

AC 2007-1864: ENTANGLED PHOTON EXPERIMENTS FOR ENGINEERING TECHNOLOGY

Scott Shepard, University of Central Florida

Dr. Shepard received a Ph.D. from MIT and worked at Bell Labs for six years. He has been teaching in Engineering Technology for five years and is currently at the University of Central Florida. His research interests include: innovative laboratory components for undergraduates; telecommunications; sensors; and solar energy.

Entangled Photon Experiments for Engineering Technology

Abstract

The fact that a Quantum Computer can (at least in principle) break the security of classical encryption codes has spurred a tremendous interest in the development of Quantum Encryption (QE) – the only means of restoring computer data and telecommunication security. Once the realm of a select few of quantum physicists, QE has now become a very important emerging technology. Herein important technological issues (that our Engineering Technology Photonics students are well versed in) arise. Two of the most important issues of practical implementation are: the brightness of the sources and the efficiency of the detectors.

Single-photon sources have only recently been made practical and economically accessible for use in undergraduate laboratories.¹ This occurred in undergraduate physics labs, where the focus has been upon the use of these to demonstrate the most strikingly non-classical aspects of quantum physics.² With similar apparatus however, our emphasis will be on the *application* of these to QE, such as: the practical implementation issue of approximating the non-classical source with a highly attenuated standard laser. This also helps connect the Entangled Photon experiments to our Laser Technology curricula.

Similarly, issues regarding detector efficiencies connect the Entangled Photon experiments to students experiences in the Lightwave Telecommunications area. Therein, we perform experiments comparing avalanche photodiodes (APDs) to PIN photodiodes. The high gain of APDs makes them attractive for single-photon and low intensity laser applications. The highest gains can be achieved in silicon APDs and the extensive use of silicon in the electronics industry makes the material advantageous for integrated photonics/electronics chips. Unfortunately silicon does not respond well to the optical wavelengths (around 1550nm) that are presently used in the telecommunications industry. Thus, the interplay of: industry; cost; technology; and materials, becomes a part of the laboratory component – even within this seemingly esoteric application.

Why Engineering Technology?

It has been said that the two most significant areas of technological innovation in current times can be categorized as: “nano” and “quantum” (with as much potential societal impact as the transistor and the laser held in the 1960’s). The promises of nanotechnology are well known and the potential impact of quantum computers and quantum communication is becoming more apparent in the public domain. Apart from exposing undergraduates to an important emerging technology however – why should quantum communication experiments be integrated into engineering technology laboratory components at this time?

One reason is that it is now time for quantum encryption to be brought into actual/practical implementation. This goal is precisely the path a committee at the Los Alamos National Laboratory (LANL) has recommended for the primary focus of future funding in the area³. As the LANL 'Quantum Information Science and Technology Roadmap' puts it: "... *will build on existing ... capabilities to integrate them within networked optical communications testbeds at*

the physical layer...” The phrases “build on existing” and “integrate...within” quickly illustrate the relevance of the role of Engineering *Technology*. Moreover: although the technological implications are astounding; the underlying mathematics is very simple and readily accessible to Engineering Technology students. These students are also well versed in most of the practical issues at hand. In particular, those in our photonics program are already experienced in practical optical hardware issues involving detectors and photonic sources (two of the key elements for implementation).

Another reason to involve Engineering Technology is because now is the time to “bridge the gap,” or as the LANL roadmap³ puts it, to incorporate LANL’s desire that: “...quantum cryptography becomes more closely integrated with conventional, basic, and applied information-security and communications...” To that end, these entangled photon experiments will also be made available to students in the Information Systems Technology (IST) program. The IST students do not have any background in photonics (let alone quantum physics). Due to our technological spin towards the applications however (instead of the physics) this is not a disadvantage. Therein the IST students perform systems level experiments, bringing us several steps closer towards accomplishing the longer term objective of ushering us into a “quantum information-assurance era.”

What the Physicists Do With Entangled Photons

The word “entangled” implies more than just correlation (however entangled photons will exhibit correlation in their measurement statistics). Systems A (or Alice) and B (or Bob) are entangled if their state vector is not a simple product, i.e., if it cannot be written in the form: (state of A) a times (state of B) b . Now taking (+) to represent the state of “spin up” along z and (-) to represent “spin down” – the only two possible spin states of an electron, an example of an entangled state is: (+) a (-) b + (-) a (+) b . If we ask “what is the spin of A?” the answer is – well it could be up or down, depending on if we “draw” the first or second term respectively when we measure it’s state. However, we see the correlation due to the entanglement as follows: if we measure the state of A and find it to be up, then we know we have drawn the first term and then we know with certainty that B has to be down. Likewise, if we find A to be down (we’ve drawn the second term) then we know with certainty that B has to be up. They are perfectly correlated (in this opposite or perfectly anti-correlated sense). What Einstein⁴ was bothered by is the fact that if detector B decides to measure spins along the x axis (instead of z) then this perfect correlation disappears and the measurement results have no correlation at all. He felt that this indicated an incompleteness of quantum mechanics – that there are “hidden variables” (unseen by quantum theory) that behaved classically and this led to the so-called “EPR paradox.”

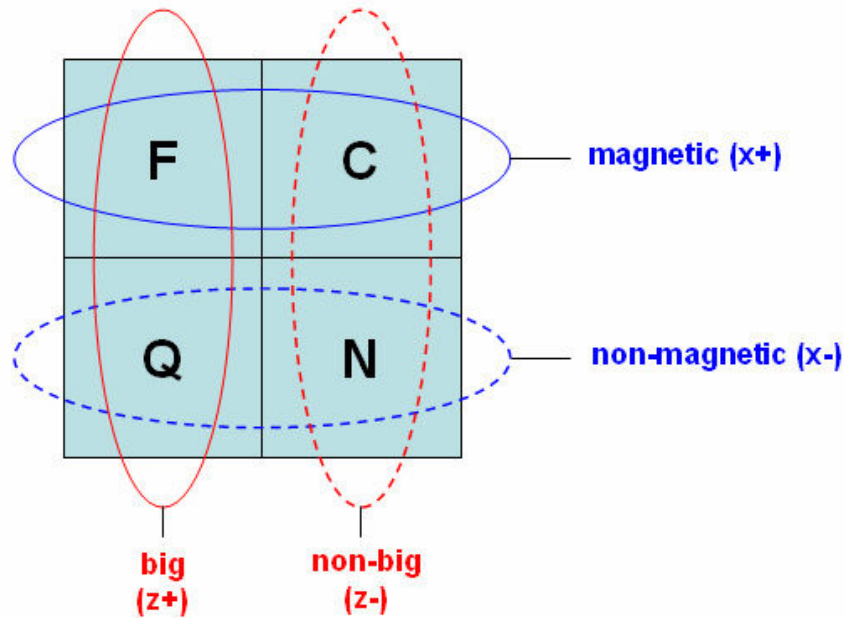


Figure 1 (an unsophisticated candy machine)

As shown in figure 1 however, this is not a paradox after all because there *is* a simple classical model that *can* explain these results. Let detectors A and B now be unsophisticated candy machines that can choose to either: sense the size of a coin; or sense if the coin is magnetic (but they can not sense both properties at the same time, just as we can not measure spin along x and spin along z simultaneously, we just chose to measure one or the other). Consider four coins: a Franc, a Canadian nickel, (both of which are magnetic), a U. S. Quarter, and a U. S. Nickel, (both of which are non-magnetic). The franc and the quarter are both big, while the Canadian and the U. S. Nickels are both non-big (i.e., small). These are our *hidden* variables, we are unable with our current senses to distinguish franc-ness or quarter-ness, etc. (although they are in principle distinguishable). You and I can only measure magnetic-ness (property x) or big-ness (property z) and either one of us can only measure one property, or the other, at any experimental trial. Now the way we select these coins is such that you and I get ones from opposite corners: if I get the franc, you get the nickel, etc. This preserves the perfectly (anti-)correlated results when we both measure the same property. For example, if we both sense magnetic-ness and I get the result “yes” (so I have either the Franc or the Canadian nickel) then your magnetic-ness result will have to be “no” (as you must have the nickel or the quarter). However, if you decide to sense big-ness instead, then our outcomes are now uncorrelated: you get either a big coin (result “yes” from the quarter) or a small one (result “no” from the nickel) with equal probability. Thus we have perfect correlation when we measure the same property (same spin axis) and this vanishes, leaving no correlation, when we measure different properties (different axes). So there *is* a hidden (classical) variable model that can explain these results – just as Einstein would have wished it. We do not run into “spooky action at a distance” (i.e., an incompatibility between hidden variable models and quantum predictions) until we consider the work of John Bell.

Bell⁵ found that when one considers the incorporation of a third axis of spin measurement (in addition to the x and z axes) then the predictions of quantum theory and any hidden variable model are fundamentally inconsistent. Hidden variable models would have to satisfy a “Bell’s inequality,” whereas the predictions of the quantum calculations violate this inequality. Therefore hidden variable models and quantum mechanics are incompatible and we should do an experiment to determine which one (if either) is correct. Many such experiments⁶ have been performed, closing various implementation loop-holes, and quantum mechanics always works. In the implementation of these experiments it has been far easier to measure optical polarization rather than electron spin (vertical and horizontal polarization being a two-state phenomenon). Polarization entanglement is accomplished in a variety of nonlinear optical processes. In the section “Reduction to Practice – Issues of Technology” we will discuss some of the details. Recent technological advances have brought such capabilities into undergraduate physics labs.^{1,2} Therein the laboratory modules have focused upon demonstrating some of the most strikingly non-classical aspects of quantum theory, as discussed above.

What the Engineers Do With Entangled Photons

For engineers these mysterious quantum correlations are a solution, rather than a problem. Quantum computers also “break the classical rules,” and in so doing they could break an encryption code in minutes that would take thousands of years on a (classical) supercomputer. This threatens all aspects of computer security. The quantum entanglements however come to the rescue in the form of quantum encryption. Therein the security is based on the laws of physics, rather than on computation time, thereby restoring security (even in the advent of quantum computers). One aspect of quantum encryption is the procedure known as quantum key distribution (QKD). In QKD the encryption is performed classically via the standard technique of scrambling (and unscrambling) the data with a “key” data stream; but the key itself is securely sent from Alice to Bob utilizing entangled photons. Think of one of the inputs to an exclusive-or (XOR) gate as a control. If the control is a 1 then the XOR gate passes the other input bit unaltered. If the control is a 0 then the XOR gate passes the other input bit inverted. When the control lead is fed a stream of ones and zeroes (a “key”) this will scramble the transmitted data (seemingly random inversions of the original data) so that it is unrecognizable to anyone who does not possess the key. If the intended receiver possesses the same key however, then XORing the scrambled data with the key will properly remove those seemingly random inversions, thereby revealing the original data. The problem then is how can we securely distribute the keys?

In QKD the key is securely distributed via entangled photons as follows. It relies upon two essential ingredients: (1) no “quantum cloning,” i.e., you cannot make a perfect duplicate of the quantum state of a photon; and (2) if you measure the quantum state you will alter it (1/2 of the time). So Alice is going to send Bob the key, while eavesdropper Eve tries to listen in. Alice sends spin up (+) as a one and spin down (-) as a zero, but she sometimes uses the x-axis, and sometimes the z-axis, as her reference or “basis.” Bob then randomly picks a basis (x or z) for each measurement that he performs. *After* he has performed his measurements (and recorded his results and which basis he used for which bits) Bob then publicly announces the sequence of basis that he used for his measurements. Alice then knows which times Bob randomly picked the same basis (x or z) that she happened to use. Alice can then publicly announce which times Bob happened to use the correct basis. Bob then knows which times he got the perfectly correlated bit

that Alice sent, and he disregards the rest of his measurements. Alice and Bob now share the same key – the stream of bits during which they both used the same basis. Notice that if Bob announced his basis *before* his measurement then Eve could use the same basis and go undetected (measuring in the same basis won't alter the state). Also, Eve can't store these up and look at them later, because she can't copy them in the first place (no cloning). Moreover, when she randomly picks a basis to eavesdrop with, she's picking the wrong basis 1/2 of the time and when she does, that alters the quantum state causing a bit-error-rate of 50% which is easily detectable. Thus Alice and Bob can easily recognize when Eve's trying to listen in the first place. This procedure is diagrammed in figure 2, where (for optical polarization) up and down along x and z, are replaced by vertical and horizontal along 0 degrees and 45 degrees, respectively.




Alice sends					
Bob uses	+	+	X	X	+
Same Basis ?		yes	yes		yes
key		0	1		0

Figure 2 (+ = vertical/horizontal basis, X = same rotated by 45 degrees)

Reduction to Practice – Issues of Technology

The preferred method of generating entangled photons is the process of parametric down-conversion. Therein a pump photon of frequency f is converted into two photons of frequency $f/2$. The two output photons are entangled in their polarization states. These experiments used to require a high intensity ion laser. Recently however, technological advances have made this much more affordable: one can use 5mW violet (400nm) *laser diodes* for the pump. That also puts the output photons at 800nm where *commercial* silicon avalanche photo-diode (Si APD) modules exist. This advance has brought entangled photons into the undergraduate physics labs. Rather than testing for hidden variables and Bell's inequality violations however, we are putting a technological spin on it for our undergraduate engineering technology labs in which we explore the *application* of entanglement for quantum key distribution. Therein, there are two major categories of practical implementation concern: sources and detectors.

Regarding detectors, the Si APD commercial single-photon counting modules have high efficiency (50%) and low dark current, but since they employ silicon they have the highest sensitivity at a wavelength of 800nm. Optical fiber losses at 800nm however are 2dB/km which is very high by today's standards. That is why the optical telecommunications industry does not employ this wavelength (they prefer to operate near 1550nm, where fiber dispersion and loss are minimal). On the other hand, silicon is the preferred material in the semiconductor industry, hence the impetus for "silicon photonics" which is an attempt to bridge the gap between the two industries. The telecom industry has utilized 1330nm as a carrier wavelength in it earlier stages of development. Here the fiber losses are now down to 0.35dB/km, but at this wavelength no commercial single-photon counting modules exist. So custom made cooled InGaAs APDs have been used in the lab for such experiments (with a detection efficiency of 10%). At the telecom

preferred wavelength of 1550nm fiber losses are even lower, at 0.2dB/km. Again, however, there are no commercial single-photon counting modules at this wavelength and so cooled InGaAs APDs have been used in the lab (with a detection efficiency of 2%). In our laboratory modules the students will perform system level experiments that emphasize the technological tradeoffs involved. For example, how much further can I go in fiber at 1550nm (as opposed to 1330nm) and still achieve the same overall (fiber and detector) efficiency? Incorporating these effects and the QKD procedure (losses of bits for which we didn't pick the same basis) what is the maximum key transmission rate at these distances? Do the experiments confirm these calculations or are there other real-world effects that we didn't account for? The students also will do readings in (the more applied) technical journals to keep abreast of progress in silicon photonics – what are the projections? How does detector cost play a roll in making choices among the current states-of-the-art, etc.? Thus, even within this seemingly esoteric application, the interplay of: industry; cost; technology; and materials, becomes an important part of the laboratory component.

Regarding sources: in order for QKD to work, within each pulse (of chosen polarization) there should only be one photon – otherwise Eve could steal one! So single-photon sources are desired. Currently, we don't really have any, so we approximate via either: (1) a weak laser; or (2) an entangled photon source with which we can use one output to gate (enable) a detector. With the weak laser approach we take a regular laser beam (which has a Poissonian distribution for the number of “clicks” within a detection integration time, T) and attenuate it (so that we normally get no more than one click per T). One problem here is that then the probability of a single click (single photon detected) is about 1/10. The photodetector's dark current (random clicks) then becomes relatively appreciable. This also lowers the key transmission data rate. Moreover, even at such a low intensity the probability of two clicks is 0.005, thus giving an “Eve's dropping” error of 5%. Note in comparison that a bit-error-rate of $5 \cdot 10^{-2}$ would be considered to be horrible by telecommunication standards. If instead, one utilizes an entangled photon source then a similar problem arises. We say that we get two entangled photons out of a parametric down-conversion crystal when one pump photon goes in. But the problem is that we still pump with a weak laser (not one photon) so multiple photon pairs can still come out. From the pairs however, we *can* now get around dark current problems by gating B's detector only when A saw one also. The low intensity of our pump however still limits our key transmission data rates. Thus, our experiments related to source issues also involve many real-world tradeoffs that are important to the practical implementation of this emerging technology.

Bibliography

1. D. Dehlinger and M. W. Mitchell, “Entangled Photon Apparatus for the Undergraduate Laboratory,” arXiv:quant-ph/0205172 v1 (2002).
2. E.J. Galvez, C. H. Holbrow, M. J. Pysher, J. W. Marting, N. Courtemanche, L. Heilig, and J. Spencer, “Interference with Correlated Photons: Five Quantum Mechanics Experiments for Undergraduates,” Am. J. Phys. 73 (2005).
3. <http://qist.lanl.gov/>
4. A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. 47 (1935).
5. J. Bell, Physics 1 (1964).

6. A. Aspect, P. Grangier and G. Roger, Phys. Rev. Lett. 49 (1982).