

Viewpoint

Don't Cry over Broken Entanglement

Tim Ralph

School of Mathematics and Physics, University of Queensland, Brisbane QLD 4072, Australia

Ping Koy Lam

Department of Quantum Science, Australian National University, Canberra ACT 0200, Australia

Published July 1, 2013

A secure communication channel that relies on quantum entanglement survives despite the noisy break up of the entanglement itself.

Subject Areas: **Quantum Information****A Viewpoint on:****Entanglement's Benefit Survives an Entanglement-Breaking Channel**

Zheshen Zhang, Maria Tengner, Tian Zhong, Franco N. C. Wong, and Jeffrey H. Shapiro

Physical Review Letters **111**, 010501 2013 – Published July 1, 2013

Quantum entanglement is a special type of correlation between two objects: if two particles—say, two photons—are in an entangled state, then measuring one determines the state of the other even if they are far apart. More than a quirky feature of quantum mechanics, entanglement is the basis for many new applications. These include technologies for sending secret signals, transmitting densely coded information, and replicating a particle a long distance away (quantum teleportation.) But in these and other applications, the fact that entanglement is fragile and easily broken by environmental noise can be the limiting factor.

In *Physical Review Letters*, Zheshen Zhang and colleagues at the Massachusetts Institute of Technology, Cambridge, have now demonstrated experimentally that the benefits of entanglement can survive even when it is broken [1]. Using a technique called quantum illumination, the group established a secure channel of communication between two parties that relied on sending one of a pair of entangled photons through a noisy environment. Even though the initial entanglement didn't survive the passage, it was enough to guarantee the communicated signal was secure. The demonstration opens up the possibility that quantum communication and metrology tasks can occur in environments previously thought too noisy for entanglement to be useful.

Quantum illumination [2], which was first proposed by Seth Lloyd, is a method to enhance the probability of detecting a far away object. The problem with just shining light on a far away object and looking for any reflected photons is that little light will be reflected and any that does may be hard to see against a thermal background of light. Lloyd showed that using an entangled photon state to illuminate the object could significantly enhance

the observer's ability to distinguish the reflected light from the background. What is surprising is that this enhancement survives even when the noisy background completely destroys the entanglement in transit.

The simplest example of how this can work involves two entangled pulses of light, each containing just one photon. "Alice" (the sender) keeps one pulse and sends the other one towards her target, "Bob." When Bob sends back the pulse, Alice interferometrically recombines it with the light she kept. Here is where the difference between classical and quantum signals becomes important: With classical light, time and frequency can't both be simultaneously localized, as the Fourier transform of a pulse that is sharply localized in time is spread out over all frequencies. In contrast, if the sent and retained signals are truly entangled, they will be simultaneously strongly correlated in both arrival time and frequency. The much stronger initial correlation of the entangled beams allows reflected photons to be distinguished from background photons with a much higher signal to noise when they are "decoded" by recombining them with the retained signal. (The decoder is basically the reverse of the original entangler—a sort of "disentangler"—which only lets through the tiny residual correlation that matches the original entanglement.) Even though the entanglement doesn't survive, a classical correlation survives that is stronger than would exist in the absence of entanglement in the first place. The enhancement in signal to noise is by a factor d , where d is the number of optical modes involved in the entanglement. In this way, the presence (or absence) of an object can be determined with far less light than a classical experiment would require.

Instead of using quantum illumination to enhance a

measurement, Zhang *et al.*[1] apply the method to making a secure transmission channel, based on an idea from group leader Jeffrey Shapiro [3]. Suppose Bob controls if the object is present, while Alice has to use her entangled photons to detect it. Upon receiving one photon, Bob encodes a “1” if the object is present and a “0” if it is not. Using the quantum illumination technique, Alice’s measurement of whether Bob sent a “0” or “1” has a high signal to noise. She can therefore determine the presence or absence of the object with confidence, even with low levels of light.

The utility of this form of communication becomes clearer with the entrance of an eavesdropper, “Eve,” who can intercept light coming from Alice and reflected from Bob. Because Eve does not have access to the other half of the entangled light in Alice’s station, she doesn’t have Alice’s advantage of an enhanced signal to noise. As a result, she can’t determine the signal indicating the presence or absence of the object at Bob’s station reliably. Shapiro showed this communication scheme could be arranged such that Eve obtained virtually no information about the message.

To demonstrate Shapiro’s proposal experimentally, Zhang *et al.* used spontaneous parametric down-conversion (SPDC), a nonlinear process in which photons are converted into pairs of photons at a lower frequency, to produce Alice’s entangled state (Fig. 1). Under the right conditions, the process can produce entangled photons across a large number of optical modes. Because it’s experimentally difficult to add or remove an object, Zhang *et al.* instead have Bob either shift the phase of an arriving photon by zero degrees (a “0”) or by π (“1”). After modulating the light, Bob gets crafty: he purposely hides the photon in a thermal background by sending it through an erbium-doped fiber amplifier. The amplifier introduces a large amount of noise (from amplified spontaneous emission) onto the signal. Once this noise is introduced, the modulated photon is no longer entangled with the one Alice kept. The signal is then returned to Alice who uses a second nonlinear crystal as a “decoder” to coherently recombine the signal from Bob with the one she kept, and hence extract the string of 0s and 1s sent by Bob.

Zhang *et al.* model the effects of eavesdropping by having Eve use a beam splitter to siphon off light to and from Bob’s station. If entanglement really has a benefit, then Alice should have a much higher success rate of correctly determining Bob’s 1s and 0s than Eve. This is exactly what the authors find: They calculate from their measurements the experimental bit error rates obtained by Alice and Eve and compare them with the rates they should get if all of the components were ideal. The key result is that the observed bit error rate achieved by Alice exceeds the theoretical best bit error rate that Eve could achieve by up to five orders of magnitude. This implies that, modulo some technical requirements on the signal statistics, the eavesdropper can obtain virtually no information about the message that Bob and Alice exchange.

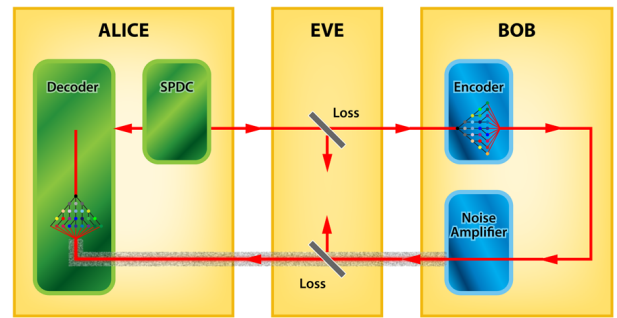


FIG. 1: Schematic showing the secure communication protocol, via photons, between Alice and Bob. Alice uses a spontaneous parametric down-converter (SPDC) to prepare two entangled photons, one of which she sends to Bob, the other of which she keeps. Bob encodes a signal on the photon he receives and sends it back, but he breaks the initial entanglement with a noise amplifier. The eavesdropper, Eve, is assumed to have access to all the transmission losses, but because she doesn’t have access to how the photons were first entangled, she can’t decode the signal as reliably as Alice. The surprising feature of this protocol is that Alice’s advantage over Eve holds despite the broken entanglement. (APS/Alan Stonebraker)

Zhang *et al.* couldn’t have achieved this result without overcoming several technical hurdles. First, to ensure Alice’s measurements were efficient, they had to find a way to match the bandwidths of the down-conversion source, the erbium amplifier, and the detectors so as to give Alice her best performance. Second, they used a spool of dispersion-shifted fiber in which Alice could store her photon coherently for long enough to recombine it with the returned signal. Finally, they ensured interferometric stability by using free-space delay lines to fine tune the timing of the stored and returned signals.

So far, Zhang *et al.* have proved that their protocol is secure for passive attacks—the kind when the eavesdropper simply steals some of the light transmitted between the legitimate parties. This kind of security does not unconditionally extend to active attacks where, for example, the eavesdropper might use their own entangled source to probe the object at Bob’s station. Closing this loophole is an important problem for turning their work into an application. Already, though, Zhang *et al.*’s demonstration is a major step forward in developing quantum technologies that are compatible with the real world of noisy and lossy communications systems.

References

- [1] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, “Entanglement’s Benefit Survives an Entanglement-Breaking Channel,” *Phys. Rev. Lett.* **111**, 010501 (2013).
- [2] S. Lloyd, “Enhanced Sensitivity of Photodetection via Quantum Illumination,” *Science* **321**, 1463 (2008).

- [3] J. H. Shapiro, "Defeating Passive Eavesdropping with Quantum Illumination," *Phys. Rev. A* **80**, 022320 (2009).

About the Authors

Tim Ralph



Tim Ralph is a Professor of Physics at the University of Queensland. He obtained his undergraduate degree from Macquarie University, Sydney, and his Ph.D. from the Australian National University, Canberra. He was awarded an Australian Research Council QEII Fellowship in 2000 and an ARC Professorial Fellowship in 2006. He is currently a Node Director and Program Manager in the Centre for Quantum Computation and Communication Technology.

Ping Koy Lam



Ping Koy Lam completed his B.Sc. degree from the University of Auckland in 1990. He worked as an engineer for Sony (Audio) and Hewlett-Packard (Semiconductor) prior to his postgraduate studies at the Australian National University where he obtained a Masters degree in theoretical physics, and a Ph.D. in experimental physics. He was awarded the Australian Institute of Physics Bragg Medal in 1999. He was an Alexander von Humboldt fellow at the Erlangen-Nürnberg Universität in 2000 and a CNRS visiting professor at Paris University in 2007. He is currently a professor and the group leader for Quantum Optics at the ANU.