Single and Entangled photons

Edward Pei

War is most commonly thought of as men fighting with their fist, and power is determined by physical strength. Behind the lines, however, knowledge is power. For example, information of the enemy’s location and when they intend to strike are vital in times of war. Furthermore, knowledge must be exchanged so that it can be used efficaciously. That is why the most powerful intellectual weapon is secrecy. The ability to exchange information securely to the intended recipient can win wars, and quantum computers, using single and entangled photons, is the next revolution to securing information.

The current approach to secure the content of a message is to dissuade the interceptors through counter measures. Consider three entities, Alice, Bob and Eve. Alice wants to communicate a secret to Bob, and Eve wants to eavesdrop. Alice sends Bob her message in a box with her lock on it so Eve can’t intercept the message. Bob, also unable to open the box, puts on his own lock with his own key and sends it back to Alice. Alice now has her box with her message and both her and Bob’s lock. She knows nobody has read her message yet since she hasn’t removed her lock. She proceeds to send the box back to Bob after removing her lock. Eve cannot open the box since Bob’s lock is on it.

Now, the box has arrived to Bob with Alice’s message and Bob’s lock. He can easily open the box by removing his lock, and he knows that the message was not intercepted by Eve. This secure transmission has been translated into the RSA encryption method used for secure communication. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1977. The above scenario deals with physical means of communication, so for computational communication the locks and keys have been transmuted into an asymmetrical cipher as the lock and prime numbers as the keys. This introduces a finiteness of the possible keys which Eve could exploit to obtain the information by trying every possible keys, referred to as a “brute force attack”. For this reason, encryption methods are compared in terms of the number of keys. In other words, to make an encryption method secure, it must have enough keys so that the interceptor would spend several lifetimes to try every possible keys. Time is the limit.

Quantum computers can break the time limitation through the use of quanta particles. These particles are the equivalent of a transistor. They can be manipulated to represent either a 1 or a 0, but unlike a conventional transistor they can achieve a superposition of both these 1 and 0 states at the same time. This new property can be translated into a comparison on how classical computers operate and how
theoretical quantum computers operate. A classical computer must compute all basic arithmetic using a sequence of classical bits (0 and 1). It would have to compute every possible prime numbers sequentially to solve the RSA encryption method. A quantum computer however could decrypt the RSA using Shor’s algorithm whereby the computation of all basic arithmetic occurs simultaneously by superposing the quantum bits into both states. Consider two qubits, each can represent a one, a zero and any quantum superposition of those two states. These two qubits can simultaneously represent 0 0, 1 0, 0 1, and 1 1. Now consider 3, 4, 5,… \(n\) qubits which can simulate up to \(2^n\) possibilities at once. A classical bit can only be one of these \(2^n\) states at a time. The introduction of parallel computing allows a dramatic reduction in time needed to solve the RSA encryption or any other conventional security measures. Quantum computing would allow Eve to decrypt any conventional encryption method.

Another security risk for any transportation of valuables is the method of transportation. We must insure that the package arrives to the intended recipient. When considering the medium of transportation we automatically expect the possibility of interception. If our method of transportation was a messenger physically carrying the valuable, then an external reality could intercept the messenger and acquire the information. Furthermore, the messenger can still deliver the message without revealing the fact that an external being has a copy of the valuable.

To achieve an ideal method of transportation we must reduce the possibility of an external factor interfering with the exchange. Currently, the method of choice has been to tackle the events following an interception by integrating security and safety measures like the RSA encryption method. Thereby preventing the message to be read by a thief. As we have discussed above, conventional methods of encryption are ineffective against quantum computers. Quantum telecommunication however can introduce a failsafe mechanism by making use of a quantum phenomenon called quantum entanglement. This phenomenon describes how two particles’ indefinite states can only be represented in term of the other even if they are separated by time and space. The two particles are linked, not because of a physical connection, but because of the uncertainty of their states. Heisenberg’s uncertainty principle states that

\[
\Delta x \Delta \rho \geq \frac{\hbar}{2}
\]

Heisenberg asserts that there is a fundamental limit to the precision of the simultaneous position in \(x\) and momentum \(\rho\). When a particle’s uncertain position and/or momentum causes a change of state of a
separate particle, these two particles become entangled. The initial interaction between both particles is uncertain, so the state of the second particle is defined by a probability distribution of said interaction. Making use of this phenomenon in conjecture with single photon sources, we can produce a method of transportation which cannot be interfered with. This method of using quantum mechanical effects to secure information is commonly called quantum cryptography. A single photon source as oppose to conventional photon source exhibits antibunching properties. These photons are emitted one at a time providing a standard chronological source of information by encoding each into a specific quantum state.

Consider Alice and Bob communicating with a single photon source and encoding each photon. Their communication would start with the creation of a unique key created and used by them called a onetime pad cipher. Alice would send a photon one by one and encode each photon using an arbitrary encoding scheme. The scheme defines what each quantum state represents (e.g. 1 and 0) for one photon. Bob would receive the photons and guess the quantum state of the photons using a random encoding scheme to decrypt the states. Alice would then compare with Bob the encoding scheme used for each photon and omit from the key the schemes Bob guessed incorrectly. Through this process Bob and Alice agree upon a shared sequence of encoding schemes. Bob would then use the correct sequence to decode the photons he received. Each decoded photon will reveal a quantum state, and the sequence of those quantum states is the key to the unbreakable onetime pad cipher. Now consider Eve eavesdropping on their conversation. According to the No-Cloning theorem, Eve would not be able to reproduce an identical photon to send to Bob, a crucial step to decipher their code. The absence of a photon on Bob’s side is inconsequential in the creation of the key since Alice ignores missing or incorrect guesses during the comparison phase. Quantum cryptography will allow truly secure methods of communication through the realization of a reliable and efficient single photon source.
Quantum computing and its underlying tools and properties, including quantum entanglement and single photon sources, will revolutionize the world of code-makers and code-breakers. All previously devised means of secure communication will be rendered useless when faced with a quantum computational machine capable of solving conventional encryptions. Furthermore, quantum cryptography will allow secure transportation of information because of the uncertainties of quantum particles.
Bibliography

Rivest Ronald L.; Shamir Adi; Adleman Leonard M.; (1977), U.S. Patent 4,405,829


Peter Shor (1994), Shor’s Algorithm

