IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13210

A Survey on Quantum Cryptography

M. Pavithra[1], M. Harisha[2]

PG Student, department of Computer Science, R.B. Gothi Jain College for Women, Red hills, Chennai-52[1,2]

Abstract: Quantum cryptography yield a cryptographic solution which is immortal as it reinforces prime secrecy that is applied to quantum public key distribution. It is a noticeable technology wherein two entities can communicate securely with the sights of quantum physics. In classical cryptography, bits are used to encode the information where as quantum cryptography that is quantum computer are uses photons or quantum particles and the photon's polarization which are their quantized attribute to encode the information. This is represented in the qubits which is the unit for quantum cryptography. The transmissions are certain as it is depended on the conclusive quantum mechanics laws. The emphasis of this paper is to be mark the gain of quantum cryptography, its components, quantum key distribution and quantum implementation

Keywords: Photon Polarization Principle, Eaves droppers, Quantum Key Distribution, Classical and Qubits, Alice and Bob, Magiq Technologies.

I. INTRODUCTION

Cryptography is the study of technique of sending messages in restricted form so that only the planned recipient is able to read the message after applying a specific key. The process of converting the message into some hid form is called Encryption. The plain text is converted into cipher text by using several key called as Encryption key. In the receiver's end, the gain of plaintext from cipher text is required.

The process of converting the message into its original figure is called as Decryption. Keys play important role of cryptography. The classification of the cryptographic algorithms is essentially on the type of key used. There has two types of keys-Symmetric (secrete key) and asymmetric (public key). "Quantum cryptography is a system of encryption that is process in the naturally occurred in the properties of quantum mechanics to secure and transmit data in a way of that cannot be hacked".

Rather than depending on the complexity of factoring large numbers, quantum cryptography is established on the fundamental and unchanging principles of quantum mechanics. In reality, quantum cryptography relaxation on two pillars of 20th century quantum mechanics –the Heisen berg Uncertainty principle and the principle of photon polarization. According the Heisenberg Uncertainty principle, it's not available to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light molecule can only be known at the point when it is measured.

This rule plays a critical role in thwarting the attempts of eaves droppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization rule describes how light photons can be oriented or polarized in specific directions. Besides, a photon filter with the correct polarization can only detect a polarized photon or else the photon will be destroyed. It is this "one-way-ness" of photons across with the Heisenberg Uncertainty principle that are make quantum cryptography an attractive option for insuring the privacy of data and defeating eavesdroppers.

II. QUANTUM KEY DISTRIBUTION

Fundamental phase of quantum physics – unitarily, the uncertainty principle, and the Einstein-Podolsk-Rosen violation of Bell's inequalities – now suggest a third paradigm for key distribution: quantum cryptography. As shown in Fig. 1, quantum cryptography – more properly labeled Quantum Key Distribution, QKD – employs two distinct channels. One is used for transmission of quantum key apparatus by very dim (single photon) light pulses.

The additional, public channel carries all message traffic, including the cryptographic Protocols, encrypted user traffic, etc.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13210

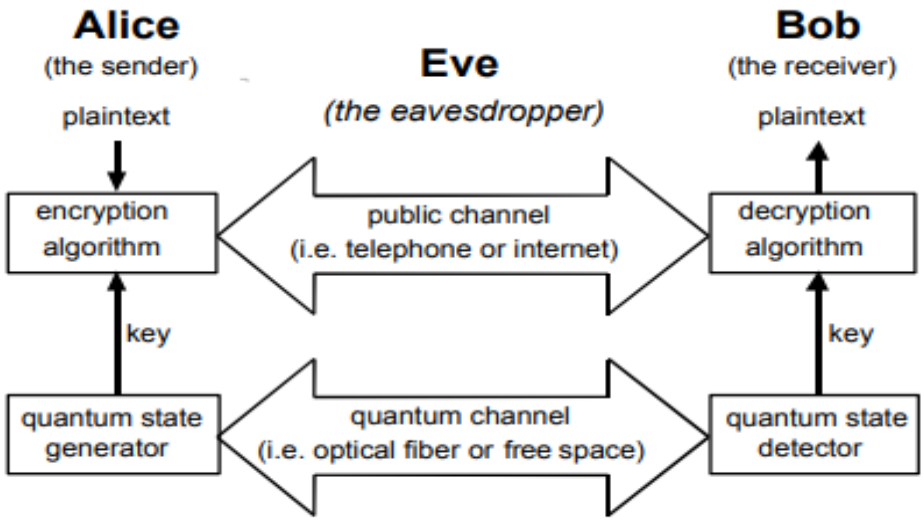
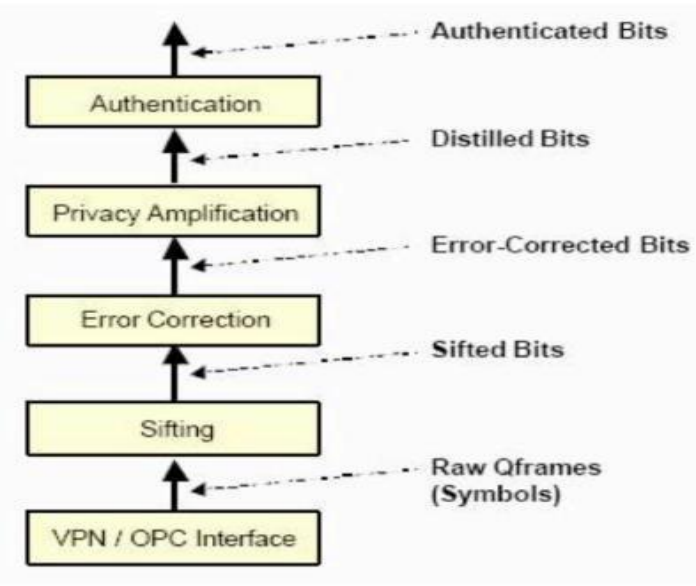


Figure 1. Quantum Key Distribution.

QKD include of the transmission of raw key material, e.g., as dim pulses of light from Alice to Bob, via the quantum channel, plus processing of this raw material to obtain the actual keys. This processing suggests public communication (key agreement protocols) between Alice and Bob, conducted in the public channel, over with specialized QKD algorithms. Under the laws of quantum physics, any eavesdropper (Eve) that snoops on the quantum channel will create a measurable disturbance to the flow of single photons. Alice and Bob can expose this, take appropriate steps in response, and hence foil Eve's attempt at eavesdropping. Quantum cryptography was prospective by Bennett and Brassard in 1984, who also defined the first QKD protocol, called BB84. At time of author, a handful of research teams across the world have succeeded in building and operating quantum cryptographic device.

III. QKD PROTOCOLS IMPLEMENTATION

Quantum cryptography involves a un usually elaborate suite of specialized protocols, which we term "QKD protocols." Many aspects of these protocols are unusual – both in motivation and in implementation – and may be of interest to specialists in communications protocols. Now, we have been showing the protocols now running in our C language QKD protocol implementation. DARPA have designed this engine so it is easy to "plug in" new protocols, and expect to devote considerable time in coming years to inventing new QKD protocols and trying them in practice.



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024
DOI: 10.17148/IJARCCE.2024.13210

1. Sifting

Sifting is the technique wherein Alice and Bob window away all of the obvious "failed q bits" from a sequence of pulses. These screw ups consist of the ones qubits wherein Alice's laser in no way transmitted, Bob's detectors didn't work, photons had been misplaced in transmission, and so forth. They also include those symbols where Alice chose one basis for transmission but Bob chose the other for receiving.

2. Error Correction

Error correction allows Alice and Bob to determine all the "error bits" among their shared, Sifted bits, and accurate them in order that Alice and Bob proportion the equal series of error-corrected bits. Error bits are ones that is Alice transmitted asa0but Bob received as a 1, or vice versa. These bit errors can be caused by noise and by eavesdropping. Error correction in quantum cryptography has been a very unusual constraint, namely, evidence revealed in error detection and correction must be assumed to be known to Eve, and thus to reduce the hidden entropy available for key material. As a result, there's very robust motivation to layout mistakes detection and correction codes that reveal as little as possible in their public control traffic between Alice and Bob.

3. Privacy amplification

Privacy amplification is the process whereby Alice and Bob reduce Eve's knowledge of their shared bits to an acceptable level. This technique is also called advantage distillation. The side that are initiates privacy amplification chooses a linear hash function over the Galois Field GF[2n] where n is the number of bits as input, rounded up to a multiple of 32.

4. Authentication

Authentication lets in Alice and Bob to protect against "guy with inside the center attacks," i.e. lets in Alice to make sure that she is speaking with Bob (and now no longer Eve) and vice versa. Authentication must be performed on an ongoing basis for all key management traffic, since Eve may insert herself into the conversation between Alice and Bob at any stage in their communication.TheauthenticBB84paperdefinedtheauthentication trouble and sketched a method to it primarily based totally on standard households of hash functions, brought with the aid of using Wegman and Carter [20].This technique calls for Alice and Bob to already percentage a small mystery key, which issued to select a hash function from the family to generate an authentication hash of the public correspondence between them.

CLASSICALANDQUBITS:

1. Classical Bits

The classical information is represented using by the classical bits i.e. 0 and 1. Classical cryptography works on classical bits. Quantum cryptography acts on quantum bits also called as qubits. A qubit can be in the superposition between zero and one. Qubits are the different from classical bits for example, they cannotbe copied.

2. Qubits

A state of a qubit can be characterized as a 2-dimentional ket vector, therefore

$$|\Psi> \epsilon C^2 \quad |\Psi> = \alpha|0> + \beta|1>$$

where α and $\beta \in \mathbb{C}$ and are the amplitudes. And,

$$|\alpha|^2 + |\beta|^2 = 1$$

Inner product helps us to choose upon whether the qubit is a valid qubit.

$$<\Psi|1\Psi> = <\Psi|\Psi>$$

$$<\Psi|\Psi> = (\alpha^* \beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha^*\alpha + \beta^* \beta = |\alpha|^2 + |\beta|^2 = 1$$

1. The DARPA Quantum Network

The DARPA security ideal is the cryptographic Virtual Private Network (VPN). Conventional VPNs use both public-key and symmetric cryptography to accomplish confidentiality and authentication/integrity. Public-key mechanisms help key exchange or agreement, and authenticate the endpoints.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024
DOI: 10.17148/IJARCCE.2024.13210

Symmetric mechanisms (e.g. 3DES, SHA1) supply traffic confidentiality and integrity. In DARPA work, existing VPN key accord primitives are augmented or completely replaced by keys provided by quantum cryptography.

1. MagiQ Technologies

One of companies developing solutions established on quantum cryptography is MagiQ Technologies, The technology start- up with headquarters in New York City. Target customers of MagiQ's solutions include the commercial services industry along with both a educational and government labs.

IV. CONCLUSION

Established on quantum mechanics and classical cryptography, quantum cryptography is a novel one in the field of cryptography. Related with classical cryptography, its ultimate advantages are the unconditional security and the sniffing detection. These characteristics can clarify cyber space security critical problem for the future Internet. Our experimental analysis results show the unconditional security and sniffing exposure of quantum cryptography, which makes it suitable for future Internet.

REFERENCES

[1]. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of Things (IOT): A vision architectural elements and future directions", Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645-1660, Sep. 2013.
[2]. Heinzelman WR, Kulik J & Balakrishnan H, "Adaptive protocols for information dissemination in wireless sensor networks" Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, (1999), pp.174-185.
[3]. Sharma H & Sharma S, "A Review of Sensor Networks: Technologies and Applications", Recent Advances in Engineering and Computational Sciences (RAECS), (2014) pp.1–4.
[4]. Hsia,S,C.; Hsu,S,W.; Chang,Y,J., "Remote monitoring and smart sensing for water meter system and leakage detection", IET Wireless Sensor Syst., *vol. 2, no. 4, pp. 402-408, Dec. 2012.*
[5]. Chi,Q.; Yan,H.; Zhang,C.; Pang,Z.; Xu,L,D., "A Reconfigurable Smart Sensor Interface for Industrial WSN in IOT Environment", in IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1417-1425, May 2014.
[6]. Buratti, C.; Conti, A.; Dardari, D.; and Verdone, R., Verdone, R., "An Overview onWireless Sensor Networks Technology and Evolution", *Sensors* 2009, vol.*9,* pp.6869-6896
[7]. J. A. Stankovic, "Research directions for the Internet of Things," IEEE Internet Things *J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.
[8]. R.Karthik Kumar, M.Chandra Mohan, S.Vengateshapandiyan M.Mathan Kumar, R.Eswaran, " Solar based advanced water quality monitoring system using wireless sensor network " - International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue3, March 2014 ISSN: 2278 – 7798.
[9]. Marco Zennaro, Athanasios FloroSs, Gokhan Doga et al, proposed the design of a water "quality monitoring system and, building upon the Sunspot technology".-JOURNAL OF ENGINEERING RESEARCH , VOL 5 NO.6, MAY 2015.
[10]. Kirankumar G.Sutar , Prof.Ramesh T.Patil ," Wireless Sensor Network System to Monitor The Fish Farm" - Int. Journal of Engineering Research and Applications Vol. 3, Issue 5, Sep-Oct 2013, pp.194-197.
[11]. Himadri Nath Saha, Supratim Auddy, Avimita et al., "Pollution Control using Internet of Things (IOT)" Dept Of Computer Science & Engineering Dept.Of Information Technology Institute of Engineering & Management Maulana Abul Kalam Azad University of Technology, Kolkata.
[12]. Cesar Encinasn, Erica Ruizy et al.,"IOT system for the monitoring of water quality in aquaculture". Cesar Encinas_, Erica Ruizy, Joaquin Cortezz and Adolfo Espinozax Dept. Electrical and Electronic Engineering, Institute Technologic de Sonora Cd. Obregon, Sonora, Mexico.
[13]. S. Zhuiykov, "Solid-state sensors monitoring parameters of water quality for the next generation of wireless sensor networks" Sens. Actuators B, Chem., vol. 161, no. 1, pp. 1–20, 2012.
[14]. A. Aisopou, I. Stoianov, and N. Graham, "In-pipe water quality monitoring in water supply systems under steady and unsteady state flow conditions: A quantitative assessment," Water Res., vol. 46, no. 1, pp. 235–246.
[15]. Napoleon D. and Praneesh M. "Detection of Brain Tumor using Kernel Induced Possiblistic C-Means Clustering", volume no.3, issue no.9, pp 436-438, 2013