Chapter 16
Einstein–Podolsky–Rosen Paradox and Certain Aspects of Quantum Cryptology with Some Applications

Narayanankutty Karuppath
Amrita Vishwa Vidyapeetham, India

P. Achuthan
Amrita Vishwa Vidyapeetham, India

ABSTRACT

The developments in quantum computing or any breakthrough in factorization algorithm would have far-reaching consequences in cryptology. For instance, Shor algorithm of factorizing in quantum computing might render the RSA type classical cryptography almost obsolete since it mainly depends on the computational complexity of factorization. Therefore, quantum cryptography is of immense importance and value in the modern context of recent scientific revolution. In this chapter, the authors discuss in brief certain fascinating aspects of Einstein-Podolsky-Rosen (EPR) paradox in the context of quantum cryptology. The EPR protocol and its connections to the famous Bell's inequality are also considered in here.

INTRODUCTION

The potential power of quantum approach to computing would render the classical cryptology almost superfluous in the not too far away future. The main problem of cryptography is that of key distribution (hereafter KD). KD can be broadly classified into public KD and private KD. In conventional classical cryptography it is the private KD of RSA type algorithms that assumes the computational complexity of factorization. Quantum computing and computational algorithms would make things possible compared to that which cannot be even imagined by conventional means. For instance, Shor quantum algorithm, defined in Shor (1997), would make an unparalleled and unheard of quantum leap as far as factoring is concerned. As an illustration, if one wants to factor a very large integer (say, having 250 digits) what the existing very fast super computers might take is a time of the order of the age of the Universe

DOI: 10.4018/978-1-60960-123-2.ch016

(≈ 13.6 billion years!). But it would only be the matter of a few seconds or at the maximum a few minutes for a quantum computer equipped with quantum polynomial algorithm for factoring like that of Shor, defined in Julian (2001). Similarly the Grover's new efficient quantum search algorithms also would speed up searching phenomenally, Grover (1996), Grover (1997). If N is number of the possible keys then Grover's quantum search algorithm can speed up the time from $O(N)$ to $O(N^{1/2})$ for a thorough exploration of the public keys. That is, searching could be speeded up millions fold for very large value of N. Modern conventional classic cryptography makes use of a trap door algorithm for its public key. The assumption is on the complexity of computation like that it is difficult to factor a very large integer. But any break-through in mathematics or leap in computation would invalidate such an assumption. Even private key or symmetric key distribution can be jeopardized by the eavesdropper. So, any cryptography scheme based on the assumption of complexity of algorithm has a very high chance of being letting down. Private key distribution runs the risk of being intercepted which cannot simply be wished away. More importantly, one is never sure if someone had eavesdropped or not, be it public or private KD scheme of the conventional classic cryptography. Additionally, as said above, quantum crypto analysis poses extremely high degree of potential threat to the present classical encryption systems. The extreme exigency of the matter becomes severely felt when one considers the possibility of quantum retro-crypto analysis (or retroactive decryption) that would spell havoc. The evil Eve might copy the existing public keys and information and create a bank of it, for potential quantum retro analysis of the future. Hence, even the present state-of-the-art cryptology methods are neither fool proof nor future proof. Ironically quantum cryptography provides a solution for the same. This fact has to be taken utmost seriously.

Modern fields like Quantum Cryptology, Quantum Teleportation, Quantum Computing, Quantum Dense Coding and the like exploit the quantum properties of individual systems rather than those of large ensembles. Historically this became possible as follows. The most celebrated Einstein-Bohr debate culminated in the ubiquitous paper by Einstein, Podolsky and Rosen which paved way to deeper understanding of the weird aspects of quantum phenomena, though the new perspectives that resulted from the testing of Bell's inequality were in a contrary manner to the expectations of EPR, Narayanankutty and Achuthan (2005), Achuthan and Narayanankutty (2009). The development of Bell's inequality was described as the most profound discovery of science (not of physics alone!) by Henry Stapp. The non-intuitive feature of quantum mechanics is being exploited in quantum cryptography just as quantum computing. A future resistant way of crypto-scheme is what is aimed at by Quantum cryptology.

The subject of Cryptology, both classical and non-classical (quantum) can be seen firmly founded on many very fundamental mathematical concepts and theories. The following brief listing gives an idea of the coverage of topics as per the latest well-known Mathematical subject classification scheme brought out under Zentralblatt (MATH) edited by European Mathematical Society and Heidelberger Academie der Wissenschaften with B.Wegener, Berlin, Germany, as editor-in-chief. We give here the relevant information:

A few features of relevance to the topic under discussion can be given.

a) Cryptography is the art and science of sending a message unintelligible and indecipherable to any unauthorized party. It is a subset of the wider field of cryptology which includes as well cryptoanalysis, the art of code breaking. In order to succeed in this, an algorithm (also called a cryptosystem or cipher) is utilized for scrambling a message with what is known as the "key". Thus a cryptogram is produced. Such a procedure