International Journal of Power System Operation and Energy Management

Volume 1 | Issue 1 Article 4

January 2012

QUANTUM CRYPTOGRAPHY: A NEW APPROACH TO INFORMATION SECURITY

Rishi Dutt Sharma
Computer science department Ambedkar Institute of Technology G.G.S.I.P.U, NEW DELHI,
rishi.abes@gmail.com

Recommended Citation

Sharma, Rishi Dutt (2012) "QUANTUM CRYPTOGRAPHY: A NEW APPROACH TO INFORMATION SECURITY," *International Journal of Power System Operation and Energy Management*: Vol. 1 : Iss. 1 , Article 4.
DOI: 10.47893/IJPSOEM.2011.1003
Available at: https://www.interscience.in/ijpsoem/vol1/iss1/4

QUANTUM CRYPTOGRAPHY: A NEW APPROACH TO INFORMATION SECURITY

Rishi Dutt Sharma
Computer science department
Ambedkar Institute of Technology
G.G.S.I.P.U, NEW DELHI
rishi.abes@gmail.com

ABSTRACT :

Quantum cryptography is an emerging technology in which two parties can secure network Communications by applying the phenomena of quantum physics. The security of these transmissions is based on the inviolability of the laws of quantum mechanics. Quantum cryptography was born in the early seventies when Steven wiesner wrote "conjugate coding". The quantum cryptography relies on two important elements of quantum mechanics-the Heisenberg uncertainty principle and the principle of photon polarization. The Heisenberg uncertainty principle states that, it is not possible to measure the quantum state of any system without distributing that system. The principle of photon polarization states that, an eavesdropper cannot copy unknownqubits i.e. unknown quantum states, due to no-cloning Theorem which was first presented by wootters andzurek in 1982.this research paper concentrates on the theory of quantum cryptography, and how this technology contributes to the network security. This research paper summarizes the current state of Quantum cryptography, and the real world application implementation of this technology and finally the future direction in which quantum cryptography is forwards

I. Introduction

The purpose of cryptography [1] is to transmit information in such a way that access to it is restricted entirely to the intended recipient, even if the transmission itself is received by others. This science is of increasing importance with the advent of broadcast and network communication, such as electronic transactions, the Internet, e-mail, and cell phones, here sensitive monetary, business, political, and personal communications are transmitted over public channels. Cryptography operates by a sender scrambling or encrypting the original message or plaintext in a systematic way that obscures its meaning. The encrypted message or crypto-text is transmitted, and the receiver recovers the message by crumbling or decrypting the transmission Existing cryptographic techniques are usually identified as "traditional" or "modern." Traditional techniques use operations of coding (use of alternative words or phrases), transposition (reordering of plaintext), and substitution (alteration of plaintext characters). Traditional techniques were designed to be simple, for hand encoding and decoding. By contrast, modern techniques use computers, and rely on extremely long keys, convoluted algorithms, and intractable problems to achieve assurances of security. There are two branches of modern cryptographic techniques: public key encryption [2] and secret key encryption [1,2]. In Public Key Cryptography, messages are exchanged using an encryption method so convoluted that even full disclosure of the scrambling operation provides no useful information for how it can be undone. Each participant has a "public key" and a "private key"; the former is used by others to encrypt messages, and the latter is used by the participant to decrypt them.

The main practical problem with secret key encryption is exchanging a secret key. In principle any two users who wished to communicate could first meet to agree on a key in advance, but in practice this could be inconvenient. Other methods for establishing a key, such as the use of secure courier or private knowledge, could be impractical for routine communication between many users. But any discussion of how the key is to be chosen that takes place on a public communication channel could in principle be cepted and used by an eavesdropper. According to quantum theory [4], light waves are opagated as discrete particles known as photons. A photon is a mass-less particle, the quantum of the electromagnetic field, carrying energy, momentum, and angular momentum. Entangled pairs" [8] are pairs of photons generated by certain particle reactions. Each pair contains two photons of different but related polarization. Entanglement affects the randomness of measurements. If we measure a beam of photons E1 with a polarization filter, one-half of the incident photons will pass the filter, regardless of its orientation. Whether a particular photon will pass the filter is random. However, if we measure a beam of photons E2 consisting of entangled companions of the E1 beam with a filter oriented at 90 degrees (deg) to the first filter, then if an E1 photon passes its filter, its E2 companion will also pass its filter. Similarly, if an E1 photon does not pass its filter then its E2 companion will not.

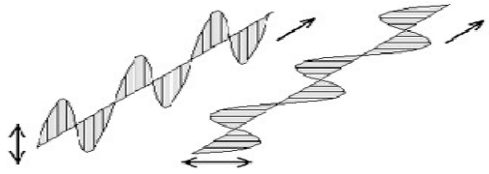

Fig.1: Diagram showing vertically and horizontally polarized light.

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from

simultaneously knowing the value of the other. In particular, when measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements. Quantum cryptography, or quantum key distribution (QKD) [9], uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. An important and unique property of quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key.

Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. Quantum cryptography is different from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model. Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages. The genius of quantum cryptography is that it solves the problem of key distribution. A user can suggest a key by sending a series of photons with random polarizations. This Sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail. In the past few years, a remarkable surge of interest from international scientific and business communities has propelled QC into mainstream computer science and physics. Furthermore, new developments are making QC increasingly practical. The first QC experiment worked over a distance of 32cm in 1989, and today, it is performed over distances of hundreds of kilometers using optical fibers.

II. WORK ALREADY DONE IN THE FIELD

A. BB84 Encoding Scheme:

The security of the BB84 protocol comes from encoding the quantum information in nonorthogonal states, where BB84 uses two pairs of states with each pair conjugate to the other and the two within a pair being orthogonal to each other. The typical polarization state pairs used are rectilinear Basis of vertical (0) and horizontal (90), the diagonal basis of 45 and 135 or the circular basis of left- and right-handed. All three of these bases are conjugate to each other, so any two can be used together.

B. B92 Encoding Scheme:

The B92 encoding scheme was developed by Charles Bennett in 1992. This quantum encoding protocol is similar to the BB84, but uses only two of the four BB84 states, 0 and 45 to represent 0 and 1.Using B92, Sender would encode the bits in two nonorthogonal BB84 states in a way that no one can determine a bit with certainty, because no measurement can distinguish between two nonorthogonal quantum states.

C. Ekert Encoding Scheme:

The Ekert Scheme was developed by Arthur Ekert in 1991, which uses entangled pairs of photons. These photon pairs can be created by sender, receiver or a third party. These pairs are created by splitting a single photon into two, using a laser. After the split, one of the photons is sent by the sender or on behalf of the sender to the receiver while the other photon is kept.

III. QUANTUM CRYPTOGRAPHY TECHNOLOGIES

Experimental implementations of quantum cryptography have existed since 1990, and today quantum cryptography is performed over distances of 30-40 kilometers using optical fibers. Essentially, two technologies make quantum key distribution possible: the equipment for creating single photons and that for detecting them. The ideal source is a so-called photon gun that fires a single photon on demand. As yet, nobody has succeeded in building a practical photon gun, but several research efforts are under way. Some researchers are working on a light emitting p-n junction that produces well-spaced single photons on demand. Others are working with a diamond-like material in which one carbon atom in the structure has been replaced with nitrogen. That substitution creates a vacancy similar to a hole in a type semiconductor, which emits single photons when excited by a laser. Many groups are also working on ways of making single ions emit single photons. None of these technologies, however, is mature enough to be used in current quantum cryptography experiments. As a result, physicists have to rely on other techniques that are by no means perfect from a security viewpoint. Most common is the practice of reducing the intensity of a pulsed laser beam to such a level that, on average, each pulse contains only a single photon.

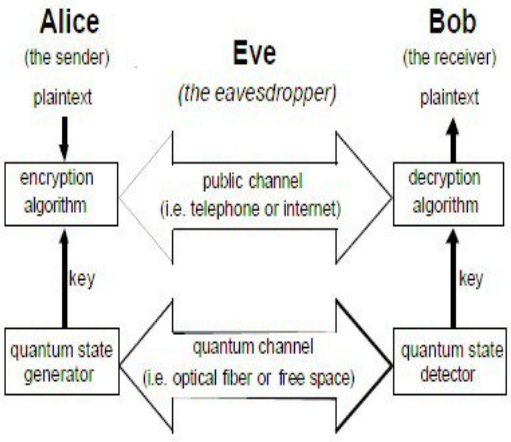

Fig. [2]: A Quantum Cryptographic communication system for securely transferring random key

The problem here is the small but significant probability that the pulse contains more than one photon. This extra photon is advantageous for the hacker, who can exploit the information it contains without sender and receiver being any the wiser. Single-photon detection is tricky too. The most common method exploits avalanche photodiodes.
These devices operate beyond the diode's breakdown voltage, in what is called Geiger mode. At that point, the energy from a single absorbed photon is enough to cause an electron avalanche, an easily detectable flood of current. But these devices are far from perfect. To detect another photon, the current through the diode must be quenched and the device reset, a time consuming process. Furthermore, silicon's best detection wavelength is 800 nanometers (nm, where 1 nm = one one-billionth of a meter), and it is not sensitive to wavelengths above 1100 nm, well short of the 1300- and 1550-nm standards for telecommunication. At telecommunications wavelengths, germanium (Ge) or indium-gallium-arsenide (InGaAs) detectors must be used, even though they are far less efficient and must be cooled well below room temperature. While commercial single-photon detectors at telecommunications wavelengths are beginning to appear on the market, they still lack the efficiencies useful for quantum cryptography.

IV. PROPOSED METHODOLOGY

Cryptography is a way to combine the relative ease and convenience of key exchange in public key cryptography with the ultimate security of a onetime pad. This research paper describe the various algorithm of quantum key exchange and tries to overcome the limitations associated with the existing algorithm by developing new technique.

V. PROPOSED OUTCOME

Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental 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, if not months, such systems could start encrypting some of the most valuable secrets of government and industry.

VI. REFERENCES

[1] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key- distribution Protocols," Phys. Rev. A vol. 73, 2006.
[2] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," Karlsruhe, Germany: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications 2003..
[3] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," Journal of
[4] Homer, Iliad 6.213, transl. Ian Johnston (in English), Malaspina University-College, Nanaimo, BC, Canada (2000).
[5] Charles Anthon, The first six books of Homer's Iliad with English notes, critical & explanatory, a metrical index, & Homeric glossary, Harper & Brothers, New York, p. 396 (1875).
[6]Old Spartan Factsat http://www.geocities.com/Athens/Aegean/7849/spfacts.html.
[7] D.R. Stinson, Cryptography, Theory and Practice, CRC Press, Inc., Boca Raton, p. 4 (1995).
[8] T.P. Leary, Cryptology in the 15th and 16th Century, Cryptologia 20, No. 3, pp. 223-242 (July 1996).
[9] E.A. Poe, The Gold Bug, in Tales of Mystery and Imagination, Wordsworth Editions Ltd., Ware, pp. 1-46 (1993).
[10] A.C. Doyle, the Adventure of the Dancing Men, in The Annotated Sherlock Holmes, Vol. 2, ed. W.S. Baring-Gould, Wings Books, New Jersey, pp. 527-545 (1992).
[11] G.S. Vernam, Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications, J. AIEE 45, pp. 109-115 (1926). cryptology vol. 18, pp. 133 - 165 200
[12] C. H. Bennett and G. Brassard, "Quantum Cryptography: 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.
[13] D. Mayers,"Unconditional security in quantum cryptography", Journal of the ACM, Vol. 48, No. 3, pp.351-406, May 2001.
[14] P. Shor, J. Priskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters, Vol. 85, pp. 441 - 444, 2000.
[15] P. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms". Proc. of the 35th Annual Symposium on Foundations of Computer Science (FOCS), IEEE Computer Society Press, 124-134,Nov. 1994.