Applications and limitations of Single and Entangled Photons

Jacob Begis

The production of single and entangled photons is very important to the developing fields of quantum computing and quantum encryption.

If two quantum particles interact physically and then separate they become entangled [1]. One method to produce entangled photons is to use a specially prepared crystal to split a photon into a pair of entangled phones [2]. One particle’s future actions are dependent on the past interactions with the other particle causing them to become entangled. Quantum entanglement is a correlation between quantum particles. This correlation can allow two or more quantum particles to be inextricable. If a measurement is taken for one member of a quantum pair the other member will have a perfectly correlated value regardless of the distance between them [3]. An important concept to understand when talking about single and entangled photons is the Heisenberg uncertainty principle. It states that there is a fundamental limit to the precision to which one can know the position and momentum of a particle simultaneously. The equation is as follows:

\[ \Delta x \ast \Delta p \geq \hbar / 4\pi \]

Where \( \Delta x \) is the uncertainty of position \( x \) and \( \Delta p \) is the uncertainty of the momentum \( p \), and \( \hbar \) is plank’s constant.

Wave packets a probability distribution of various properties of a quantum particle such as position and momentum [4]. These can be used to represent a quantum particle. According to the Copenhagen interpretation, quantum mechanics are not a description of reality but only a description of a probability of observing various properties. In addition the observation of quantum particle causes it to immediately and randomly assume a set of values for its properties. It is the reduction of its physical possibilities as defined in its wave packet reduced to a single possibility as seen by its observer. This is a called a wavefunction collapse. Because of this the entangled photons shared state is uncertain until measured.

Non-quantum computers use binary bits which are encoded to be a zero or a one while quantum computing could theoretically use quantum bits known as qubits. A qubit is a quantum system with two states; vertical and horizontal polarization. A qubit ‘state’ os the superposition of both states concurrently. Qubits also exhibit entanglement which results from the superposition. Based on the principles of superposition and quantum entanglement a quantum computer can process calculations simultaneously. While a non-quantum computer
has zeroes and ones, a quantum computer has ones, zeroes and any possible superposition of
the ones and zeroes. For example while three classical bits could represent any of the numbers
from 0 to 7, three qubits could represent the numbers 0 to 7 simultaneously. This is called
quantum parallelism [5]. N qubits can perform $2^n$ calculations at once [6]. Another way to
explain this concept is a quantum computer could theoretically do computations on many
numbers and once and subsequently interfere the results to get a single answer [7]. This
concept could allow a quantum computer to factor a 500 digit number quickly, while a classical
super-computer cannot do so. This is important because factoring extremely large numbers is
very important in the field of cryptography [3].

A ubiquitous method for encryption is the RSA algorithm. It is an asymmetric cryptography
system. This is an alternative to symmetric encryption systems where the key could be secretly
stolen allowing the hacker to read messages, and create fake messages without detection [2].
Under the RSA algorithm a product of two large prime numbers along with an auxiliary value is
produced as a public key while the prime factors are kept secret. This public key can be used to
encrypt a message and if the public key is large enough only someone with knowledge of the
prime factors can decode the message [8]. The private key is used to decrypt. While RSA can
crypt any message its mathematical routines take so much processing power that it is often
only used to exchange keys, after which convention, symmetric encryption methods are
established [2]. Quantum cryptography solves this problem.

Quantum cryptography can be applied to distribute quantum keys. This is based on the
principle of quantum indeterminacy (which is an implication of the Heisenberg uncertainty
principal); if someone attempts to eavesdrop on a quantum signal they will disturb it. Imagine
if person A was receiving one half of a string of entangled photons with random polarizations
while person B was receiving the other half from an allied source through an optical fiber
quantum communication channel. Since the polarizations are random there is no way to
predict properties of individual photons [3]. However if person A and person B both measure
the polarization states of the entangled photons they receive they would measure the same
polarization states since they are entangled. If the photons are given vertical and horizontal
polarizations represented by ones and zeroes than person A and person B should receive the
same string of ones and zeroes. Even if a spy knew the photons were being sent out with either
a vertical or horizontal polarization they could not intercept the signal. This is because if an
eavesdropper observes a photon it will have a wavefunction collapse causing it to no longer be
entangled, leading to person A’s and person B’s string of ones and zeros to mismatch. Person A
and person B can continue to receive photons while comparing the results until the string is
long enough. They can now treat this long string of ones and zeros as an encryption key. They
can now use this key with an encryption algorithm to encrypt and decrypt messages which can
be transmitted over a communication channel such as wire or radio channel [9].
In the past a laser pulse attenuated to a single photon level was used to send the photons but now single photon sources are used. These dim laser pulses allowed hackers to find a group of two photons that are not anti-bunched, measure one photons polarization and then send the other to the intended receiver without leaving a trace [12]. Now that single photon sources are used a hacker cannot do this because one cannot create an identical copy of an intercepted quantum particle in accordance to the no-cloning theorem. Single photon sources produce anti-bunched photons – meaning the photons are separated in space and time. This is different than a laser attenuated to a single photon level because in the case of the laser there is only an average of one photon per some distance while there are sometimes groups of two or more photons [6]. One way in which anti-bunched photons are produced is by exciting a single atom, allowing a photon to be emitted and then exciting the atom again emitting another photon. There will always be a delay between the two excitations called fluorescence time. Another single photon source is the quantum dot. Quantum dots are nanoparticles of a semiconductor material that have unique optical and electrical properties. When excited they emit photons with its bandwidth as a function of its size allowing a manufacturer to choose the emission frequency [13]. Because of quantum dots’ small size they are subject to quantum confinement since the diameter of the dot is on the same order of magnitude as the wavelength of its electron wavefunction [14]. Quantum confinement allows quantum dots to have fluorescence and in-turn become single photon sources under certain conditions [15].

If an efficient and functional quantum computer is developed then by using Shor’s algorithm every RSA and some quantum encrypted keys could be decoded [16]. It could find the prime factors of a given integer given a quantum computer with a sufficient number of qubits. Quantum cryptography can encrypt codes that only a quantum computer could feasible decode. It will be a race between quantum encryption technology and quantum computing technology. As quantum computers increase the number of qubits quantum encryptions technologies will increase the length of keys and one-time pads (OPT) which have been proven to be impossible to crack if used properly may become more widespread [2]. In an OPT each character from the plaintext (information from the sender to the receiver) is encrypted by using modular arithmetic with a bit or character from a secret and random pad key of the same length of the plaintext resulting in encoded information (ciphertext) [17]. If the pad is random and as large as the plaintext and never used more than once, then the ciphertext will be impossible to decrypt [18]. Infinite computational power and infinite time cannot break one-time pad encryption because it is mathematically impossible [19].

The limits of quantum computing result from qubits interacting with the environment around them which can cause a qubit’s quantum state to change or decay [20]. However this decay time is small compared to the computation time since physicists have come up with ways to statistically compensate for this decay using computations error-correction schemes (ECS).
in the case of one qubit a computation can be done before the quantum state decays completely. However in the case of two qubits the entanglement sudden death happens too quickly to be compensated for by ECS [20]. Imagine if one qubit of an entangled pair is traveling to the left and another qubit is of the same entangled pair is traveling to the right. If one of the qubits is effected by environmental noise then ECS will correct for it, however if both are effected by ECS simultaneously sudden death will happen and entanglement cannot be restored. In other words, ECS can compensate for the environmental effects on one qubit of an entangled pair but not more than one at once. According to Joseph Eberly, a physicist at the University of Rochester, "The degree of information entangled can disappear faster than the information itself" [21]. Since quantum computing, quantum cryptography, and quantum teleportation require entanglement, this sudden death principle is a pressing problem which contemporary researchers are working are hard to solve.
Appendix: Additional explanation of how quantum cryptography prevents spies from eavesdropping

Imagine that person A wants to send a secret message to person B. First they will send a random sequence of photons travelling in one direction, as a key that represent two different initial bits of data represented by 0 and 1. The photons are also oscillating in 4 particular states of polarization as shown in the below table.

<table>
<thead>
<tr>
<th>Basis</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rectilinear</td>
<td>↑↓</td>
<td>→←</td>
</tr>
<tr>
<td>Diagonal</td>
<td>↗↙</td>
<td>↘↖</td>
</tr>
</tbody>
</table>

Person A has a rectilinear and diagonal polarization filter and swaps between them as well as their orientations randomly to produce transmissions that represent either a 0 or 1. As person B receives each photon he will guess to measure the polarization state using a rectilinear or diagonal polarizer. So if person B uses the Diagonal polarizer to measure ↑↓ and →← the photons will pass through the polarizer in a changed state, half transformed to ↗↙ and half to ↘↖ on average. However person B does not know which photons are transformed to which polarization state. Person B will measure some photons correctly and some incorrectly. Now that the key has been established the channel of communication no longer needs to be secure. Person A now tells person B which polarizer they used to send each photon bit but not how they polarized each photon. So person A tells person B that photon number N was sent using a rectilinear polarizer but doesn’t say whether it was a 1 or a 0 bit. Person B then checks if he used the correct polarizer for photon N. After all the photons have been checked every measurement person B did with the wrong polarizer is discarded. Now they have a sequence of 1’s and 0’s that is about half the length of the original key. This is now a basis for the one-time pad. Now if a person C eavesdrops while having the same polarizers as person B and knowing to guess rectilinear or diagonal for each photon. Like person B, about half of the time person C will guess the wrong polarizer. However person C did not speak to person A to know which polarizer was used for each photon. In addition if person C transforms a photon then that photon will either have been discarded regardless or it will cause person B to make an error if he used the right polarizer causing person A and B’s keys to no longer be identical. Person A and person B would no longer use the key. They would check for this by comparing a small percentage of the large amount bits to check this. If they matched then those bits would be discarded from the final key.

The following example is based off of an article on source [23] from techtargert.com
References


   http://iqc.uwaterloo.ca/welcome/quantum-computing-101


   http://www.optics.rochester.edu/workgroups/lukishova/QuantumOpticsLab/index.html

   http://www.perimeterinstitute.ca/personal/dgottesman/qcomp.html

   http://en.wikipedia.org/wiki/RSA_%28algorithm%29

   http://en.wikipedia.org/wiki/Quantum_key_distribution


    http://www.aip.org/tip/INPHFA/vol-10/iss-6/p22.pdf

    http://www.nanocotechnologies.com/content/AboutUs/AboutQuantumDots.aspx


