Detecting nonlocal correlated errors: Bob gets caught faking a Bell-inequality violation

M. E. Feldman[1], G. K. Juul[1], S. J. van Enk[2], M. Beck[1,*]
[1]*Department of Physics, Whitman College, Walla Walla, Washington 99362, USA*
[2]*Department of Physics, University of Oregon, Eugene, Oregon 97403, USA*
* *beckmk@whitman.edu*

Abstract: We demonstrate that loop state-preparation-and-measurement tomography is capable of detecting nonlocal correlated errors by catching Bob as he tries to fake a Bell-inequality violation while using nonlocal knowledge of Alice's measurement settings.
OCIS codes: (270.5585) Quantum information and processing; (270.0270) Quantum optics; (200.0200) Optics in computing.

1. Introduction

One technique for Alice and Bob to secure their communications is to share a quantum key that is derived from a pair of entangled particles. To demonstrate that their key is secure they can verify that their measurements satisfy a Bell inequality; this is the basis of device independent QKD. However, it is possible to exploit experimental loopholes and "fake" a Bell inequality violation [1]. For example, if Bob has nonlocal information about Alice's detector settings he can modify his settings to make her believe that their particles violate a Bell inequality.

Loop state-preparation-and-measurement (SPAM) tomography is a technique for detecting correlated errors between state preparations and measurements [2-4], without needing information about the states or the measurements (other than the dimensions of their Hilbert spaces). It has been shown theoretically that loop SPAM tomography is capable of detecting nonlocal correlated measurement errors [3], and here we perform experiments demonstrating that this is the case. We prepare entangled photon pairs in states that approximate Werner states; the states we create are not capable of violating the Clauser-Horne-Shimony-Holt (CHSH) inequality $S<2$. Bob cheats by managing to have nonlocal knowledge of Alice's detector settings, and he modifies his settings in order to create measurements that yield $S>2$. However, Alice performs loop SPAM tomography in order to catch Bob's fakery.

2. Theory

An unbiased detector that measures polarization is described by a positive-operator-value-measure (POVM) that has $n=3$ independent parameters, and we can construct Hermitian operators (linear combinations of POVMs) that correspond to polarization measurements that also are described by three independent parameters. Let Alice's measurement operators be denoted by $\hat{A}_i$, where *i* labels the different measurement settings that Alice can choose. Similarly denote Bob's measurement operators by $\hat{B}_j$. If Alice and Bob have a source of photon pairs that is described by the density operator $\hat{\rho}$, the expectation value for a joint measurement is given by

$$E_{ij} = \mathrm{Tr}\left[\hat{\rho}\left(\hat{A}_i \otimes \hat{B}_j\right)\right] \ . \tag{1}$$

Assume that $\hat{\rho}$ is held constant during the measurements, and consider the E_{ij}'s to be elements of a matrix $\overline{E}$. The rows of $\overline{E}$ refer to a fixed measurement for Alice $\hat{A}_i$, while the columns refer to a fixed measurement for Bob $\hat{B}_j$. The largest $\overline{E}$ that will consist entirely of independent elements is 3x3.

Consider the case where Alice and Bob make an over-complete set of measurements. Alice makes measurements with $2n=6$ different detector settings and so does Bob. The 6x6 matrix of expectation values $\overline{E}$ can be partitioned into corners consisting of 3x3 matrices as follows

$$\overline{E} = \begin{pmatrix} \overline{A} & \overline{B} \\ \overline{C} & \overline{D} \end{pmatrix} \ . \tag{2}$$

The *n*x*n* corner matrix $\overline{A}$ consists of independent measurements, but the other corners cannot be independent. For example, matrix $\overline{A}$ is connected to matrix $\overline{B}$ in the sense that they share a common set of Alice's measurements, and the measured matrix elements of $\overline{B}$ must be consistent with that fact.

Define the partial determinant of $\overline{E}$ as $\Delta\left(\overline{E}\right) \equiv \overline{A}^{-1}\overline{B}\overline{D}^{-1}\overline{C}$. It can be shown that the measured data are internally consistent as described above, and free of correlated SPAM errors, under the condition that $\Delta\left(\overline{E}\right) = \overline{1}$, where $\overline{1}$ is the 3x3 identity matrix [2,3]. No knowledge of the detector settings is necessary to make this determination. If Bob has nonlocal knowledge of Alice's detector settings, and uses that knowledge to change his detector settings to achieve a desired outcome, he will create a correlated error. Thus, to determine if Bob cheats we construct the matrix of expectation values $\overline{E}$ as given in Eq. (2), and then calculate the partial determinant $\Delta\left(\overline{E}\right)$. If $\Delta\left(\overline{E}\right) - \overline{1} \neq 0$, to within the statistical errors of the measurements, then Bob's fakery has been detected. Furthermore, it is not necessary to use the full $2n = 6$ settings. Alice and Bob can each make $n+1 = 4$ measurements, and embed these measurements into a 6x6 matrix [2,4].

3. Experiments

We use parametric down conversion in a two-crystal geometry to produce polarization-entangled photons in the Bell state $\left|\Phi^{+}\right\rangle = 1/\sqrt{2}\left(\left|HH\right\rangle + \left|VV\right\rangle\right)$. We also use LEDs to illuminate our detectors with photons that produce an uncorrelated, randomly polarized background. The combination of $\left|\Phi^{+}\right\rangle$ and background produces a detected state that approximates a Werner state. The uncorrelated background makes up approximately 1/3 of the total detected coincidences, creating a state that is incapable of violating the CHSH inequality [5].

If Bob does not cheat, he and Alice measure $S = 1.659 \pm 0.018$, which does not violate the CHSH inequality; measurements of $\Delta\left(\overline{E}\right)$ indicate that there are no correlated errors. However, if Bob uses nonlocal knowledge of Alice's measurement settings to adjust his own settings, the measurements yield $S = 2.312 \pm 0.014$, which violates the CHSH inequality by 22 standard deviations. In Fig. 1(a) we show the mean and standard deviation of $\Delta\left(\overline{E}\right) - \overline{1}$ and the ratio of these two quantities; we see that $\Delta\left(\overline{E}\right) - \overline{1}$ differs from 0 by 16 standard deviations [Fig. 1(c)] and Bob's treachery is detected. This is possible because loop SPAM tomography works without information about either the states or the measurements, so Alice doesn't have to trust the settings that Bob reports to her.

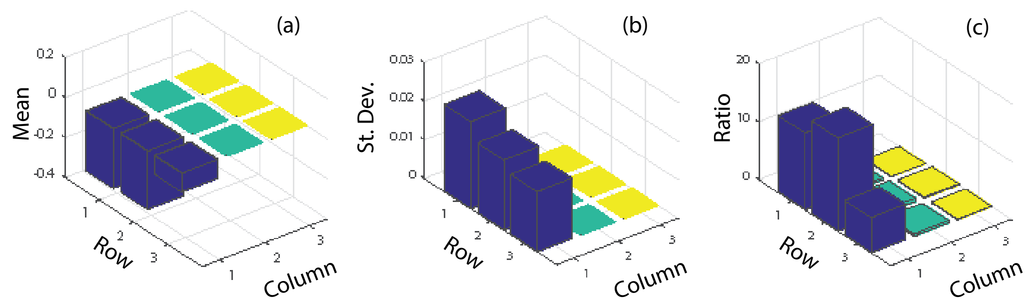

Fig. 1. (a) the mean of $\Delta\left(\overline{E}\right) - \overline{1}$, (b) the standard deviation of $\Delta\left(\overline{E}\right) - \overline{1}$, and (c) the absolute value of the ratio of these two quantities (mean divided by standard deviation).

Acknowledgements: This project was funded by NSF (1719390) and ARO (W911NF-14-C-0048).

4. References

[1] I. Gerhardt et al., "Experimentally Faking the Violation of Bell's Inequalities," Phys. Rev. Lett. **107**, 170404 (2011).

[2] C. Jackson and S. J. van Enk, "Detecting correlated errors in state-preparation-and-measurement tomography," Phys. Rev. A **92**, 042312 (2015).

[3] C. Jackson and S. J. van Enk, "Nonholonomic tomography. II. Detecting correlations in multiqudit systems," Phys. Rev. A **95**, 052328 (2017).

[4] A. F. McCormick, S. J. van Enk, and M. Beck, "Experimental demonstration of loop state-preparation-and-measurement tomography," Phys. Rev. A **95**, 042329 (2017).

[5] R. Horodecki, P. Horodecki, and M. Horodecki, "Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition," Phys. Lett. A **200**, 340-344 (1995).