Modern Physics

Writing Project: Entanglement’s Benefit Survives an Entanglement-Breaking Channel

Peter Vlasenko

100395185

New Results in Communication Based on Quantum Entanglement

A recent study conducted at the Massachusetts Institute of Technology (MIT) by a team of researchers has shown experimentally for the first time that a well-known property of quantum mechanics known as quantum entanglement can be utilized for practical communications technology even in environments where this quantum property would normally not function. The researchers further discovered that this property can be used to attain “eavesdropping-immune” communication.

Quantum entanglement is a hot topic in the ever-growing field of quantum information and computing, and this study helps to confirm the practical viability of this process in future applications. The study also demonstrates that quantum entanglement can be used for the purposes of establishing highly secure two way communications.

So what is this so-called property of quantum entanglement? Quantum mechanics, the scientific theory that accounts for the workings of atomic and sub-atomic particles, allows for some very interesting physical processes that we could never imagine for objects of a macroscopic scale, that is, everyday objects that we can see and touch. In quantum mechanics, a particle is described by a “quantum state”. This state gives us statistical information about the particle’s properties such as its position in space, its velocity, its energy, and so on. A principle known as superposition allows two or more distinct particles to become “intertwined”, effectively placing both particles in the same quantum state. These particles can remain in the same state even if they are split apart or are moving away from each other.

Why is this important? A curious feature of quantum mechanics is that even if one knows everything there is to know about the state of a particle, one still cannot predict with certainty where the particle will be at any given moment, or what its velocity or energy will become. In other words, quantum mechanics introduces a sort of indeterminacy in nature. However, once we directly measure, say, the position of a particle, the particle is forced to “take a stand” at some definite location, although we cannot predict beforehand where this position will be (at least not with complete certainty). Furthermore, the measurement of a property of one particle in a superimposed system can have a direct impact on the properties of the other particles in that system. The most salient example is found in a quantum property called “spin.” Every particle has some associated spin, which is a defining feature of the particle. For example, all electrons have a spin value of either +1/2 or -1/2. We do not know (before measuring) which value a particular particle will have, but if two such particles are superimposed in the same quantum state, one particle must have a +1/2 value, while the other must have a -1/2 value. This means that a measurement of the spin value of one particle will determine the spin value of the other particle as well, even if the second particle happens to be arbitrarily far away. What’s more is that this “communication” between the superimposed particles happens extremely quickly (if not instantaneously). This is known as quantum entanglement. Recent experiments have confirmed that the speed of this communication is at least 10000 times faster than the speed of light.

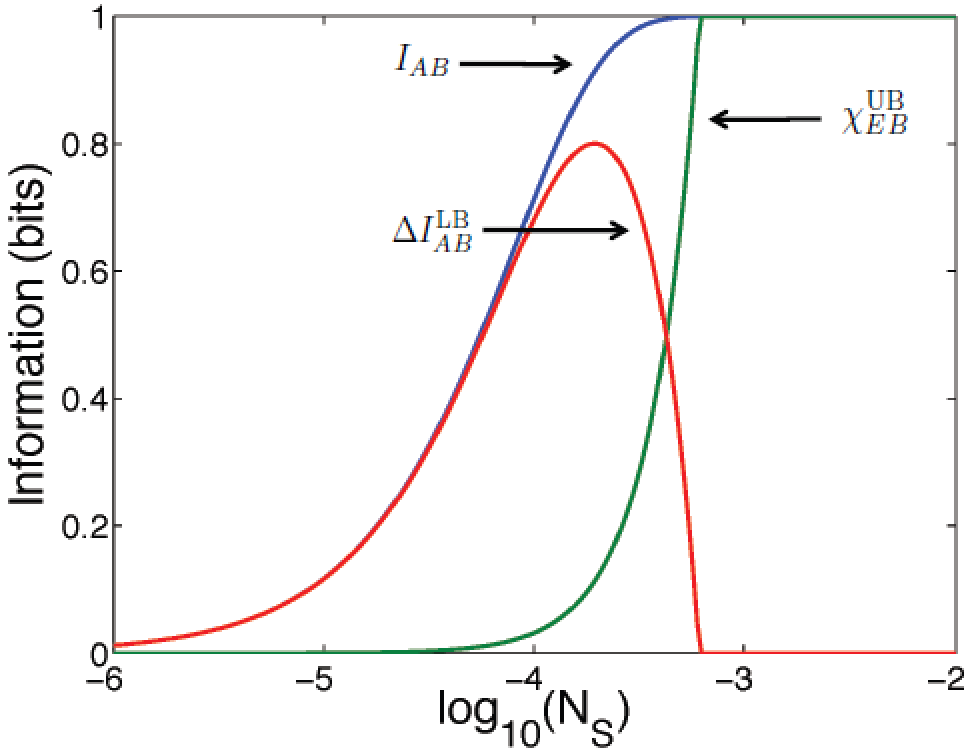
Due to this instantaneous (or near instantaneous) communication the potential applications of quantum entanglement in communications technology and computing are astounding. But this is where we run into some problems. One of the issues that scientists are concerned about is whether or not this process will actually be viable on a macroscopic scale. After all, we are interested in using this property in everyday sized objects, not sub-atomic particles, and as it turns out entanglement between two particles can be destroyed quite easily by interference from the surrounding environment, in which case all communication potential is lost.

Or so it seems at first glance. This study conducted by Dr. Zheshen Zhang and his team has shown that the potential benefits of quantum entanglement can actually survive, despite the loss of entanglement.

Their experimental setup is as follows. Data in the form of encrypted laser beams is sent from one source (Alice, in this experiment) to another source (Bob) and then back to the first source. A third party is also introduced (Eve) whose goal is to try to “eavesdrop” on the communication between Alice and Bob by stealing a portion of the data flowing between them. This experimental method is known as “quantum illumination.” The laser beams are prepared in an initially entangled state, and are then intentionally made to flow through “entanglement-breaking channels” with a background noise of up to 8.3 decibels higher than the cut-off value for entanglement. The experiment shows that communication is nonetheless achieved between Alice and Bob, and more importantly, Eve is unable to eavesdrop on the communication. This would not be the case if the laser beams were not initially entangled; in this case the communication would not be immune to eavesdropping.

Roughly speaking, the reason why Eve is unable to eavesdrop on the “conversation” between Alice and Bob when entangled states are used is because Alice and Bob both retain a portion of their entangled states when they communicate with each other. These entangled states are necessary for proper decryption of the other source’s data. Eve, on the other hand, has access to the data but no access at all to the initial retained portions of the entangled states. Therefore Eve is unable to decode the message. The authors note, however, that Eve could potentially eavesdrop on the communication via “active attacks” whereupon Eve sends a separate light beam into the mix. This experiment only confirms immunity against “passive” eavesdropping.

The figure shown below illustrates some of the conclusions made by the authors.



This figure from the authors' original article shows the amount of information obtained in bits by Alice (blue curve) as a function of the signal brightness (or intensity). The green curve shows the amount of information obtained by Eve, while the red curve shows the difference in information obtained between the two. In other words, the red curve demonstrates Alice's advantage over Eve. Notice that the advantage is highest for a particular value of beam brightness. For brightness above this critical point the quantum entanglement starts to become irrelevant, and Eve quickly gains the same level of information as Alice.

The novelty of this experiment is that the useful applications of quantum entanglement for quantum information should not be immediately disregarded just because the environment is noisy and destroys the entanglement. It also provides a basis for communication security in the quantum realm.

I interviewed Dr. Zhang to ask him a few questions pertaining to his research. A transcript of the questions and his answers is given below.

Interview:

Question: *What was the motivation behind this research?*

Answer: The main motivation of this research is to demonstrate entanglement-enhanced performance in a noisy environment. In particular, one goal is to harness and benefit from entanglement in an entanglement-breaking channel. This research would enrich the understanding of entanglement and lead to more entanglement-based applications.

Question: *What are some of the other interesting applications of quantum entanglement and/or quantum illumination, aside from communication security?*

Answer: Quantum entanglement is the basis for many applications that outperform their classical counterparts. Quantum teleportation enables transferring an unknown quantum state by classical communications and local operations. Quantum dense coding can beat the classical channel capacity. Quantum algorithms also require entanglement to achieve an exponential speed up. However, all these applications need high-quality entanglement. Quantum illumination is a different paradigm that allows for use of entanglement in situations that dramatically destroy the entanglement quality. Besides the secure communication, quantum illumination can also be utilized to enhance the signal-to-noise ratio of detecting a remote target.

Question: *Your article talks about quantum illumination's immunity to passive eavesdropping, but mentions that it is potentially vulnerable to active attacks. Do you think that methods of security against such active attacks can be achieved relatively soon?*

Answer: To defeat active attacks, we need to monitor some physical properties of the channel. The same idea arises in quantum key distribution, for which unconditional security has been achieved. We are currently working on the theoretical investigation on the active attack immunity. We hope to propose a theoretical model in the near future and then implement active-attack immune secure communication.

Question: *In your article you say that eavesdropping-immune communication is achieved despite a channel noise 8.3 dB beyond the threshold for entanglement breaking. Is this the upper limit to the amount of noise that can still sustain communication, or could an even higher threshold be reached?*

Answer: Our scheme can actually tolerate more noise and loss at the cost of higher bit-error rate and lower information advantage over Eve. An alternative is to improve some of our current device imperfections, such as detector noise and internal loss. By doing that, the bit-error rate and information advantage over Eve will be maintained, and we will be able to reach a longer communication distance.

Question: *Will you be doing more research on this particular subject, and if so, what's next?*

Answer: For the future research on this subject, we first plan to demonstrate the ability against active attacks and hope to increase the data transmission rate and distance. It is also valuable to explore other applications based on quantum illumination.

References:

- Zhang, Z., Tenger, M., Zhong, T., Wong, F., & Shapiro, J. (2013). *Entanglement's benefit survives an entanglement-breaking channel*. Unpublished manuscript, Massachusetts Institute of Technology, Cambridge, Retrieved from http://arxiv.org/abs/1303.5343