WG4 (Contributed Oral)
9:45 AM – 10:00 AM

Tamper-Indicating Quantum Optical Seals

Travis S. Humble, D. Duncan Earl, and Brian P. Williams
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831
Email: humblets@ornl.gov

***Abstract*—We demonstrate a quantum optical seal using entangled photons to monitor the integrity of a fiber-optic channel subject to tampering. This application of quantum photonics provides a basis for physical layer security in cyber-physical systems.**

I. Introduction

Tamper-indicating optical seals are widely used for verifying the integrity of enclosed systems, including storage containers, physical perimeters, and fiber networks [1], [4], [7], [9]. These optical seals operate by confirming transmission of an encoded light pulse from source to receiver, where tampering is indicated by either the absence of light or an error in the received encoding. In the classical setting, detection of tampering requires failure of the intruder to accurately replicate the original transmission. However, if the attacker perfectly replicates the classical light, e.g., using either an optical repeater or *a priori* knowledge, then the classical variant of an optical seal is vulnerable to an intercept-resend spoofing attack.

By contrast, Wootters and Zurek [10] and Dieks [2] have shown that cloning quantum information is prohibited by the linearity of quantum mechanics. Attempts to clone quantum information, even optimally, necessarily introduce noise into the resulting state and its subsequent observables [8]. These guarantees of the no-cloning theorem are well known from quantum key distribution, in which the non-local correlations inherent to quantum states are used to establish correlated measurements outcomes between users [3].

In this contribution, we demonstrate that the intercept-resend vulnerability for classical optical seals can be closed by using quantum light sources to monitor the continuity of the optical channel. Building on initial efforts [6], this work demonstrates detection of tampering on a fiber optic link by monitoring quantum correlations. Our experimental system uses time-bin entanglement between a pair of photons to monitor the continuity of an active fiber link. We employ the visibility as an indicator of tampering and provide a simple example of how it may be applied.

II. Theoretical Model

In our quantum optical seal, a quantum light source generates a pair of time-bin entangled photons. This state is prepared using cw-pumped spontaneous parametric down-conversion (SPDC) in a nonlinear optical crystal [5]. The crystal mediates the decay of a high-energy pump photon into a pair of lower-energy photons (labeled 1 and 2) while conserving both energy and transverse momentum. We model the SPDC output using a pure-state approximation with filtering of the transverse spatial modes to define the normalized biphoton temporal state

$$|\psi_{12}\rangle = \int dt \int dt' F_{12}(t,t')\,|t_1, t_2'\rangle, \tag{1}$$

where $F_{12}(t,t')$ is the joint temporal amplitude describing correlations between the photon generation times t and t' and the temporal states are defined relative to the Fourier transform of the creation operator for a single spectral mode.

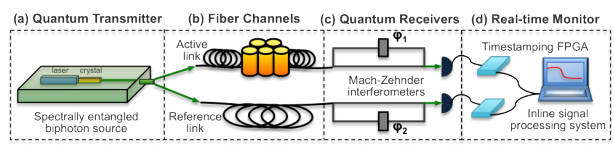

Fig. 1. A schematic of the tamper-indicating quantum optical seal showing its four major components: (a) quantum transmitter consisting of time-bin entanglement source, (b) fiber channels for both the active and reference links, (c) quantum receivers based on Mach-Zehnder interferometers and single photon detectors, and (d) real-time monitor of the visibility.

The photons 1 and 2 are next coupled into separate optical fibers, which we label the active and reference fibers, respectively. We assume the input photons are spatially mode matched with the single-mode fibers. As indicated in Fig. 1, the active fiber is exposed to potential tampering while the reference fiber is secured from tampering. In practice, these fibers take separate paths and terminate at different receivers. Consequently, the security of the reference fiber can be established, e.g., by co-locating it with the transmitter.

The interferometric receivers are composed from an interferometer and single-photon detectors. The interferometer has a short and a long path with relative time difference τ over which the photon amplitude is distributed, where in the long arm a variable phase is applied to the photon amplitude. The phase angle is denoted as φ_1 and φ_2 for the probe and reference receivers, respectively, with $\phi_{12} = \phi_1 + \phi_2$. The photon amplitudes from the long and short arms are then linearly combined. This yields the biphoton state

$$|\psi_{12}\rangle = \tfrac{1}{4}\int dt \int dt' F_{12}(t,t')\left(|t_1, t_2'\rangle + e^{i\phi_1}\,|(t+\tau)_1, t_2'\rangle + e^{i\phi_2}\,|t_1, (t'+\tau)_2\rangle + e^{i\phi_{12}}\,|(t+\tau)_1, (t'+\tau)_2\rangle\right), \tag{2}$$

The time-of-arrival of photons 1 and 2 are then measured using single-photon detectors. Only those measurements corresponding to coincidences in arrival (the first and last terms

U.S. Government work not protected by U.S. copyright

of Eq. (2)) are monitored. The correlations in arrival time for the photon pair with respect to ϕ_{12} provides a fringe depth, or visibility, that serves as an indicator of tampering. Moreover, the visibility can be used as a statistic for binary hypothesis testing, as shown previously [6]. Notably, the visibility must exceed a well-characterized quantum-classical threshold to confirm the transmission was genuine. This threshold can also be modified to account for system specific parameters including channel and detector noises.

III. Experimental Results

Our entanglement source is based on cw-pumping of type-II spontaneous parametric down-conversion (SPDC) in a nonlinear optical crystal. We pump at 405 nm in a 30-mm length PPKTP crystal which is periodically poled to phase-match the pump laser for typ-II degenerate, downconversion with colinear photon pairs at 810 nm. The orthogonal polarizations of the photons are then used to steer them each into their respective fiber links.

For experimental simplicity, each receiver was built using a Michelson interferometer as opposed to the Mach-Zehnder interferometers in Fig. 1. Incoming light is split by a 50:50 beam splitter with arm at a fixed length and the other varied using a moveable mirror stage. The returning light passes though the beam splitter and with 50% probability travels to the output port. The time-of-arrivals are then measured by single-photon detectors that trigger a coincidence unit to count the number of coincidences in each time bin. Forthcoming work replaces the coincidence unit with individual timestamping units that interface directly with an inline digitial signal processing system. An example of the measured visibility for our prototype system is shown in Fig. 2.

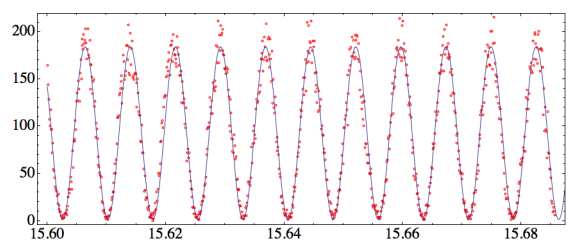

Fig. 2. Variations in temporal coincidence counts with respect to relative phase delay (mirror position) give a fitted visibility of $98.3 \pm 0.41\%$

A time series of visibility samples can be used to diagnose changes to the quantum state. Figure 3 shows a time series in which nearly constant visibility is maintained for approximately 15 minutes before the active link is blocked. The sudden loss of correlated arrivals leads to a vanishing visibility. Removal of the beam blocker returns the visibility to its nominal value, as expected. These dynamic changes are indicative of if and when tampering with the active link occurs. Current working is investigating the sensitivity to detecting more sophisticated attacks, e.g., where uncorrelated photons are intentionally injected into the active link.

In support of monitoring exisiting fiber networks, we have also investigated the development of quantum optical seals using non-polarization maintaining (PM) singlemode fibers. Visibility data for 2-meter long singlemode and multimode fiber links indicate a small reduction in visibility relative to the (PM) fiber, but the difference remains well above the quantum-classical threshold. If these results hold for slightly longer links, we believe the quantum optical seal may be useful fo monitoring the physical layer of conventional fiber networks.

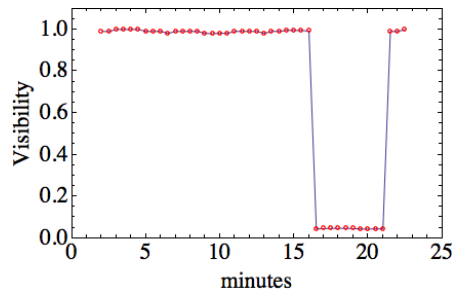

Fig. 3. A time series of the visibility demonstrating a sudden change in the when the optical beam is blocked. Comparing the measured visibility to a threshold value indicates when tampering has occurred.

IV. Conclusion

We have shown how the intercept-resend vulnerability of classical photonic seals can be closed using quantum photonics. Our reported demonstration is the first step in the detection intercept and resend attacks against a replica of a (quantum) photonic carrier. Our current efforts focus on integrating the quantum transmitters and receivers into a real-time monitoring systems that can quickly diagnose the presence of tampering in a fiber-based network. This application of quantum photonics could then be useful for monitoring the integrity of the physical layer in cyber-physical systems.

Acknowledgment

This work was supported by the Defense Threat Reduction Agency. This manuscript has been authored by UT-Battelle, LLC, under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy.

References

[1] A.A. Chtcherbakov, P.L. Swart, and S.J. Spammer, Proc. ISIE '98., vol. 1, jul 1998, pp. 267 –270.
[2] D. Dieks, Phys. Lett. A **92** (1982), 271–272.
[3] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Rev. Mod. Phys. **74** (2002), 145–195.
[4] B. Griffiths, Proceedings. Security Technology, 1995., oct 1995, pp. 325 –330.
[5] C. K. Hong and L. Mandel, Phys. Rev. A **31** (1985), 2409–2418.
[6] Travis S. Humble, Ryan S. Bennink, Warren P. Grice, and Israel J. Owens, Proc. SPIE **7342** (2009), 73402H.
[7] J.C. Juarez, E.W. Maier, Kyoo Nam Choi, and H.F. Taylor, Lightwave Technology, Journal of **23** (2005), no. 6, 2081 – 2087.
[8] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antion Acin, Rev. Mod. Phys. **77** (2005), 1225–1256.
[9] Mieczyslaw Szustakowski and Marek Zyczkowski, Proc. SPIE **5954** (2005), 59540C.
[10] W. K. Wootters and W. H. Zurek, Nature **299** (1982), 802–803.