International Journal on Emerging Technologies **2**(1): 11-13(2011) **ISSN : 0975-8364**

Study of Various Quantum State Attacks in Quantum

T.K. Bandopadhyay*, Bharat Mishra** and Swapnil Jain***

**Deptt. of Electronics and Communications, BIST, Bhopal, (MP)*
***Deptt. of Electronics and Communications, MGCGC, Chitrakoot*
****Deptt. of Electronics and Communications, SISTec, Bhopal, (MP)*

(Received 12 March, 2011, Accepted, 12 April, 2011)

ABSTRACT : Quantum Key Distribution (QKD) is an automated method for distributing secret keys across an optical fiber. A unique feature of QKD is that its security is derived from the fundamental laws of Quantum Physics and does not therefore rely upon assumptions about the computing power of an eavesdropper. An added benefit is that the keys distributed by QKD will be highly secure. For any cryptographic system, be it of quantum or classical nature, it is important to carefully analyze the actual implementation for weak points that may compromise its principle security. Applied to QKD, these include deficiencies in the preparation of quantum data at Sender's that can be exploited by an eavesdropper to gain information about the sifted key. These kinds of attacks are known as quantum state attack. Once the deficiencies are found, it may be possible to eliminate them by devising a better optical setup, or to remove the corresponding amount of information that eavesdropper may have obtained through additional privacy amplification. Yet, we point out that loopholes may also arise from a careless implementation of privacy amplification, e.g. improper choice of Hash function, or of insufficient authentication of the classical channel. Finally, the size of the error corrected key has to be considered when calculating the appropriate amount of privacy amplification, i.e. to distil a secure key.

Keywords : Quantum key distribution, Polarization, Quantum State attack, Intensity Modulator, Beam Splitter

I. INTRODUCTION

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.

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.

II. OUR QKD SYSTEM

QKD is based upon sending encoding single photons (particles of light) along the optical fiber. The laws of Quantum Physics dictate that any attempt by an eavesdropper to intercept and measure the photons alters their encoding. This means that eavesdropping on quantum keys can be detected.

QKD system is based on polarization qu-bits and employs the BB84 protocol [1], supplemented with two decoy states [2]–[3]. It allows alternating sequences of strong and faint laser pulses, encoding classical data and quantum data, respectively. A simplified schematic of the QKD system is depicted in figure 1. Alice uses two laser diodes to generate the classical data (LD2) and the quantum data (LD1). The pulses emitted from LD1 are first attenuated by an optical attenuator (ATT), and then sent through an intensity modulator (IM) to create signal and decoy states with different mean photon numbers. To create vacuum decoy states, no electrical pulses are sent to LD1. The horizontally polarized faint pulses are then transmitted through a polarization beam splitter (PBS), and combined with the strong, vertically polarized pulses from LD2. All pulses are then sent to a polarization modulator (PM), where horizontal (H), vertical (V), right (R), or left (L) circular polarization states can be created.

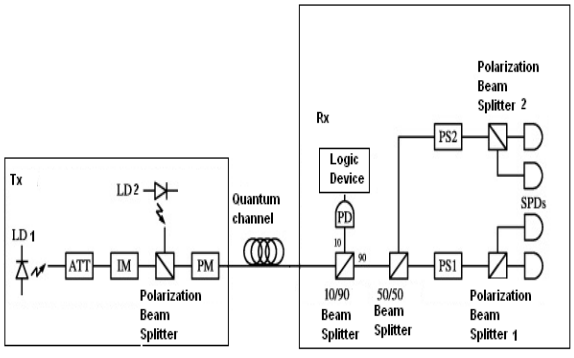

Fig. 1. Schematic of Quantum Key Distribution.

Quantum and classical data are transmitted to the receiver through a quantum channel. At Receiver's end, 10% of the light is directed towards a fast photo detector (PD) followed by a logic device. The detector and the logic device will read the information encoded in the classical data and take appropriate action, e.g. for clock synchronization, optical routing, or communication of protocol specific information used by receiver for the measurement and subsequent processing of the quantum data.

The remaining light is split at a 50/50 beam splitter (BS), and directed to two polarization stabilizers (PSs) (PS1 and PS2) followed by Polarization Beam Splitters (PBS1 and PBS2) and single photon detectors (SPDs). PS1 ensures that horizontally polarized classical data, and hence qubits, emitted at sender's arrive unchanged at PBS1. Similarly, PS2 is set up such that right circular polarized classical data and qubits emitted at sender's always impinge horizontally polarized on PBS2. Since the transformation in the quantum channel is described by a unitary matrix (i.e. orthogonal states remain orthogonal), our stabilization scheme ensures that qubits prepared in H and V, or R and L states arrive horizontally and vertically polarized on PBS1 or PBS2, respectively. Hence, the two sets of PS, PBS and two SPDs both allow compensation of unwanted polarization transformations in the quantum channel, and projection measurements onto H, V, R and L, as required in the BB84 protocol.

III. SECURITY ISSUES

For any cryptographic system, be it of quantum or classical nature, the principle issue is its security. In QKD, these include deficiencies in the preparation of quantum data at sender's that can be exploited by an eavesdropper to gain information about the sifted key. These kinds of attacks are known as *quantum state attacks.* Furthermore, eavesdropper may also attempt to actively sense the classical devices that create or measure the quantum data, or try to actively impact on the interaction between quantum and classical systems to influence the outcomes of measurements. These kinds of attacks are called as *classical system attacks.*

Once the deficiencies are found, it may be possible to eliminate them by devising a better optical setup, or to remove the corresponding amount of information that Eve may have obtained through additional privacy amplification [4]. Yet, we point out that loopholes may also arise from a careless implementation of privacy amplification, e.g. improper choice of Hash function, or of insufficient authentication of the classical channel. Finally, the size of the error corrected key has to be considered when calculating the appropriate amount of privacy amplification, *i.e.* to distil a secure key [5, 6].

A. Quantum state attacks

The use of attenuated laser pulses, as opposed to pairs of entangled photons [7], entails the possibility that non-orthogonal qubit states (here encoded into the polarization degrees of freedom) may become distinguishable when taking into account other degrees of freedom needed to fully describe the quantum data, e.g. frequency, temporal modes, or transverse modes. Obviously, in this case, the security offered by QKD would break down. These attacks are called as *quantum side channel attacks.* Furthermore, as the number of photons in the attenuated laser pulses is described by a Poisson's distribution, it may be possible for an eavesdropper to gain information based on *photon-number-splitting (PNS) attacks.*

Attacks exploiting quantum side channels. In our QKD system, all four qubit states are produced by the same laser diode, which is triggered independently of the subsequent action of the polarization modulator or IM. Together with the polarization independent spectral transmission of both modulators and the attenuator, due to the use of the FMs, this ensures that correlation between polarization state and spectrum or temporal modes do not exist. However, we recall that the circulator (CIR) at the output of the polarization modulator adds basis-dependent PMD, which manifests as a basis-dependent QBER. This may induce detectable temporal broadening of the photonic wave packets, *i.e.* may partially reveal the basis used for encoding the qubit. The circulator will be replaced in a future, improved setup.

Furthermore, as the entire setup is built with (transverse) single mode optical fibers, correlation between polarization states and transverse modes, which may be present in a free space system, are ruled out.

PNS attacks and decoy states. The use of faint laser pulses makes our system principally susceptible to PNS attacks, [8]A possibility to remove the threat of the PNS attack is the use of so-called decoy states [2]–[3]. This allows establishing a conservative lower bound for the key that can be created from single photons emitted at sender's, *i.e.* key that was not subject to the PNS attack. As described before, our setup has been devised to allow for the implementation of decoy states. In the following, we will examine experimentally the accuracy with which the decoy state method allows bounding the size of the secret key.

B. Classical system attacks

Trojan Horse attacks. As in any QKD system, regardless of whether it employs one-way or two-way quantum communication, appropriate measures have to be implemented to protect against Trojan Horse attacks [9]. In these attacks, the eavesdropper injects light through the optical fiber into sender's or receiver's preparation or measurement device, respectively, and analyses the back reflection, which may reveal information about the quantum state created at sender's or the measurement basis to be used at receiver's. In both cases, the security of the key distribution would be compromised as eavesdropper either knows the state, or knows in which basis to perform an intercept resend attack without creating errors. In our QKD system, given the static setup at receiver's, Trojan Horse attacks have to be considered only at sender's. Towards this end, a polarization independent optical isolator and a spectral filter that absorbs all wavelengths not blocked by the isolator should be placed at the output of sender's.

Time-shift attacks. In a time-shift attack [10]–[11] the eavesdropper exploits the fact that the detection efficiency of different detectors may, for a given arrival time of a photon, be different. It may thus be possible for an eavesdropper to bias the detection probabilities by actively time-shifting the arrival time of photons and thereby acquire information for each photon if it was detected in a detector that codes for a bit value 0, or 1. This attack, which is possible in our current system, can be overcome if receiver randomly rotates the polarization state of each incoming qubit by 0 or $\pi/2$, thereby de-correlating detection in a particular detector with a particular bit value. This can be done by placing a rapidly variable $\lambda/2$ wave plate in between the PS and the PBSs, at the expense of rendering Bob's setup 'active', *i.e.* vulnerable to Trojan Horse attacks.

IV. CONCLUSION

In QKD system the primary concern is the security of the key during the transmission, the security may be affected due to various attacks such as quantum state attack and classical system attack. Once the deficiencies are found it can be eliminated by an improved optical setup or by removing the corresponding amount of information

which any eavesdropper may have collected through privacy amplification. In this paper we have studied various attacks and their Protective measures.

REFERENCES

[1] Bennett, C.H. and Brassard G. *Proc. IEEE Int. Conf. on Computers, Systems and Signal Process (Bangalore, India)* pp 175–9., (1984).

[2] Hwang W.Y. *Phys. Rev. Lett.* **91,** 057901, (2003).

[3] Wang, X.B., *Phys. Rev. Lett.* **94,** 230503, (2005).

[4] Bennett, C.H., Brassard, G, Crepeau, C. and Maurer U., *IEEE Trans. Inf. Theory* **41,** 1915–23, (1995).

[5] Scarani, V. and Renner, R. *Phys. Rev. Lett.* **100,** 200501, (2008).

[6] Hayashi, M. *Phys. Rev.* A **76,** 012329, (2007).

[7] Gisin, N., Ribordy, G, Tittel, W. and Zbinden H. *Rev. Mod. Phys.* **74,** 145–95, (2002).

[8] Gisin, N., Huttner, B., Imoto, N. and Mor, T., *Phys. Rev.* A **51,** 1863–9, (1995).

[9] Gisin, N., Fasel, S., Kraus, B., Zbinden, H. and Ribordy G., *Phys. ev.* A **73,** 022320, (2006).

[10] Makarov, V., Anisimov, A. and Skaar, J. *Phys. Rev.* A **74,** 022313, (2006).

[11] Zhao Y, Fung C H F, Bing Q, Chen C and Lo H K., *Phys. Rev.* A **78,** 042333, (2008).

[12] Dusek M, Haderka O and Hendrych, M., *Opt. Commun.* **1**, (1999).