Quantum cryptography essay sample

Engineering

I. Introduction

Privacy is paramount when communicating sensitive information, and humans have invented some unusual ways to encode their conversations. Quantum cryptography describes the use of quantum mechanical effects (in particular quantum communication and quantum computation) to perform cryptographic tasks or to break cryptographic systems. The goal of quantum cryptology is to thwart attempts by a third party to eavesdrop on the encrypted message.

II. QUANTUM CRYPTOGRAPHY

Cryptology is the process of encoding (cryptography) and decoding (crypto analysis) information or messages (called plaintext). All of these processes combined are cryptology. Earlier cryptology was based on algorithms — a mathematical process or procedure which were created by a sender and transmitted to a receiver. These algorithms are used in conjunction with a key, a collection of bits (usually numbers). Without the proper key, it’s virtually impossible to decipher an encoded message, even if you know what algorithm to use. In modern cryptology, the third party (adversaries) can passively intercept sender and receiver’s encrypted message — he can get his hands on the encrypted message and work to decode it without the sender and receiver knowing he has their message. The adversary can accomplish this in different ways, such as wiretapping sender or receiver’s phone or reading secure e-mails. Quantum cryptology is the first cryptology that safeguards against passive interception as photons come into play. Since we can’t measure a photon without affecting its behaviour, Heisenberg’s Uncertainty Principle emerges when the third party makes his own eavesdrop measurements.

A. Photon Properties:

Photons are some pretty amazing particles. They have no mass, they’re the smallest measure of light, and they can exist in all of their possible states at once, called the wave function. This means that whatever direction a photon can spin in — say, diagonally, vertically and horizontally — it does all at once. Light in this state is called unpolarized. This is exactly the same as if we constantly moved east, west, north, south, and up-and-down at the same time. The foundation of quantum physics is the unpredictability factor. This unpredictability is pretty much defined by Heisenberg’s Uncertainty Principle. This principle says, essentially, that it’s impossible to know both an object’s position and velocity — at the same time. But when dealing with photons for encryption, Heisenberg’s principle can be used to our advantage. To create a photon, quantum cryptographers use LEDs — light emitting diodes, a source of unpolarized light.

LEDs are capable of creating just one photon at a time, which is how a string of photons can be created, rather than a wild burst. Through the use of polarization filters, we can force the photon to take one state or another — or polarize it. If we use a vertical polarizing filter situated beyond a LED, we can polarize the photons that emerge: The photons that aren’t absorbed will emerge on the other side with a vertical spin (|). The thing about photons is that once they’re polarized, they can’t be accurately measured again, except by a filter like the one that initially produced their current spin. So if a photon with a vertical spin is measured through a diagonal filter, either the photon won't pass through the filter or the filter will affect the photon's behaviour, causing it to take a diagonal spin. In this sense, the information on the photon's original polarization is lost, and so, too, is any information attached to the photon's spin.

A. Working:

Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. A photon becomes a key and information is attached to its spin using the usual binary code. Each type of a photon's spin represents one piece of information — usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 11100100110 could correspond with h-e-l-l-o. So a binary code can be assigned to each photon — for example, a photon that has a vertical spin (|) can be assigned a 1. The sender can send his photons through randomly chosen filters and record the polarization of each photon. He will then know what photon polarizations receiver should receive.

Suppose the sender A sends the receiver B his photons using an LED, he'll randomly polarize them through any filter so that each polarized photon has one of four possible states: (|), (–), (/) or ( ). As B receives these photons, he decides whether to measure each with any of the filters — he can't use all the filters together. B has no idea what filter to use for each photon, he's guessing for each one. After the entire transmission, B and A have a non-encrypted discussion about the transmission. The reason this conversation can be public is because of the way it's carried out. B calls A and tells him which filter he used for each photon, and A tells him whether it was the correct or incorrect filter to use. Their conversation may sound a little like this: • B: Plus A: Correct

- B: Plus A: Incorrect
- B: X A: Correct

Since B isn’t saying what his measurements are — only the type of filter he used — a third party listening in on their conversation can’t determine what the actual photon sequence is. Here’s an example. Say A sent one photon as a (/) and B says he used a + filter to measure it. A will say “ incorrect” to B. But if B says he used an X filter to measure that particular photon, A will say “ correct.” A person listening will only know that that particular photon could be either a (/) or a ( ), but not which one definitively. B will know that his measurements are correct, because a (–) photon traveling through a + filter will remain polarized as a (–) photon after it passes through the filter. After their odd conversation, A and B both throw out the results from B’s incorrect guesses. This leaves A and B with identical strings of polarized protons. It might look a little like this: — / | | | / — — | | | — / | … and so on. To A and B, this is a meaningless string of photons. But once binary code is applied, the photons become a message. B and A can agree on binary assignments, say 1 for photons polarized as ( ) and (—) and 0 for photons polarized like (/) and (|).

Fig. 1. Converting unpolarised photon to polarized photon

Fig. 2. Binary codes are being attached to each photon based on their orientation

This means that their string of photons now looks like this: 11110000011110001010. Which can in turn be translated into English, Spanish, Navajo, prime numbers or anything else the B and A use as codes for the keys used in their encryption.

III Conclusions

Advantages of Quantum Cryptography lies in the fact that it allows completion of various cryptographic tasks that are conjectured to be impossible using only classical applications. In predictive sense quantum cryptography may become a technological reality; it is therefore important to study cryptographic schemes (supposedly) secure even against adversaries with access to a quantum computer. In practical sense various confidential research work that has to be passed to defence development centers needs to be protected from adversaries. And also data transmitted through WWW using Quantum Cryptography cannot be wiretapped when compared to other traditional transmission methods and hence limits the cyber warfare adding to this personal medical data of individuals pertaining to fatal diseases needs to be kept confidential in the interest of both citizens and the country.

All these can be achieved securely and efficiently using Quantum Cryptography.

Acknowledgment

We would like to thank all the members of ISTE-PESCE chapter and other contributors for giving us this prolific platform to present our views on the above mentioned topic. We would also like to thank CS&E faculty, our seniors and fellow classmates for extending their support.

References

1] Security of continuous variable quantum key distribution- A. Leverrier, E. Karpov, P. Grangier and N. J. Cerf J. 2] Optical Networking for Quantum key Distribution and Quantum Communication.- T. E Chapuran, N. A. Peter, Jackle and M. S. Goodman. 3] Engineering Physics-P Basavaraju

4] Wikipedia

5] www. howstuffworks. com