International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), August 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

QUANTUM CRYPTOGRAPHY

Maneesha Bisht[1], Jyoti Kumari[2]

[1,2]Department of Computer Science and Engineering, JIET Group of Institutions, Jodhpur, (India)

ABSTRACT

Quantum cryptography is a technology that ensures ultimate security. Compared to current cryptography that could be defeated by the development of an ultra-high-speed computer, quantum cryptography ensures secure communication because it is based on the fundamental physical laws. It is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light. Quantum cryptography is a new method for secret communications offering the ultimate security assurance of the inviolability of a Law of Nature. The quantum cryptography relies on two important elements of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization. This research paper concentrates on the principle of quantum cryptography, and how this technology contributes to the network security. This paper outlines the real world application implementation of this technology and the future direction in which quantum cryptography accelerates. The discovery of the content of such data could lead to very serious consequences. These include the misuse of bank account numbers, identity information, items relating to military security and other sensitive information. Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure.

Keywords: Quantum Cryptography, Network Security, Quantum Key Distribution (QKD)

I. INTRODUCTION

Cryptography is literally the art of "secret writing". It is used to secure communication by protecting the confidentiality and integrity of messages and sensitive data. Without it, anyone could read a message or forge a private conversation. Messages are made secret by transforming them from "plaintext" into "cipher text" using a cipher and performing the process of encryption. Decryption turns scrambled and unreadable cipher text back into plaintext. When cryptographers talk about a "key", they are referring to a shared secret that controls the ability to hide and unhide information. There are two types of cryptography that are often referred to as "symmetric key" and "public key"

cryptography:

1. In symmetric key cryptography, the same key is used for both encryption and decryption, and that key needs to be kept a secret by everyone who is sending and receiving private messages. The major difficulty of symmetric key cryptography is to provide the secret keys to legitimate parties without divulging the keys to eavesdroppers. 2. Public key cryptographyis more involved and complex. There are two keys, one for encrypting and another key for decrypting. The two keys are mathematically related, and only one key is intended to be kept a secret. Public key cryptography allows anyone to send an encrypted message, but only one

person, with the private key, can decrypt the message. Public key cryptography can also be used for digital signatures where someone with a private key can sign a message that anyone can verify with the public key [1].

II. MECHANICS OF QUANTUM CRYPTOGRAPHY

The quantum cryptography depends on two important components of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization. The Heisenberg Uncertainty principle states that, it is impossible to determine the quantum state of any system without distributing that system. The theory of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem which was first introduced by Wootters and Zurek in 1982.

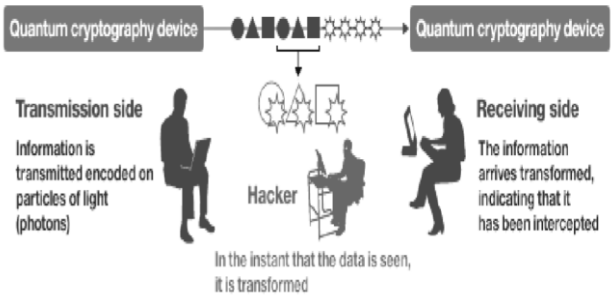

Figure 1: Mechanics of Quantum Cryptography

Depending on the theory of physics, quantum cryptography does not make it possible to eavesdrop on transmitted information. It is attracting considerable attention as a

replacement for other contemporary cryptographic methods, which are based on computational security. Quantum cryptographic transmission encrypts the 0s and 1s of a digital signal on individual particles of light called photons. By contrast, modern optical transmission expresses the 0s and 1s of the digital signal as the strength and weakness of light respectively. Because the strong and weak light are made up of tens of thousands of photons which each convey the same information, if several photons are stolen (i.e., the signal is eavesdropped on) during transmission, it is not detected. On the other hand, in the case of quantum cryptography, if a third party detects (eavesdrops on) the signal, the information on the photons is suddenly transformed, meaning both that it is immediately noticeable that eavesdropping has appeared and that the third party is not able to decrypt the information[2].

III. HOW DOES QUANTUM COMPUTING IMPACT CRYPTOGRAPHY AND SECURITY?

Cryptography plays a very important role in most secure electronic communication systems today because it ensures that only authentic parties can read each other's exchanged messages. Quantum computing threatens the basic goal of secure, authentic communication because in being able to do certain kinds of computations that conventional computers cannot, cryptographic keys can be broken quickly by a quantum computer and this allows an eavesdropper to listen into private communications and pretend to be someone whom they are not. Quantum computers accomplish this by quickly reverse calculating or guessing secret cryptographic keys, a task that is considered very hard and improbable for a conventional computer. A quantum computer cannot break all types of cryptographic keys and some cryptographic algorithms in use today are also safe to use in a world of

widespread quantum computing. The following sections will describe which types of cryptography are safe from quantum attacks and which ciphers, protocols and security systems are most vulnerable.

IV. TECHNOLOGY SURVEY – CURRENT STATE OF THE ART

Some of the most important people responsible for the ongoing strength of our security tools are the people who try to break them. At the network level this includes approaches such as penetration testing, or sometimes security research, and at the cryptography level it is called cryptanalysis. The researchers that perform this level of testing are exceptionally creative when it comes to circumventing security systems or compromising ciphers and it is directly because of their research and efforts that state-of-the-art tools and ciphers are constantly improved. Security research and cryptanalysis is a long practiced art form. The designers of security products are so accustomed to people trying to break their security systems that they build in redundant controls and layer these controls so that, over time, if a particular safeguard fails then the security of the system may still be recovered. With regards to cryptography, security architects will also design in recoverable security features, for instance, if a cipher is broken or discovered to be weak then the system can accommodate with a change in key size, parameter, or possibly even a new cipher or cipher suite combination. Many generic security protocols have some form of cryptographic agility, but in most cases, the only public key cryptography options designed into these protocols are variants of RSA or ECC, as well as Diffie Hellman for key exchange, which from the perspective of quantum computing are not resilient against quantum attacks. Even if the protocols support other algorithms, RSA and ECC are the most widely deployed in practice. RSA and ECC are the most popular and pervasive public key cryptographic algorithms in use today due to their historical precedent as well as their efficiencies. RSA was the first practical public-key cryptosystem discovered and was built into early versions of the Secure Sockets Layer (SSL) protocol; ECC was the first algorithm discovered after RSA to offer considerably smaller keys and comparable-speed operations. Unfortunately, due to Shor's algorithms and the progressing maturity of quantum computing, ECC and RSA will become increasingly vulnerable to quantum attacks over time. Changing from classical algorithms to quantum safe algorithms is not a simple task. It takes a long time for a particular algorithm to be accepted by security practitioners, researchers and standards bodies. Classical algorithms like ECC and RSA are widely studied and well accepted by the security community. Quantum safe algorithms have been around for a long time, but have not benefited from nearly as much public scrutiny and cryptanalysis, so they are less prevalent in standards and a difficult feature to find in security products.

V. QUANTUM KEY DISTRIBUTION

One of the proposed solutions to the key distribution problem is known as Quantum Key Distribution (QKD). There do exist alternative key distribution algorithms using public key schemes that are not RSA or ECC. However, in contrast to these public key schemes, QKD as a cryptographic primitive offers security that is guaranteed by the laws of physics. QKD as a method for secure key establishment [GIS02] is proven to be information theoretically secure against arbitrary attacks, including quantum attacks. This means that even assuming an adversary to have unlimited computational resources, including unlimited classical and quantum

computing resources, QKD is secure now and always will be. By enabling provable security based on fundamental laws of quantum physics, QKD remains resilient even to future advances in cryptanalysis or in quantum computing. Consequently, quantum key distribution provides the means to securely distribute secret keys that can be used with quantum safe symmetric key algorithms like Advanced Encryption Standard (AES), or one-time pad encryption. Conceptually, the security of QKD is achieved by encoding information in quantum states of light. Using quantum states allows security to be based on fundamental laws in quantum physics and quantum information theory. There are three deeply related notions from quantum physics that illustrate the source of the unique security properties of QKD:

1. The Heisenberg uncertainty principle implies that by measuring an unknown quantum-mechanical state, it is physically changed. In the context of QKD, this means that an eavesdropper observing the data stream will physically change the values of some of the bits in a detectable way.
2. The no cloning theorem states that it is physically impossible to make a perfect copy of an unknown quantum state. This means that it is impossible for an adversary to make a copy of a bit in the data stream to only measure one of the copies in hopes of hiding their eavesdropping.
3. There exist properties of quantum entanglement that set fundamental limits on the information leaked to unauthorized third parties.

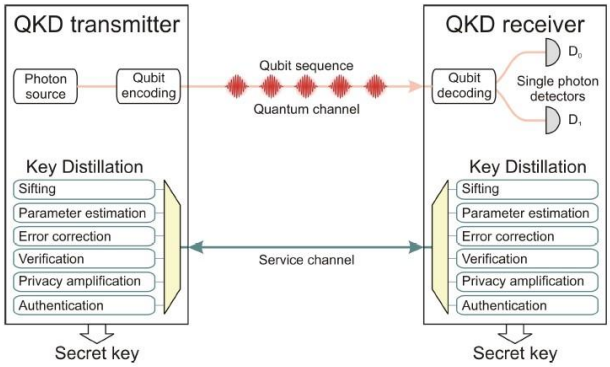

Figure 5 - Illustration of a typical prepare-and measurement QKD setup.

Importantly, these are not technological limitations that can be overcome by clever advances in engineering, but rather are fundamental and irrefutable laws of quantum physics. Interestingly, due to the laws of quantum mechanics, it is physically impossible for an adversary to invisibly eavesdrop on quantum key distribution. Looking at the information encoded in quantum states actually changes the information in ways that can be detected by the legitimate parties. The mere act of her observing the data in transmission will physically change the bits of information in the data stream and introduce errors in ways that the sender and recipient can readily detect and quantify. The percentage of errors which an eavesdropper necessarily introduces allow the sender and recipient to calculate not only whether an eavesdropper was present, but also precisely how much of the information about the key the adversary could have gained in the worst possible case with the most powerful algorithms and hardware. This allows them to use well-studied post- processing methods to remove any information an eavesdropper could have gained about the shared key. An important characteristic of quantum key distribution is that any attack (e.g. any attempt to exploit a flaw in an implementation of transmitters or receivers) must be carried out in real time. Contrary to classical cryptographic schemes, in QKD there is no way

to save the information for later decryption by more powerful technologies. This greatly reduces the window of opportunity for performing an attack against QKD; the window is much wider for conventional cryptography.

The security of QKD has been proven in a number of frameworks including the universal composability [BHL05, Sca09], the abstract cryptography framework [MAU11], or the authenticated key exchange framework [MSU13]. The composability of QKD as a cryptographic primitive allows safely combining the distributed keys with other provably secure schemes such as Wegman-Carter authentication or onetime pad encryption while maintaining quantifiable long term security [3].

VI. BENEFITS OF QUANTUM SAFE SECURITY

Agency which decoded foreign diplomatic codes; the work performed by British GCHQ to solve World War II era ciphers, leading to breakthroughs in computation and machine computing; the advent of wide scale commercial use of cryptography starting in the 1970's with the invention of DES through research performed at IBM. Popular documentaries are broadcast on television that glamorize encryption systems that have come and gone over past decades, and when these cryptographic systems fade, they are always replaced with stronger, faster algorithms and technologies because the global research community is forever redefining the state of the art. If history can be used to accurately predict events yet to come, then breaking a cryptographic cipher can have catastrophic repercussions for anyone using a cipher who is ignorant of its compromise. And great advantages are bestowed upon anyone who takes advantage of their adversary's ignorance. If history can be used to accurately predict events yet to come, then breaking a cryptographic cipher can have catastrophic repercussions for anyone using a cipher who is ignorant of its compromise. And great advantages are bestowed upon anyone who takes advantage of their adversary's ignorance.

VII.CHALLENGES FOR QUANTUM SAFE SECURITY

Many of the challenges for the adoption of quantum safe security are rooted in common best practices within the security industry. Very early in their careers security practitioners are taught to avoid new cryptographic algorithms that have not received years of public scrutiny, to not design their own security protocols, and rely on well-established security standards.

1. **Confidence in Algorithms**. There are many well-studied public key based cryptographic algorithm options that could be used as a substitute for RSA or ECC, however, many of these substitutes do not have the benefit of wide spread practical use.
2. **Rigidity of Security Protocols**. Quantum safe ciphers may not fit into an established protocol because of historical protocol design assumptions, key size choices and tolerance for message expansion. Earlier sections in this whitepaper give examples of common security protocols that demonstrate the varying degree to which quantum safe cryptography can be used effectively. Many protocols were not designed with cryptographic agility in mind, and may not easily accommodate a change of cipher.
3. **Perception of non-urgency.** An exact date for the arrival of general purpose quantum computing cannot be given, however, global interest is growing and steady progress is being made. As quantum computing matures, computer security weakens. Some businesses require their security to have medium longevity in

the sense that confidential information that is worth protecting now, will also remain sensitive and should be kept private a year or two in the future. Other businesses require their security to have greater longevity, keeping information private for decades. Quantum safety is "not urgent" only for those with short term security needs but any business that requires its secrets to remain secret will need to consider their quantum safe transition strategy now. A quantum attack is just as effective at divulging all past communications, i.e. encrypted military information residing on physical storage medium.

VIII. APPLICATION OF QUANTUM CRYPTOGRAPHY

The most infamous and developed application of quantum cryptography is quantum key distribution (QKD). Quantum key distribution [3] is a method used in the framework of quantum cryptography in order to produce a perfectly random key which is shared by a sender and a receiver while making sure that nobody else has a chance to learn about the key, e.g. by capturing the communication channel used during the process. The best known and popular scheme of quantum key distribution is based on the Bennet–Brassard protocol (i.e. BB84), which was invented in 1984. It depends on the no-cloning theorem [4], for non-orthogonal quantum states. Briefly, the Bennet–Brassard protocol works as follows:

- The sender (usually called Alice) sends out a series of single photons. For each photon, it arbitrarily selects one of two possible base states, with one of them having the possible polarization directions up/down and left/right, and the other one polarization directions which are angled by 45°. In each case, the actual polarization direction is also arbitrarily selects.
- The receiver (called Bob) detects the polarizations of the incoming photons, also randomly selecting the base sates.

  This means that on average half of the photons will be determined with the "wrong" base states, i.e. with states not corresponding to those of the sender.
- Later, Alice and Bob use a public communication channel to talk about the states used for each photon (but not on the chosen polarization directions). In this way, they can find out which of the photons were by chance preserved with the same base states on both sides.
- Then they reject all photons with a "wrong" basis, and the others signify a sequence of bits which should be identical for Alice and Bob and should be known only to them, provided that the transmission has not been influenced by anybody. Whether or not this happened they can test by comparing some number of the obtained bits via the public information channel. If these bits agree, they know that the other ones are also correct and can finally be used for the actual data transmission.

IX. CONCLUSIONS AND OPPORTUNITIES FOR FURTHER WORK

We presented an aspect of the workings of quantum cryptography and quantum key distribution technology. This technology is basically depends upon the polarization of photons, which is not a well regulated quantity over long distances and in multi-channel networks. Quantum cryptography could be the first attention of quantum mechanics at the single quanta level. Quantum cryptography promises to reform secure communication by providing security based on the elementary laws of physics, instead of the current state of mathematical

algorithms or computing technology. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, such systems could start encrypting some of the most valuable and important secrets of government and industry. For now, non-quantum cryptography is very secure, because it depends on algorithms that can't be broken in less than the lifetime of the universe by all the currently existing computers. So in theory, there is not much demand for quantum cryptography yet; thus, we don't know when this technology will take a step forward and quantum cryptography techniques will become essential to protect our information. When quantum computers will come into play, the computational speeds will increase considerably, so the mathematical complexity of algorithms will become less of a challenge. It is still arguable whether or not it will be possible to simply increase the numbers use in the algorithms and thus increase the complexity enough to outrun even quantum computer. Yet there is no question about the fact that quantum cryptography is a true invention in the field. It is still being refined and developed further. However, already it had been clear that even with its current defectiveness, it is many steps above everything that was settled before it. All we need is some years, or maybe decades or even centuries, to renew this method and make it feasible in the real world.

REFERENCES

[1] Matthew Campagna, Ph.D., IQC Affiliate., Lidong Chen, Ph.D, Mathematician, National Institute of Standards and Technology, "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges".

[2] Miss. Payal P. Kilor, Mr.Pravin.D.Soni, "Quantum Cryptography: Realizing next generation information security", feb 2014

[3] Mehrdad S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System". 2009, pp. 1644-1648.

[4] C. H. Bennett and G. Brassard, "QuantumCryptography: Public Key Distribution and Coin Tossing", In Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pp. 175-179, December 1984. (Bennet–Brassard protocol).