INTRODUCTION

Preserving confidentiality during communications is always considered a hard task; encryption is one solution for such a problem. The simplest, yet proved (Shannon, 1949) secure, encryption method is one-time pad (Vernam, 1926); which uses symmetric keys between communicating parties. The main two problems of one-time-pad is i) the need to always generate new keys, and ii) the need to securely distribute such keys between the communicating parties; while the first problem can be solved using any real random number generator, the second is harder to solve and known as Key Distribution problem (KD).

Diffie and Hellman (1976) were the first to solve the (KD) problem, utilizing a mathematical problem known as discrete log (DL) (Menezes, Oorschot, & Vanstone, 1997). Based on DL problem and utilizing another mathematical problem known as factorization problem (FP) Rivest, Shamir, and Adleman (1978) introduced the asymmetric encryption technique RSA using two correlated keys; Multiple methods were introduced to generated such keys see FIM (Abu-Ayyash & Jabbar, 2003).

Another recent solution for key distribution was achieved by utilizing a well-known scientific problem related to quantum physics known as uncertainty (Price, Chissick, & Heisenberg, 1977); were two co-related properties of a quantum particle cannot be measured with high precision at the same time, Wiesner (1983) was the first to suggest using it, followed by Bennett and Brassard (1984); Since then, lots
of quantum key distribution (QKD) protocols were proposed (Nung & Kuo, 2002; Bennett, 1992; Ekert, 1991; Kak, 2006; Kanamori, Yoo, & Al-Shurman, 2005; Bostrom & Felbinger, 2002; Lucamarini & Mancini, 2004; Wang, Koh, & Han, 1997; Barrett, Hardy, & Adrian, 2005).

Some well-known protocols, in addition to implementations, suffers from big losses comparing the size of the final key to the number of quantum states (particles) used. The loss is due to the protocol implementation steps, in addition to the characteristics and implementations of physical devices and channels used (Abu-ayyash & Ajlouni, 2008; Bennett & Brassard, 1992).

Researchers have already tried to solve this problem in a multi-dimensional space: first by enhancing the physical devices, channels, parameters and implementations (Chou, Polyakov, Kuzmich, & Kimble, 2004; Santori et al, 2004; Tisa, Tosi, & Zappa, 2007); second by increasing the information content in the quantum particle states used (Groblacher, Jennewein, Vaziri, Weihs, & Zeilinger, 2005; Kuang & Zhoul, 2004); third by using other quantum phenomena such as EPR (Einstein, Pololsky, & Rosen, 1935; Ekert, 1991; Kuang & Zhoul, 2004); fourth by changing or enhancing the way the protocol works (Abu-ayyash & Ajlouni, 2008; Nung & Kuo, 2002; Kak, 2006; Kanamori, Yoo, & Al-Shurman, 2005; Barrett, Hardy, & Adrian, 2005).

For example Ching and Chen (Nung & Kuo, 2002) enhanced the gain of Bennett protocol B92 (Bennett, 1992) by using another stage back from Bob to Alice; where he sends back a new qubits using the same bases he used initially at the times where he fails to measure a qubit sent by Alice, this increases the key size by around 3.6% on the expense of more qubits. Another example, RUQB, uses a different technique for improving the gain, based on discovering the relationship among the original random bits that were used during the protocol to aid in enhancing the gain (by 5.5% for BB84) (Bennett & Brassard, 1984). In this research it is intended to investigate permuting RUQB sets to increase gain, and study the effect of this permutation on the security of this method.

First, the QKD idea is presented along with RUQB; then we discuss the studied method of P-RUQB, afterwards we discuss gain analysis, followed by a discussion on security aspect of P-RUQB and then we conclude with the results.

QUANTUM KEY DISTRIBUTION AND RUQB

The basic element of quantum key distribution will be illustrated using the original four-state QKD protocol developed by Bennett and Brassard in 1984 known as “BB84” protocol. Assume that the individual photons, precisely the polarization states of photons, serve as the quantum bits for the protocol. The protocol starts by one of the two parties transmitting a sequence of photons to the other party. The parties publicly agree to make use of the two distinct polarization bases which are chosen to be maximally non-orthogonal. In a completely random order, a sequence of photons are prepared in states of definite polarization in one or other of the two chosen bases and transmitted by one of the parties to the other through a channel that preserves the polarization. The photons are measured by the receiver in one or the other of the agreed upon bases, again chosen in a completely random order. The choices of bases made by the transmitter and receiver thus comprise two independent random sequences. Since they are independent random sequences of binary numbers, about half of the basis choices will be the same and are called the “compatible” bases, and the other half will be different and are called the “incompatible” bases. The two parties compare publicly, making use for this purpose of a classical communication channel, the two independent random sets of polarization bases that were used, without revealing the polarization states that were observed.

Cryptographic protocols, in the absence of real random bit generator RBG, uses pseudorandom bit generator (PRBG), for that, it is required that the PRBG used for cryptography
Distributed Computing for Internet of Things (IoT)
Dharmendra Trikamlal Patel (2019). *Computational Intelligence in the Internet of Things* (pp. 84-109).
www.igi-global.com/chapter/distributed-computing-for-internet-of-things-iot/224445?camid=4v1a

Semantic Clustering of Web Documents: An Ontology based Approach Using Swarm Intelligence
www.igi-global.com/article/semantic-clustering-web-documents/75122?camid=4v1a