Nishant Mehta / International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.1411-1413

Traditional Cryptography versus Quantum Cryptography

Nishant Mehta
15/443, Pantnagar, Ghatkopar(East), Mumbai-400075. Maharashtra, India

ABSTRACT
Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). Traditional cryptography created security protocols by intersecting the principles of mathematics, computer science and electronics. An adversary or a cryptanalyst with his determination and the computational power of a soon-to-be available quantum computer can break the security using his resources. This gave rise to the introduction of an entirely new field of cryptology called Quantum Cryptography which makes use of the quantum mechanical effects to make or break the cipher. This paper highlights the need of Quantum Cryptography and also elaborates the basic concept behind it

Keywords - **Bob-Alice-Eve, Eavesdropping, Entanglement, Photons, Quantum**

I. INTRODUCTION

Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called cipher text) .Decryption is the reverse, in other words, it is moving from the unintelligible cipher text back to plaintext. Until the 1990s, cryptology was based on algorithms -- a mathematical process or procedure. These algorithms are used in conjunction with a key, a collection of bits (usually numbers and alphanumeric for advanced ones). Without the proper key, it's virtually impossible to decipher an encoded message, even if you know what algorithm has been used for encoding. [1][2]

II. KEYEMPLOYMENT TECHNIQUES

There are limitless possibilities for keys used in cryptology. But there are only two widely used methods of employing keys: public-key cryptology and secret-key cryptology.

Public Key Cryptography(PKC)

In the public-key cryptology (PKC**)** method, a user chooses two interrelated keys. He lets anyone who wants to send him a message know how to encode it using one key. He makes this key public. The other key he keeps to himself. In this manner, anyone can send the user an encoded message, but only the recipient of the encoded message knows how to decode it. Even the person sending the message doesn't know what code the user employs to decode it

Secret Key Cryptography(SKC)

The other usual method of traditional cryptology is secret-key cryptology (SKC)**.** In this method, only one key is used by both Bob and Alice. The same key is used to both encode and decode the plaintext. Even the algorithm used in the encoding and decoding process can be announced over an unsecured channel. The code will remain un-cracked as long as the key used remains secret.[11]

III. NEED FOR QUANTUM CRYPTOGRAPHY

Both the secret-key and public-key methods of cryptology have unique flaws. The problem with public-key cryptology is that it's based on the staggering size of the numbers created by the combination of the key and the algorithm used to encode the message. These numbers can reach unbelievable proportions. They can be made so that in order to understand each bit of output data, you have to also understand every other bit as well. This means that to crack a 128-bit key, the possible numbers used can reach upward to the 10^{38} power. That's a lot of possible numbers for the correct combination to the key.

The keys used in modern cryptography are so large, in fact, that a billion computers working in conjunction with each processing a billion calculations per second would still take a trillion years to definitively crack a key. This isn't a problem now, but it soon will be. Current computers will be replaced in the near future with quantum computers, which exploit the properties of physics on the immensely small quantum scale. Since they can operate on the quantum level, these computers could operate at speeds no computer in use now could possibly achieve. So the codes that would take a trillion years to break with conventional computers could possibly be cracked in much less time with quantum computers. This means that secret-key cryptology (SKC)

looks to be the preferred method of transferring ciphers in the future.

But SKC has its problems as well. The chief problem with SKC is how the two users agree on what secret key to use. The problem with secret-key cryptology is that there's almost always a place for an unwanted third party to listen in and gain information the users don't want that person to have. This is known in cryptology as the key distribution problem.[9]

IV. QUANTUM CRYPTOLOGY

Quantum physics has provided a way around the problem that appears while using traditional methods of cryptography. By harnessing the unpredictable nature of matter at the quantum level, physicists have figured out a way to exchange information on secret keys. The introduction of the concept of quantum physics has revolutionized the field of cryptology. 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.

Photon Properties

Photons are some zero-mass particles. They are 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. 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 i.e. 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 (|). [7]

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 behavior, 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.

Using Quantum Cryptology

Binary code is the way of attaching information data to a photon's spin. 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. For all cryptographic purposes, the sender is called Alice, the receiver Bob and the eavesdropper or the third party adversary is called Eve.

Thus, in order to transmit secure data, Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive. Alice randomly polarizes the photons through either the X or the + filters, so that each polarized photon has one of four possible states: (|), (--), (/) or ( ). As Bob receives these photons, he guesses and decides whether to measure each with either his + or X filter. After the entire transmission, Bob and Alice have a non-encrypted discussion about the transmission. Bob calls Alice and tells her which filter he used for each photon, and she tells him whether it was the correct or incorrect filter to use. Since Bob isn't saying what his measurements are but only the type of filter he used. A third party listening in on their conversation can't determine exactly what the actual photon sequence is. This eliminates the need of the conversation being carried out in private and under strict security. [8]

Introduction to the eavesdropper(Eve)

In modern cryptology, Eve (E) can passively intercept Alice and Bob's encrypted message and can get her hands on the encrypted message and work to decode it without Bob and Alice knowing she has their message. Quantum cryptology is the first cryptology that safeguards against passive interception. Since we can't measure a photon without affecting its behavior, Heisenberg's Uncertainty Principle emerges when Eve makes her own eavesdrop measurements. Thus if Eve tries to intercept the message, it inadvertently changes the polarization of the photon and thus Bob receives incorrect data which will be noticed when

Bob and Alice discuss the data obtained after the transmission has taken place.[10]

V. CONCLUSION

Despite all of the security it offers, quantum cryptology also has a few fundamental flaws. Chief among these flaws is the length under which the system will work. The reason why the length of quantum cryptology capability is so short is because of interference. A photon's spin can be changed when it bounces off other particles, and so when it's received, it may no longer be polarized the way it was originally intended to be. One group of Austrian researchers may have solved this problem by using what Albert Einstein called "spooky action at a distance." This observation of quantum physics is based on the entanglement of photons. At the quantum level, photons come to depend on one another after undergoing some particle reactions, and their states become entangled. This entanglement doesn't mean that the two photons are physically connected, but they become connected in a way that physicists still don't understand. In entangled pairs, each photon has the opposite spin of the other -- for example, (/) and ( ). If the spin of one is measured, the spin of the other can be deduced. The strange thing about the entangled pairs is that they remain entangled, even when they're separated at a distance. A group of researchers from Massachusetts Institute of Technology took advantage of another property of entanglement. In this form, two states of a single photon become related, rather than the properties of two separate photons. By entangling the photons the team intercepted, they were able to measure one property of the photon and make an educated guess of what the measurement of another property -- like its spin -- would be. By not measuring the photon's spin, they were able to identify its direction without affecting it. So the photon travelled down the line to its intended recipient none the wiser.

ACKNOWLEDGEMENTS

I, the author, take this opportunity to express our sincere gratitude to Prof. Priti Tyagi, Head of Department(Electronics) and Prof. Leena Govekar for their invaluable support and guidance throughout the entire formation of this paper.

REFERENCES

[1] http://www.crypto-class.org/

[2] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm

[3] http://en.wikipedia.org/wiki/Cryptography

[4] http://en.wikipedia.org/wiki/Quantum_cryptography

[5] http://www.ee.stanford.edu/~hellman/publications/32.pdf

[6] http://en.wikipedia.org/wiki/List_of_important_publications_in_cryptography

[7] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology3.htm

[8] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology4.htm

[9] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology2.htm

[10] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology5.htm

[11] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology1.htm