A Review on Quantum Cryptography

[1]Darshan. P B, [2]Apoorva. R, [3]Aparnashree, [4]Chandana

Students
Alva's Institute of Engineering and Technology, Mijar

***Abstract*: The preferment from conventional computing to quantum computing has created new challenges in the field of cryptography. The cryptographic algorithms which ensured intractability in conventional computing surfaces serious challenge in quantum computing. By applying the quantum mechanics quantum cryptography can be used to unrestrictedly for reliable data communications. Advances in quantum computing, can easily break this security by reverse computing keys faster than the conventional computers. This paper is an attempt to review fundamentals of quantum cryptography.**

Index Terms: Quantum cryptography, cryptography, computing.

Introduction

Cryptography is the study of methods of sending messages in secretes form so that only the intended recipient is able to read the message after applying a specific key. The process of converting the message into some disguised form is called Encryption. The plain text is converted into cipher text by using some key called as Encryption key. At the receiver's end, the recovering of plaintext from ciphertext is required. The process of converting the message into its original form is called Decryption. Keys play important role in cryptography.
The classification of the cryptographic algorithms is basically on the type of key used.

A. Symmetric (secrete key)

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

B. Asymmetric (public key)

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key.

Assume that Alice and Bob are communicating through an insecure communication channel with best of the conventional cryptography algorithm for encryption and decryption which is almost intractable for any conventional computing system. Now, suppose, there is Eve who is an intruder is constantly listening to the communication channel through which Alice and Bob send and receive message and has powerful quantum computing resources. Suppose Alice and Bob are using factoring based algorithm then even can make use of quantum algorithm for factoring. The other applications are quantum key distribution. Quantum digital signatures are another application. These and many more signify the need of quantum cryptography.

II. Quantum Key Distribution

Quantum key distribution (QKD) is a revolutionary security technology that exploits the laws of quantum mechanics to achieve information-theoretic secure key exchange. QKD enables two parties to "grow" a shared secret key without placing any limits on an adversary's computational power and is unique in its ability to detect the presence of any third-party eavesdropping on the key exchange. Due to the fundamental laws of quantum mechanics, any third-party eavesdropping on the key exchange will introduce detectable errors. If the errors are below a defined threshold, an unconditionally secure key can be distilled. When QKD is used in conjunction with the one-time pad symmetric cryptographic algorithm, the result is an unconditionally secure cryptographic system.
The beginning of quantum key distribution (QKD) can be traced back to Stephen Wiesner, who developed the idea of quantum conjugate coding in the late 1960s (Wiesner, 1983). Wiesner's quantum multiplexing utilizes photons polarized in conjugate bases as quantum bits (qubits) in order to pass information. In 1984, Charles Bennett and Gilles Brassard exploited this concept when they proposed the first QKD protocol, BB84, for secure communication (Bennett and Brassard, 1984).

III. .QKD Attributes

QKD offers an agreement based on a shared random sequence of bits in between two distinct devices/users, with a very less probability of other devices (eavesdroppers) being able to make successful inferences. In practice, such sequences are used as secret keys for encoding and decoding messages between the two devices/users. In this view, QKD is quite clearly a key distribution technique, and one can rate QKD's strengths against a number of important goals for key distribution, as summarized below.

a. Confidentiality of Key

Confidentiality is the main attribute in QKD. Public key systems have an uncertainty that decryption is mathematically intractable. Hence key agreement primitives are widely used in today's Internet security architecture, which may perhaps be broken at some point in the future. This could not only hinder future ability to communicate but could reveal past traffic. Classic secret key systems suffered from various problems, namely, insider threats, logistical burden of distributing keying material. Assuming that QKD techniques are properly embedded into an overall secure system, they can provide automatic distribution of keys that may offer security superior to that of its competitors

b. Authentication
It is crucial for security to authenticate some (or all) of the classical messages communicated during the public discussion. We will explain why this is the case, how authentication is achieved and what type of authentication must be used in the following sections.

c. Rapid Key Delivery
Key distribution system should deliver keys fast so that encryption devices do not exhaust their supply of key bits. This is a race between the rate at which key material is put into place and the rate at which it is consumed for encryption or decryption activities.

d. Robustness
It is extremely important that the flow of keying material not be disrupted, whether by accident or by the deliberate acts of an adversary. Here QKD has provided a highly fragile service to date since QKD techniques have implicitly been employed along a single point-to-point link. If that link were disrupted, whether by active eavesdropping or indeed by fiber cut, all flow of keying material would cease.

e. Distances and Location Independence
This feature is notably lacking in QKD, which requires the two entities to have a direct and unencumbered path for photons between them, and which can only operate for a few tens of kilometers through fiber.

f. Resistance to Traffic Analysis
Adversaries may be able to perform useful traffic analysis on a key distribution system eg., a heavy flow of keying material between two points might reveal that a large volume of confidential information flows, or will flow, between them.

IV. QKD limitations

If it sounds too good to be true, then it probably is. The ideal BB84 protocol assumptions include (1) Alice emits perfect single photons, (2) the channel between Alice and Bob is noisy but lossless, (3) Bob has single photon detectors with perfect efficiency, and (4) the basis alignment between Alice and Bob is perfect. If these conditions are met, QKD provides for an unconditionally secure key exchange, as shown in several mathematical proofs (Mayers, 2001; Renner, Gisin, & Kraus, 2005; Shor & Preskill, 2000). However, many of these assumptions are not valid when building real-world systems. For example, the protocol relies on the transmission of single photons because if there are multiple photons sent an adversary may be able to intercept and measure a photon while letting the remaining photons pass unaffected. Reliable on-demand photon generation is not currently practical, so instead a weak coherent photon pulse is generated and attenuated so that on average there are only 0.1 photons in each packet (that means only 1 in 10 packets will contain a photon). This significantly reduces the efficiency of the protocol, but is required to limit and bound the knowledge gained by an eavesdropper. At the receiving side, single photons must be reliably detected. Unfortunately, single photon detectors are rate limited, have low detection efficiencies, and spuriously trigger. Even when there is no eavesdropper present, the physical characteristics of the quantum channel can introduce errors which affect the polarization of the photons while in transit. The result of these technical limitations is that the final key rate is reduced and errors are introduced into the sifted key even though there is no malicious eavesdropper present. These errors must be corrected before using a cryptographic algorithm since Alice and Bob must have identical copies of the key.

V. Conclusion

QKD provides significant advantages when compared to conventional key distribution. First, the security of QKD security rests on the foundations of quantum mechanics. This is in stark contrast to traditional key distribution protocols which rely on computational security, where the computational difficulty of certain mathematical functions is the foundation of security. Second, when using QKD, one can determine if an adversary is eavesdropping on the link because it will induce errors in the key exchange process. In contrast, traditional key exchange algorithms cannot provide any indication of eavesdropping or guarantee of key security.

References

[1] C. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.

[2] .A. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” Phys. Rev. Lett. 67, 661 (5 August 1991).

[3] Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation –Oxford University. Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).

[4] Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002.

[5] Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

[6] Petschinka, Julia. "European Scientists against Eavesdropping and Espionage." 1 April 2004. 7. Salkever, Alex. "A Quantum Leap in Cryptography." BusinessWeek Online. 15 July 2003.

[7] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004..
[8] MagiQ Technologies Press Release. 23 November 2003.

[9] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004.

[10] C. Elliott, "Building the quantum network," New J. Phys. 4 (July 2002) 46.

[11] Pearson, David. "High!speed QKD Reconciliation using Forward Error Correction." Quantum Communication, Measurement and Computing. Vol. 734. No. 1. AIP Publishing, 2004.

[12] Curcic, Tatjana, et al. "Quantum networks: from quantum cryptography to quantum architecture." ACM SIGCOMM Computer Communication Review 34.5 (2004): 3-8.

[13] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical Review Letters 85.2 (2000): 441.

[14] Bienfang, J., et al. "Quantum key distribution with 1.25 Gbps clock synchronization." Optics Express 12.9 (2004): 2011-2016.

[15] Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. "Differential phase-shift quantum key distribution." Photonics Asia 2002. International Society for Optics and Photonics, 2002.

[16] Barnum, Howard, et al. "Authentication of quantum messages." Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on. IEEE, 2002.

[17] Elliott, Chip, David Pearson, and Gregory Troxel. "Quantum cryptography in practice." Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. ACM, 2003.
[18] Buttler, W. T., et al. "Fast, efficient error reconciliation for quantum cryptography." Physical Review A 67.5 (2003): 052303.

[19] Poppe, A., et al. "Practical quantum key distribution with polarization entangled photons." Optics Express 12.16 (2004): 3865-3871.

[20] Lütkenhaus, Norbert. "Estimates for practical quantum cryptography." Physical Review A 59.5 (1999): 3301.