QUANTUM CRYPTOGRAPHY

Swagat Pretam Mohapatra
MA12C048
2014

In this project we discuss about quantum cryptography. When information is transmitted in microscopic systems, such as single photons or atoms, it's information carriers obey quantum physics rather than classical physics. This offers many new possibilities for information processing, since it is possible to invent novel information processes prevented by classical physics. This is called quantum cryptography. Unlike cryptographic techniques where the security is based upon unproven mathematical assumptions, the security of quantum cryptography relies on the laws of physics. For instance, two parties involved in communication can detect the presence of an eavesdropper due to laws of quantum physics.

We referred to the popular paper by Artur K. Ekert titled "*Quantum cryptography based on bell's theorem*" of physical review

letters, vol. 67, 5 august 1991. We tried to reduce the number of analysers with each party from three to two with one analyser common to both the party but found that in this case the necessary lower bound is not satisfied. We present this project as a survey project discussing some of the prominent quantum key distribution protocols.