKD provides:

1. Source authentication
2. Channel integrity testing

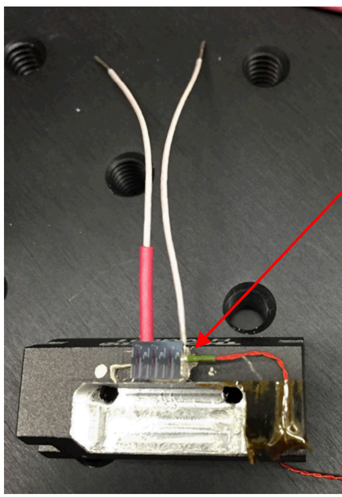
Provides security against a wider range of attacks/tamper modes

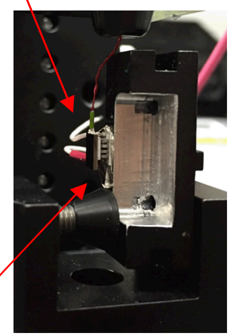
Will focus on CV-QKD-based implementations

Hardware: towards long-term stability

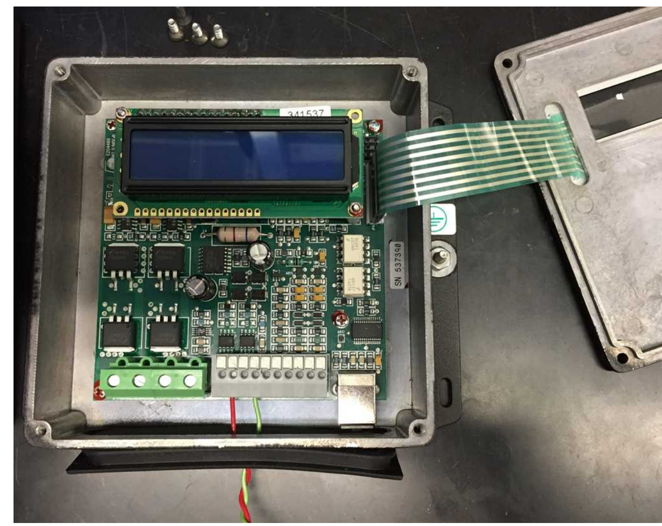
New mount for feedback stabilized temperature control

Thermistor





TE cooler



PID controller

Sensitivity analysis

A completely general framework for understanding what information about the channel parameters we can obtain from measurement is given by the Cramer-Rao lower bound:

Given data $X_1, ...X_N$, i.i.d. drawn according to a parameterized distribution $p(x|\theta)$,

$$\mathrm{cov} T_\theta(X_1, ...X_N) \geq \frac{F(\theta)^{-1}}{N}$$

Fisher information matrix

Covariance matrix for any estimator of θ

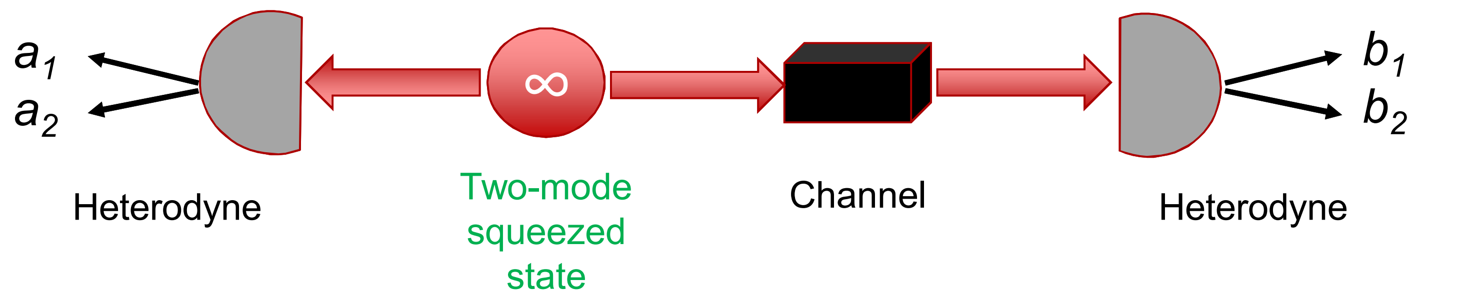
$$F(\theta)_{ij} = \int dx p(x|\theta) \frac{\partial \ln p(x|\theta)}{\partial \theta_i} \frac{\partial \ln p(x|\theta)}{\partial \theta_j}$$

Quantifies the influence each of the parameters have on the measurement outcomes. This in turn dictates how estimable the parameters are from the measurements.

What is $p(x|\theta)$ for the seal concept?

Sensitivity analysis

In the entanglement-based picture,



Assume the channel is a passive Gaussian channel characterized by T and ε. Then:

$$p(a_1, a_2, b_1, b_2) = \frac{1}{(2\pi)^2\sqrt{\det \Lambda}} \exp\left[-\frac{1}{2}A^{\mathsf{T}}\Lambda^{-1}A\right] \qquad A = (a_1, a_2, b_1, b_2)^{\mathsf{T}}$$

$$\Lambda = \begin{bmatrix} V+1+\sigma^2 & 0 & \frac{C}{2} & 0 \\ 0 & V+1+\sigma^2 & 0 & -\frac{C}{2} \\ \frac{C}{2} & 0 & T(V+\chi)+1+\sigma^2 & 0 \\ 0 & -\frac{C}{2} & 0 & T(V+\chi)+1+\sigma^2 \end{bmatrix}$$

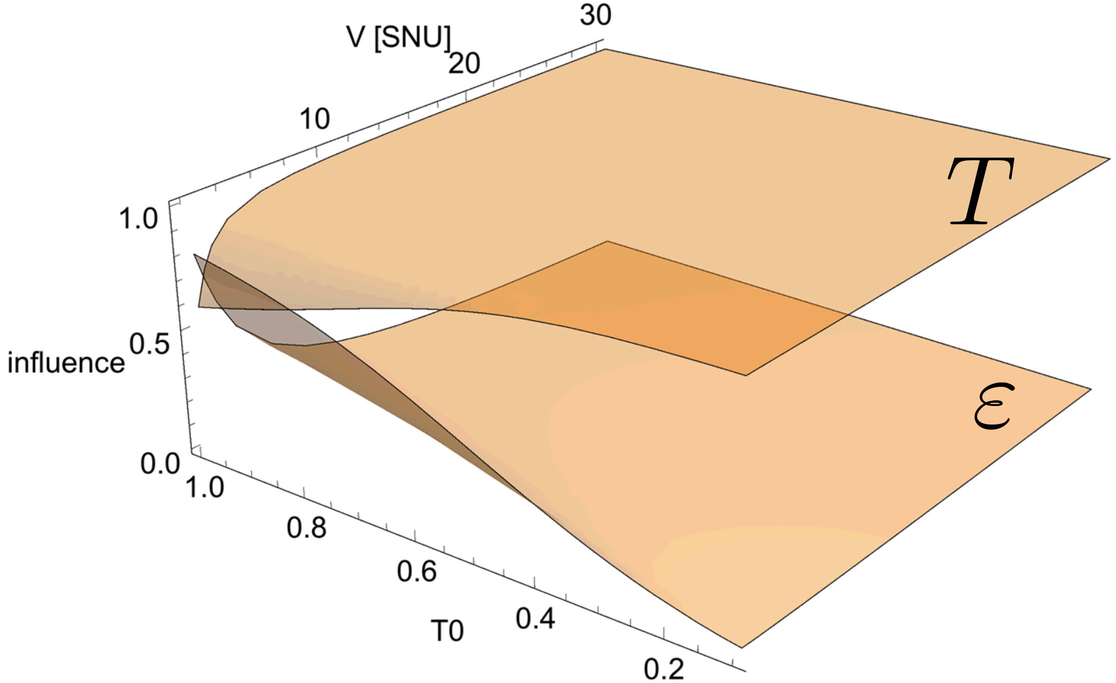
$$V = V_A + 1$$

$$C = \sqrt{T(V^2-1)}$$

$$\chi = \frac{1-T}{T} + \varepsilon$$

Sensitivity analysis

Sandia National Laboratories



- Excess noise has a large influence only when the modulation variance is small and the channel transmission is high
- Channel transmission has the most influence in the opposite regime
- Fundamental tradeoff between estimating these two parameters

Hypothesis testing framework

Sandia National Laboratories

Tamper detection formalized within a hypothesis testing framework

$\mathcal{H}_0$: Data is consistent with calibration run

$\mathcal{H}_1$: Data is inconsistent with calibration run

Require data processing protocol to perform this hypothesis test :

1. With as few assumptions on the data generating distribution as possible
2. In real-time, using simple arithmetic operations (ideally, FPGA implementable)
3. With as little data as possible

Hypothesis testing framework

What is the data in CV-QKD (with homodyne measurements)?

$$(\mathbf{d}_1, ...\mathbf{d}_N) = \left(\begin{pmatrix} d_A \\ d_B \end{pmatrix}_1, ... \begin{pmatrix} d_A \\ d_B \end{pmatrix}_N \right)$$

Two continuous random variables per pulse

Simple statistics we can calculate about this data:

$$\bar{d}_i = \frac{1}{N} \sum_{k=1}^{N} d_i$$

Sample means

$$S = \frac{1}{N-1} \sum_{k=1}^{N} (\mathbf{d} - \bar{\mathbf{d}})(\mathbf{d} - \bar{\mathbf{d}})^{\mathsf{T}}$$

$$= \begin{bmatrix} \sigma_A^2 & \sigma_{AB} \\ \sigma_{AB} & \sigma_B^2 \end{bmatrix}$$

Sample covariance matrix

Collect these into the vector:

$$\theta = (\bar{d}_A, \bar{d}_B, \sigma_A, \rho_{AB}, \sigma_B)^{\mathsf{T}}$$

Hypothesis testing framework

Now we can formalize the hypothesis test

$$\mathcal{H}_0 : \hat{\delta} = 0$$
$$\mathcal{H}_1 : \hat{\delta} \neq 0$$

$$\hat{\delta} = \theta - \theta_0$$

Test statistic:

$$\chi^2 = \hat{\delta}^\mathsf{T} \Sigma_{\hat{\delta}}^{-1} \hat{\delta}$$

Sullivan *et al.*, J. Quality Tech., **39** 66 (2007)

If we use maximum likelihood estimates for elements of δ, this test statistic is asymptotically chi-square distributed with 5 degrees of freedom.

Therefore can use this test statistic to bound hypothesis testing error probabilities, *e.g.*

$$p(\chi^2) < 0.01 \implies \text{reject } \mathcal{H}_0$$

Hypothesis testing framework

Now we can formalize the hypothesis test

$$\mathcal{H}_0 : \hat{\delta} = 0$$
$$\mathcal{H}_1 : \hat{\delta} \neq 0$$

$$\hat{\delta} = \theta - \theta_0$$

Test statistic:

$$\chi^2 = \hat{\delta}^\mathsf{T} \Sigma_{\hat{\delta}}^{-1} \hat{\delta}$$

Sullivan *et al.*, J. Quality Tech., **39** 66 (2007)

Notes:

$\Sigma_{\hat{\delta}}$ is difficult to calculate directly, so we will use an approximation to it based on the Cramer-Rao bound.

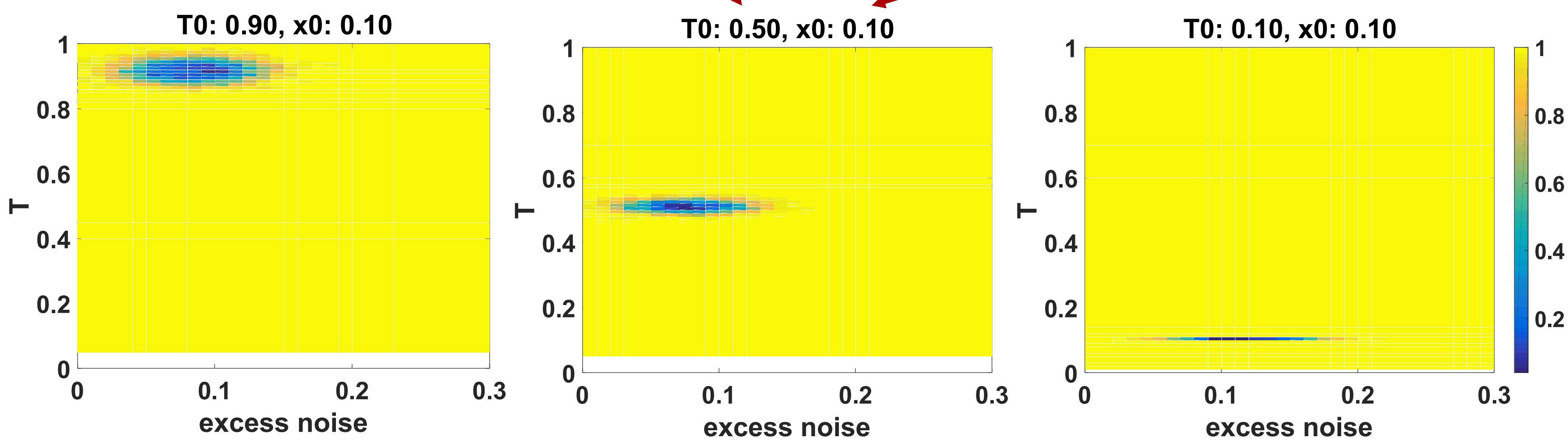
No assumptions on data until now. This last approximation assumes the data collected under the calibration run is from a Gaussian channel.

Hypothesis testing framework

Probability of rejecting null hypothesis (detecting tampering)

Simulated data (N = 10,000, V_a = 30 SNUs) under a passive Gaussian channel.

Calibrated, nominal value of transmission and excess noise



- Test is very sensitive to changes in channel transmission, especially at low transmission.
- Less sensitive to excess noise in this parameter regime (requires lower V_a).
- Improve test to have greater power – achieve good rejection with smaller N.