Abstract

In this report we discuss the subject of Cryptography. Cryptography is a physical or mathematical system of transforming information so that it is undecipherable by polynomial time computational adversaries. In classical cryptography we look at purely mathematical transformations. We discuss the one time pad and the RSA protocol. The former being provably secure while the latter is only conjectured to be secure and moreover the security is algorithmic in nature. The one time pad has limited usage since it requires private exchange of keys. Secure cryptography is possible if we are able to do secure key distribution. Therefore, in Quantum Cryptography we look at the problem of secure key distribution. Once a secure key distribution is established we can use the one time pad to securely transmit data. Since fundamentally secure key distribution is possible quantum cryptography offers provably secure communication. We discuss various quantum key distribution protocols[BB84, BBM92, Eke91] that work under noiseless conditions. Since real quantum channels are always noisy we have to consider the noise effect of noise on quantum states passing through noisy channels. In order to protect against errors we do quantum error correction. We present the CSS[CS96, Ste96] protocol for quantum error correction and derive certain general results for the fidelity of the communication protocols. We show that the BB-84 protocol is robust against noise by following the discussion in [SP00]. We then tackle the problem of Quantum Private Communication(QPC) under noise. In QPC the idea is to protect private information during its public comparison. We discuss quantum protocols that work under noiseless conditions [TLH12, WYBW12]. We analyze [TLH12] under bit-phase flip channel and depolarizing channel. We show how noise gives a bound on the length of the string that can be compared using the protocol given in [TLH12]. We then present another protocol based on CSS codes to perform Quantum Private communication under noisy channels. Here we can compare strings of arbitrary length as long as the error rate is under a given level.