QUANTUM CRYPTOGRAPHY: A NEW GENERATION OF INFORMATION SECURITY SYSTEM

Ritesh Kumar Jain  
Sr. Lecturer, S. S. College of Engineering, Udaipur  
India

Kamal Hiran  
Sr. Lecturer, Amity University, Jaipur  
India

Gaurav Paliwal  
Lecturer, Geetanjali Institute of Technical Studies, Udaipur  
India

ABSTRACT

Quantum Cryptography is an approach to securing communications by applying the phenomena of quantum physics. Unlike traditional classical cryptography, which uses mathematical techniques to restrict eavesdroppers, quantum cryptography is focused on the physics of information. The security of these transmissions is based on the inviolability of the laws of quantum mechanics. The quantum cryptography relies on two important elements of quantum mechanics—the Heisenberg Uncertainty principle and the principle of photon polarization. This paper summarizes the current state of quantum cryptography and the real-world application implementation of this technology.

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

INTRODUCTION

The development of quantum cryptography was motivated by the short-comings of classical cryptographic methods, which can be classified as either “public-key” or “secret-key” methods. The physics of quantum cryptography opens a door to tremendously intriguing possibilities for cryptography, the art and science of communicating in the presence of adversaries [1, 2]. Modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one way functions such as that of factoring large integers [8]. For that reason, for past decade efforts have been made to establish new foundation for cryptography science in the computer communications networks. One of these efforts has led to the development of quantum cryptography technology, whose security relies on the laws of quantum mechanics [1, 2, 6, 9].

Quantum cryptography takes advantage of the unique and unusual behavior of microscopic objects to enable users to securely develop secret keys as well as to detect eavesdropping. Although work on quantum cryptography was begun by Stephen J. Wiesner in the late 1960’s, the first protocol for sending a private key using quantum techniques was not published until 1984 by Bennett and Brassard. Quantum key distribution (QKD) [3] is a method in which quantum states are used for encryption. The strength of quantum cryptography (QC) is that the codes that are generated are not even in theory decodable.

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 [4, 5, 6]. The principle of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem which was first presented by Wootters and Zurek in 1982[7]. Throughout the paper, the transmitter is referred as ‘A’, the receiver as ‘B’, and an adversarial eavesdropper as ‘E’.

QUANTUM CRYPTOGRAPHY

It is impossible to establish a secret key with conventional communications, and so key distribution has relied on the establishment of a physically secure channel (“trusted couriers”) or the conditional security of “difficult” mathematical problems in public key cryptography. However, provably secure key distribution becomes possible with quantum communications. In this procedure the key is distributed over the quantum channel and not the encrypted message. That is why we need two channels between A and B. One public channel for transmission of encrypted message or cryptogram and another channel which is called quantum channel, and used for key distribution. Hence, a more accurate name is quantum key distribution (QKD).
In 1984, Bennett and Brassard suggested the first protocol, called “BB84,” for establishing a secret key using quantum transmissions. This is the first known quantum distribution scheme. This protocol uses the rectilinear and diagonal polarization bases for photons.

Polarization angles are used to encode bits to be transmitted. A basis is chosen to distinguish the two values 0 and 1 without ambiguity. One choice is the rectilinear basis where photons are polarized at angle 0° or 90° representing 0 and 1 respectively. Another choice is the diagonal basis where 0 is represented by photons polarized at 45° and 1 by photons polarized at 135°. For simplicity, denote the 0°, 90°, 45° and 135° as H, V, D and A respectively. The polarization basis H, V is denoted by + and D, A by x[16].

The steps of the protocol are explained below, using that A is the sender, B is the receiver, and E is the eavesdropper.

1. A prepares photons randomly with either rectilinear or diagonal polarizations.
2. A records the polarization of each photon and then sends it to B.
3. B receives each photon and randomly measures its polarization according to the rectilinear or diagonal basis. He records the measurement type (basis used) and the resulting polarization measured. (It is important to remember that the polarization sent by A may not be the same polarization B finds if he does not use the same basis as A.
4. B publicly tells A what the measurement types were, but not the results of his measurements.
5. A publicly tells B which measurements were of the correct type. A correct measurement is the correct type of B used the same basis for measurement as A did for preparation.
6. A and B each throw out the data from measurements that were not of the correct type, and convert the remaining data to a string of bits using a convention such as:

   \[ D = 0, \ A = 1 \]
   \[ H = 0, \ V = 1 \]

If A sends random sequence of photons:

++x+++x+xx

Polarizations of photons sent by A

VHDHADAVHHDAD

Measurement types made by B

++++xxx+xx+

Results of B’s measurements

VHHHADHDAH

B publicly tells A which type of measurement he made on each photon
A publicly tells B which measurements were the correct type

yes yes yes yes yes no yes yes no yes no

A and B each keep the data from correct measurements and convert to binary:

10 0101 0 1

The string of bits now owned by A and B is: 10010101. This string of bits forms the secret key or private key. Thus, what is dubbed “quantum cryptography” (QC) is a process that consists of two major parts, the quantum key distribution (QKD, and the message encryption/decryption process. Assuming that for a long sequence, logic “1” and “0” bits have equal probability of occurrence, statistically half of B’s states will be correct. Because a key operates on a message bit-by-bit (using a modulo-2 operation), A’s initial sequence to B must be twice as long.

The key point in both processes is the polarization state of photons and the variable polarization filter. In addition, because the polarization of single photons is not readable without altering it and because it is not reproducible, the eavesdropper cannot read the polarization of single photons, reproduce it and send it to B. This is the key point in quantum cryptography.

IMPLEMENTING QUANTUM CRYPTOGRAPHY

BBN, Harvard, and Boston University built the DARPA quantum network, the world’s first network that delivers end-to-end network security via high-speed quantum key distribution, and tested that network against sophisticated eavesdropping attacks [10,11,12]. This network is suitable for deployment in metro-size areas via standard telecom (dark) fiber.

This network allows users at BBN Technologies, Harvard University, and Boston University to tap into a fiber-optic loop secured by a quantum cryptography system [12]. The DARPA security model is the cryptographic virtual private network (VPN). To achieve confidentiality, and authentication/integrity, the conventional VPNs use public-key and symmetric cryptography. Public key mechanism support key exchange or agreement, and authenticate to endpoints. Symmetric mechanism (e.g. 3DES, AES) provides traffic confidentiality and integrity [15]. In DARPA quantum cryptography network, existing VPN key agreement primitives are augmented or completely replaced by keys provided by quantum cryptography (Fig. 2).

TECHNICAL CHALLENGES AND FUTURE DIRECTION

One of the challenges for the researchers is distance limitation. Currently, quantum key distribution distances are limited to tens of kilometers because of optical amplification destroys the qubit state, and also to develop optical device capable of generating, detecting and guiding single photons; devices that are affordable within a commercial environment [13].

Another issue is the lack of a security certification process or standard for the equipment [14]. Also users need reassurance not only that QKD is theoretically sound, but also that it has been securely implemented by the vendors. Overall, the theoretical and experimental results will present a main impact, in near future, on the process of commercialization of the QKD systems.

CONCLUSION

We presented a critical view of the workings of quantum cryptography and quantum key distribution. This technology is based on the polarization of photons, which is not a well controlled quantity over long distances and in multi-channel networks.
Quantum cryptography could be the first application of quantum mechanics at the single quanta level. Experiments have demonstrated that keys can be exchanged over distances of a few tens of kilometers at rates at least of the order of a thousand bits per second. There is no doubt that the technology can be mastered and the question is not whether quantum cryptography will and commercial applications, but when. Present quantum cryptography is still very limited in distance. These days public key systems occupy the market and every so often, classical cipher systems are broken. This would be impossible with properly implemented quantum cryptography.

REFERENCES