International Journal of Electronics,
Communication & Instrumentation Engineering
Research and Development (IJECIERD)
ISSN(P): 2249-684X; ISSN(E): 2249-7951
Vol. 4, Issue 2, Apr 2014, 1-4

NETWORK SECURITY WITH QUANTUM CRYPTOGRAPHY – A REVIEW

KRANTISH V. POL & D. J. PETHE

Department of Electronics and Telecommunications, Datta Meghe College of Engineering,

Airoli, Navi Mumbai, Maharashtra, India

ABSTRACT

In today's so called modern World, most digital networks rely on classical cryptosystems (CC) to secure the confidentiality and integrity of traffic carried across the network. However, these classical schemes for key distribution rely on the unproven computational assumptions and hence keys can be easily compromised in many ways. Quantum cryptography (QC) is an emerging approach to secure communications by applying the phenomena of quantum physics. Unlike classical or current cryptosystems, which uses mathematical techniques to restrict eavesdroppers, quantum cryptography focuses on the physics of information. The security of these transmissions is guaranteed by the inviolability of the laws of quantum mechanics. The quantum cryptography is based 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 review of quantum key distribution via the BB84 protocol and its use to secure data. Paper also summarizes a review on whether Quantum cryptography is really better and should replace conventional or modern cryptographic techniques.

KEYWORDS: CC V/S QC, Heisenberg Uncertainty Principle, Photon Polarization, QKD Protocol, Quantum Cryptography