Arts & Sciences / PHYSICS

Preparing Indistinguishable States for a Prepare-and-Measure BB84 Polarization-Based Decoy State QKD Protocol Using Three FPGA-Driven LEDs

Daniel Sanchez-Rosales, Roderick D. Cochran, Daniel J. Gauthier

INTRODUCTION

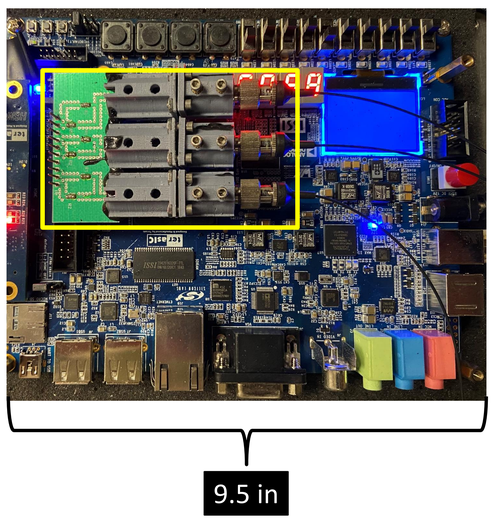
Quantum key distribution (QKD) systems provide a method for two users to exchange a provably secure key.

- In prepare-and-measure QKD protocols, the indistinguishability of states is an important aspect for preventing side-channel attacks.
- We use a prepare-and-measure three-state BB84 [1] polarization-based decoy state protocol.
- Our system is designed to operate under size, weight, and power (SWaP) restrictions such as that needed for drone-based QKD.
- The Decoy-State protocol allows us to use imperfect sources and still guarantee secure communication [2].
- Using 3 states achieves the same secure key rate as 4 states [3, 4].

Setup

- We use three separate LEDs, driven by an FPGA, that go through different optical paths that set the state of polarization (left-circular, right-circular, or horizontal).
- Each LED is connected to two GPIO pins via a different resistive path.
- Using only 3 LEDs we send 3 signal states, 3 decoy states, and a vacuum state,

Figure 1, Actual LED-FPGA Setup.



METHODS & RESULTS

Information is encoded using the polarization degree of freedom of the photon. All other degrees of freedom (spatial, spectral, and temporal) need to be indistinguishable for all states.

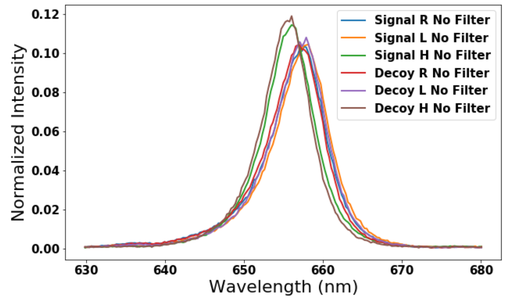
Spatial Indistinguishability

- By coupling all three optical paths into the same single mode fiber, spatial indistinguishability is guaranteed.
- While our fiber is not polarization-preserving, the transformation is unitary and can corrected for using waveplates.

Spectral Indistinguishability

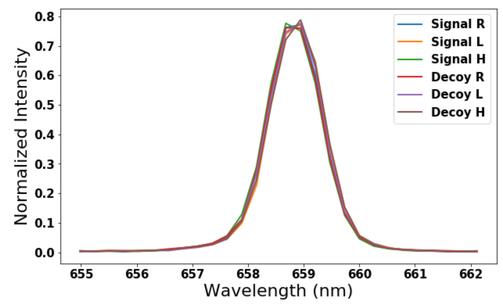
- The spectra from the three LEDs is broad (~12 nm) and they are partially distinguishable (78% overlap), as shown in Figure 2.

Figure 2, Unfiltered LED Spectra.



- By passing the optical pulses through a 1 nm narrow-band filter (Andover 656FS02-12.5), the overlap is drastically improved to 94.6%. The results are shown in Figure 3.

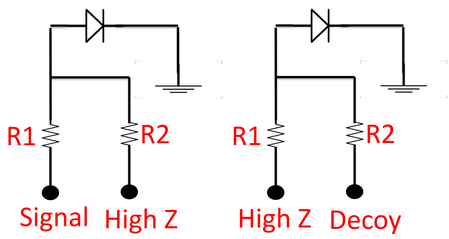
Figure 3, Filtered LED Spectra.



Temporal Indistinguishability

- We use dynamic shifting of the FPGA phase-locked-loops to control the phase and the width of the electrical pulses that drive the LEDs
- This allows us to control the optical pulses produced by the LEDs with a resolution of 250 ps.
- Signal and decoy states are of different intensity. We send decoy and signal pulses through different resistive paths, as shown in Figure 4.
- The difference in resistive paths for signal and decoy causes timing differences in the optical pulses due to non-linear LED current response.

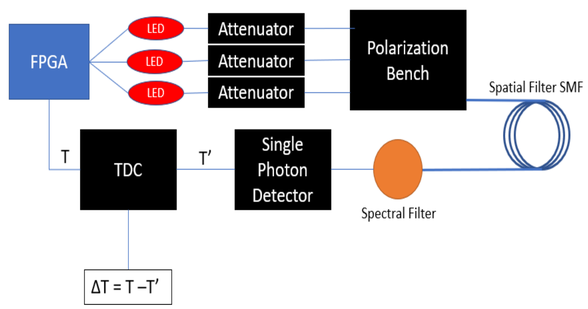
Figure 4, Electrical paths for signal and decoy.



Measuring temporal indistinguishability:

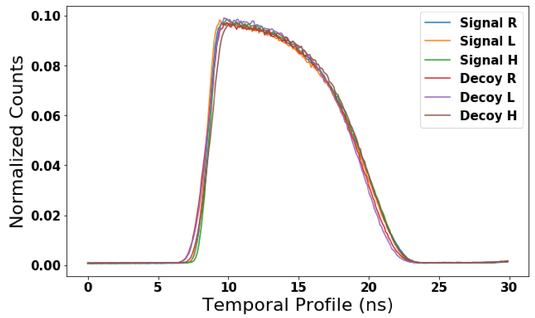
- We drive a single LED with a 10 ns wide electrical signal at a repetition rate of 12.5 MHz.
- The resulting photonic wavepacket is measured by a single-photon detector whose electrical output is measured by a time-to-digital converter and histogrammed. This setup is shown in Figure 5.

Figure 5, Experimental setup to quantify temporal indistinguishability



The resulting adjusted temporal waveforms are 97.1% overlapped. These are shown in Figure 6.

Figure 6, Temporal Waveforms for all 6 states.



CONCLUSIONS

Using a spatial filter single-mode fiber, a narrow-band spectral filter, and dynamic shifting of the FPGA phase-locked-loops, we can make the spatial, spectral, and temporal degrees of freedom of our quantum states indistinguishable. We are able to achieve 94.6% and 97.1% overlap in the spectral and temporal waveforms, respectively, with an overall indistinguishability of 91.9%.

E-mail **sanchez-rosales.1@osu.edu**
Physics Research Building
191 W Woodruff Ave, Columbus, OH 43210

BIBLIOGRAPHY

1 Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. Theor. Comput. Sci. 2014, 560, 7–11. doi:10.1016/j.tcs.2014.05.025
2 Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. Phys. Rev. Lett. 2005, 94, 230504. doi:10.1103/PhysRevLett.94.230504..
3 Islam, N.T.; Lim, C.C.W.; Cahall, C.; Kim, J.; Gauthier, D.J. Securing quantum key distribution systems using fewer states. Phys. Rev. A 2018, 97, 042347. doi:10.1103/PhysRevA.97.042347.
4 Tamaki, K.; Curty, M.; Kato, G.; Lo, H.K.; Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. Phys. Rev. A 2014, 90, 052314. doi:10.1103/PhysRevA.90.052314.

ACKNOWLEDGEMENTS

This material is based on research sponsored by NASA under grant 80NSSC20K0629 and the Air Force Research Laboratory and the Southwestern Council for Higher Education under agreement FA8650-19-2-9300. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of NASA, the Southwestern Council for Higher Education and the Air Force Research Laboratory (AFRL), or the U.S. Government.

THE OHIO STATE UNIVERSITY