Chapter 7

Practical Quantum Key Distribution

Sellami Ali
International Islamic University Malaysia (IIUM), Malaysia

ABSTRACT

We have presented a method to estimate parameters of the decoy state protocol based on one decoy state protocol for both BB84 and SARG04. This method can give different lower bound of the fraction of single-photon counts ($y_1$), the fraction of two-photon counts ($y_2$), the upper bound QBER of single-photon pulses ($e_1$), the upper bound QBER of two-photon pulses ($e_2$), and the lower bound of key generation rate for both BB84 and SARG04. The effects of statistical fluctuations on some parameters of our QKD system have been presented. We have also performed the optimization on the choice of intensities and percentages of signal state and decoy states which give out the maximum distance and the optimization of the key generation rate. The numerical simulation has shown that the fiber based QKD and free space QKD systems using the proposed method for BB84 are able to achieve both a higher secret key rate and greater secure distance than that of SARG04. Also, it is shown that bidirectional ground to satellite and inter-satellite communications are possible with our protocol. The experiment of decoy state QKD has been demonstrated using ID-3000 commercial QKD system based on a standard ‘Plug & Play’ set-up. One decoy state QKD has been implemented for both BB84 and SARG04 over different transmission distance of standard telecom fiber.

DOI: 10.4018/978-1-60960-851-4.ch007
INTRODUCTION

The need for highly secure communication systems is quite evident in the world today. Large amounts of information are transferred continuously, whether it be important banking information or a simple phone call. With this growing information exchange, the possibilities for unauthorized reception are also increased. In the classical cryptography a variety of encryption algorithms have been introduced, providing different levels of security. Apart from one, they all have in common that in principle they can be cracked. For example, the RSA cryptosystem, one of the widely used algorithms (e.g. in SSL, SSH), relies on the fact that it is difficult to find the factors of large integers. There are two threats to this method: The first is that more computational power will help to make time-consuming attacks (like brute-force attacks) more convenient. Moreover, someone might even think of an efficient algorithm for factoring integers. The second problem is that quantum computers are in fact already capable of executing the factorization efficiently. Until now, it cannot be done with large integers and it will probably take some time for it to become practical, but for crucial applications “probably secure” is not enough.

On the other hand, there exists a classical, unconditionally secure cryptographic algorithm, but it has a big problem: It requires a random key, which has to be as long as the message itself and this has to be transported securely from one party to the other. This cannot be done classically.

Here, an amazing idea comes into play: Quantum mechanics has the property of hiding some information from us, as expressed in Heisenberg’s uncertainty relation. Could this inherent ignorance be used as an advantage over a potential eavesdropper? It turns out, that this is indeed possible and after discussing the essential quantum mechanical properties, it will be introduced a method of establishing a secret key between two parties, which is provably secure. This security is a direct consequence of the fundamental axioms of quantum mechanics. As long as we do not find that we can gain more information on quantum states than described by quantum mechanics, this scheme has to be regarded secure.

Really interesting about this method is that a usually unfavorable property of quantum mechanics is actually employed to achieve something that can’t be done outside the quantum world. The fact that two non-commuting observables can only be measured with limited precision allows unconditionally secure key distribution. The whole idea has been named quantum cryptography or quantum key distribution (QKD).

The central objective of this chapter is to study and implement practical systems for quantum cryptography using decoy state protocol. In particular we seek to improve dramatically both the security and the performance of practical QKD system (in terms of substantially higher key generation rate and longer distance). The main objectives of this research are:

1. Presenting a method to estimate parameters of decoy state method based on one decoy state protocol for both BB84 and SARG04.
2. Simulation of fiber-based and free space Decoy State Quantum Key Distribution based on practical decoy state protocols which are mentioned in the first objective for both BB84 and SARG04.
3. Experimental realization of one decoy state protocols which is mentioned in the first objective: one decoy state protocol.

BACKGROUND

Quantum cryptography is based on physical principles which cannot be defeated. This need for secure communications provided the driving force for interest in quantum cryptography, or quantum key distribution in particular. In 1983 Wiesner put forth as idea for counterfeit-proof money by employing
Related Content

Intrusion Detection Algorithm for MANET
www.igi-global.com/article/intrusion-detection-algorithm-manet/58981?camid=4v1a

Future Trends in Digital Security
www.igi-global.com/chapter/future-trends-digital-security/43817?camid=4v1a

Data Security for Cloud Datasets With Bloom Filters on Ciphertext Policy Attribute Based Encryption
www.igi-global.com/article/data-security-for-cloud-datasets-with-bloom-filters-on-ciphertext-policy-attribute-based-encryption/237208?camid=4v1a

SEACON: An Integrated Approach to the Analysis and Design of Secure Enterprise Architecture-Based Computer Networks
www.igi-global.com/article/seacon-integrated-approach-analysis-design/2473?camid=4v1a