# Using Permutations to Enhance the Gain of RUQB Technique

*Abdulla M. Abu-ayyash, Central Bank of Jordan, Jordan*

*Naim Ajlouni, Al-Balqa University, Jordan*

## ABSTRACT

*Quantum key distribution (QKD) techniques usually suffer from a gain problem when comparing the final key to the generated pulses of quantum states. This research permutes the sets that RUQB (Abu-ayyash & Ajlouni, 2008) uses in order to increase the gain. The effect of both randomness and permutations are studied; While RUQB technique improves the gain of BB84 QKD by 5.5% it was also shown that the higher the randomness of the initial key the higher the gain that can be achieved, this work concluded that the use of around 7 permutations results in 30% gain recovery in an ideal situations.*

*Keywords:* *Cryptography, Key Distribution, Pseudo-Random Bit Generator (PRBG), Quantum Cryptography, Quantum Key Distribution*

## 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).

DOI: 10.4018/jitwe.2012040103

Diffie and Hellman (1976) were the first to solve the (KD) problem, utilizing a mathematical problem known as *discreet 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 pseudo-random bit generator (PRBG). for that, it is required that the PRBG used for cryptography

passes what is known to be the *next bit test* in which it is unlikely to predict the next bit the PRBG generates given the previous sequence that were generated, at this point the PRBG that passes this test is classified as *"cryptographically secure" pseudo-random bit generator* CSPRBG (Menezes, Oorschot, & Vanstone, 1997); for that, and for maximum security, QKD protocols uses RBG based on physical phenomena like radiation.

RUQB is based on the idea that, in-spite that random bits are generated in random, there are some relationships between the random bits generated, those relationships are approximately different for each bit; RUQB technique seeks to find a relationship, based on dividing the original random sequence of bits into subsets, P-RUQB will further seeks to find other relationships by permuting the subsets.

## PERMUTED RUQB (P-RUQB)

Most QKD algorithms start by using random (not a pseudo-random) numbers generated by any physical phenomena, a lot of such random numbers are used for testing the presence of an eavesdropper which reduces the gain of the protocol. P-RUQB is based on the idea of permuting the subsets that was used by RUQB for discovering the relationship of the random bits, the actual recovery process will concentrate on recovering such random numbers by making use of the agreed bits from the random number list. The following will emphasize P-RUQB:

1. Alice generate a list of $n$ random bits,

$$\mathbb{A} = \{a_0, a_1, \cdots, a_{n-1}\}, n = 2^{l-1}, \text{ where } l \in Z .$$

2. Alice encodes the bits into quantum states to have a list $\mathbb{Q} = \{|\, q_0\rangle, |\, q_1\rangle, \cdots, |\, q_{n-1}\rangle\}$ and sends the quantum states to Bob.

3. Bob measures each quantum state received based on any QKD method to obtain the list $\mathbb{B} = \{b_0, b_1, \cdots, b_{n-1}\}$.

4. Alice and Bob start a sifting process based on the same QKD method result in a list $\mathbb{F}$ (a list of agreed on locations of bits).

5. Alice and Bob directly compare $\frac{|\,\mathbb{F}\,|}{2}$ bits to estimate the number of errors $e_T$ and its percentage given by $\epsilon = \frac{2e_T}{|\,\mathbb{F}\,|}$, if the percentage is more than an agreed on threshold $t$ they abort the protocol and start again, if not, they start an error correction process to eliminate the list $\mathbb{E}$ of bits to obtain the initial key string $\mathbb{K}_I^A = \{a_i \mid \forall a_i \in \mathbb{A}, i \in \mathbb{F} - \mathbb{E}\}$, $\mathbb{K}_I^B = \{b_i \mid \forall b_i \in \mathbb{B}, i \in \mathbb{F} - \mathbb{E}\}$, note that $\mathbb{K}^A{}_I = \mathbb{K}^B{}_I$ and $|\,\mathbb{K}_I^A\,| = |\,\mathbb{K}_I^B\,| < n$.

6. P-RUQB: Alice construct multiple lists $L_p$ and send them to Bob as follows:
   a. Let $l$ denotes the number of bits needed to represent any location of the originally (Alice) generated random bits. i.e., $l = \lfloor log_2 n \rfloor + 1$.
   b. Let $P$ denote the set of permutations that Alice and Bob agreed on, such that $p \in P, 0 \le p \le l!$.
   c. for each permutation number $p$ Alice do the following:
      i. Construct multiple lists of bits of size $l$ from the initial key bits

$$\mathbb{S}_{ip}^A = \{c_j \mid \forall c_j \in \mathbb{K}_I^A, \; i \le j \le i + l - 1\}, 0 \le i \le |\,\mathbb{K}_I^A\,| - l.$$

      ii. Let $\mathbb{P}_{ip}^A$ denote the permutation of the set $\mathbb{S}_{ip}^A$, using permutation number $p$.
      iii. construct a temporary set of results $\mathbb{K}_{Tp}^A = \{(r_i, l_i, i)\}, 0 \le i \le |\,\mathbb{K}_I^A\,| - l$, where $r_i$ is the result of XORing the elements of the set $\mathbb{P}_{ip}^A$, $l_i$ is the binary location calculated from set $\mathbb{P}_{ip}^A$ as shown in Equation (1) and (2) respectively:

$$r_i = \underset{0\le j\le l-1}{\oplus} c_j, c_j \in \mathbb{P}_{ip}^{A} \quad (1)$$

$$l_i = \sum_{0\le j\le l-1} c_j 2^j \mod n, c_j \in \mathbb{P}_{ip}^{A} \quad (2)$$

iv. Construct indexing lists $L_p$ for each permutation $p$,

$$L_p = \{i \mid \forall (r_i, l_i, i) \in \mathbb{K}_{Tp}^{A}, a_{l_i} = r_i, l_i \notin \mathbb{F} \bigcup \mathbb{E}, a_{l_i} \in \mathbb{A}, l_i \notin L_w \forall w \neq p\},$$

note that the location $l_i$ should not be within any previous lists.

d. Alice key is $\mathbb{K}^A = \{k_i\}$, such that for all $L_p$

$$k_i = \begin{cases} a_i & \forall a_i \in A, i \in \mathbb{F} - \mathbb{E}. \\ r_i & \forall (r_i, l_i, i) \in \mathbb{K}_{Tp}^{A}, \forall i \in L_p, \\ & \forall p, 0 \le p \le l! \end{cases} \quad (3)$$

7. Once Bob receives all lists $L_p$ he will calculate the following:
   a. $l = \lfloor log_2 n \rfloor + 1$.
   b. for each permutation number $p$ used, $0 \le p \le l!$ do the following:-
      $\mathbb{S}_{ip}^{B} = \{c_j \mid \forall c_j \in \mathbb{K}_I^B,$
      i. $i \le j \le i + l - 1\}, \forall i \in L_p$.
      ii. $\mathbb{P}_{ip}^{B}$ a permutation of the set $\mathbb{S}_{ip}^{B}$, using permutation number $p$.
      $\mathbb{K}_{Tp}^{B} = \{(r_i, l_i, i)\}, \forall i \in L_p$ where

$$r_i = \underset{0\le j\le l-1}{\oplus} c_j, c_j \in \mathbb{P}_{ip}^{B} \quad (4)$$

$$l_i = \sum_{0\le j\le l-1} c_j 2^j \mod n, c_j \in \mathbb{P}_{ip}^{B} \quad (5)$$

   c. Bob key is $\mathbb{K}^B = \{k_i\}$, such that for all $L_p$

$$k_i = \begin{cases} b_i & \forall b_i \in \mathbb{B}, i \in \mathbb{F} - \mathbb{E}. \\ r_i & \forall (r_i, l_i, i) \in \mathbb{K}_{Tp}^{B}, \forall i \in L_p, \\ & l_i \notin \mathbb{F}, \forall p, 0 \le p \le l! \end{cases} \quad (6)$$

Based on step (6) points (a),(b) and (c) above, the complexity of this algorithm is related to three internal loops, they are the number of permutations used $p$, the size of each set which is $l = \lfloor log_2 n \rfloor + 1$ and the number of bits used from the key $\mathbb{K}_I^A = \frac{|\mathbb{F}|}{2}$, i.e., $O(\frac{p \mid F \mid log\, n}{2})$.

## Gain Analysis

To calculate the gain of P-RUQB it is needed to have a deeper analysis of the gain of RUQB. The new analysis is based on finding the probability of having single gain after performing each iteration, and then extending the analysis for P-RUQB.

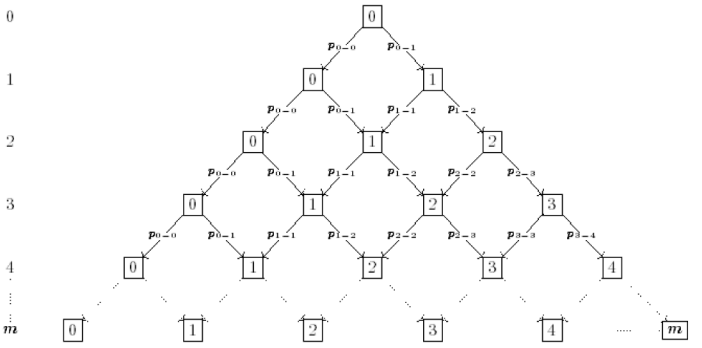
## RUQB Analysis

The analysis of gain $G$ done by Abu-ayyash and Ajlouni (2008) for RUQB was shown to be calculated as

$$G = \left(\frac{|F|}{2} - |E| - l\right) P_{clu} P_{cv} (1 - P_{l_r}) \quad (7)$$

where $|F|$ the size of the sifted key {for BB84 it is approximately $\frac{n}{2}$ and B92 is approximately $\frac{n}{4}$ }, $|E|$ is the expected number of bits to be eliminated if there is an error, in the best case the algorithm eliminates only the errors, but this is not the case (it depends on the algorithm used to eliminate those errors, Shannon estimated the minimum limit for the number of bits that need to be communicated to

*Figure 1. Probability diagram for the gain value of* $0,1,\ldots,m$ *after iterating* $\boldsymbol{m}$ *times where* $\boldsymbol{p_{i\to j}}$ *is the probability of having gain* $\boldsymbol{j}$ *if the previous gain was* $\boldsymbol{i}$



eliminate errors based on the probability of error for each transmitted bit $\epsilon$ to be $nh(\epsilon)$, some algorithms needs more $ynh(\epsilon)$, where $y \geq 1$, see Gilbert and Hamrick (2000), $l = \lceil log_2 n \rceil + 1$, $P_{clu}$ the probability that the calculated location of RUQB will not be used within the initial key {for BB84 it is approximately $\frac{1}{2}$ and for B92 $\frac{3}{4}$}, $P_{cv}$ probability of correct value found at unused location and it is approximately $\frac{1}{2}$, $P_{l_r}$ is the probability of redundant locations which is a random number generator (RNG) dependent.

The idea of RUQB starts with no gain (the original QKD key length), then after the first iteration, the gain is either increased by 1 or not with probability $p_{0\to 1}$ and $p_{0\to 0}$ respectively, such probabilities is based on the random result of the interpretation on the sets used, with respect to the percentage of the length of the original key to the total number of qubits used. From Figure 1, a more comprehensive analysis for the probability to have gain $x$ after $m$ iterations, where $P(x)_m$ is the sum of all the products of the paths from 0 (top most node) to the node $x$ at level (iteration) $m$:

$$P(x)_m = \prod_{i=0}^{x-1} p_{i\to(i+1)} \left( \sum_{\substack{0\leq y_k \leq x \\ \sum_{k=0}^{x} y_k = m-x}} \left( \prod_{k=0}^{x} (p_{k\to k})^{y_k} \right) \right) \quad (8)$$

Where $p_{i\to(i+1)}$ is the probability for having a gain value of $(i+1)$ after single iteration when the previous gain was $i$, $p_{k\to k}$ is the probability of no change of gain after single iteration.

A simplified recursive version of Equation (8) can be defined as:

$$P(x)_m = \left(P\left(x\right)_{m-1}\right) p_{x\to x} + \left(P\left(x-1\right)_{m-1}\right) p_{(x-1)\to x} \quad (9)$$

Where

$$p_{i\to i} = \left(1 - p_{i\to i+1}\right) \quad (10)$$

and

$$p_{i\to i+1} = (p_{0\to 1} - iD) \quad (11)$$

Where $D$ is the decrease in probability due to increase of gain by $1$; typically equal to $\frac{1}{n}$).

For example the probability of having no gain $0$ after $m$ iterations is

$$P(0)_m = \overbrace{(p_{0\to 0})...(p_{0\to 0})}^{m\ times} = (p_{0\to 0})^m = (1-p_{0\to 1})^m$$

Hence, the probability of having no gain after one iteration is $P(0)_1 = p_{0\to 0} = 1-p_{0\to 1}$.

And the probability of having the maximum gain $m$ after $m$ iterations is

$$P(m)_m = (p_{0\to 1})(p_{1\to 2})...(p_{(m-1)\to m}) = \prod_{i=0}^{m-1}(p_{i\to(i+1)}).$$

Hence, the probability of having one gain after one iteration is $P(1)_1 = p_{0\to 1}$.

The expected gain after $m$ iterations is

$$E = \sum_{i=0}^{m} iP(i)_m \tag{12}$$

$$= p_{0\to 1}\sum_{j=0}^{m-1}\left(\frac{-1}{2n}\right)^{m-j-1}\binom{m}{j} \tag{13}$$

$$= 2np_{0\to 1}\left(1-(1-\frac{1}{2n})^m\right) \tag{14}$$

Note that the expected gain depends on three factors; $n$ number of all qubits used by original QKD protocol, $p_{0\to 1}$ probability to have a gain of one bit after one iteration when previously no gain was found (it is also a QKD protocol dependent) and $m$ the number of iterations used by RUQB protocol.

Note that $m$ dependents on $n$ the total number of original random bits, the size of the final sifted key $\frac{|F|}{2}$ after eliminating more bits due to errors found within the key $\frac{|F|h(\epsilon)}{2}$, list size $l = \log_2 n + 1$ and $I_e$ information gained by the eavesdropper, let's sum all that in a function divided by $n$ and call it:

$$f(\epsilon) = \left(\frac{|F|}{2n} - \frac{|F|h(\epsilon)}{2n} - \frac{\log_2 n}{n} - \frac{1}{n} - \frac{I_e}{n}\right) \tag{15}$$

$$= \left(\frac{|F|}{2n}[1-h(\epsilon)] - \frac{\log_2 n}{n} - \frac{1}{n} - \frac{I_e}{n}\right) \tag{16}$$

Where $h(\epsilon)$ is the Shannon limit, $I_e$ is the Information gained by an eavesdropper, so replacing $m$ maximum iterations by $nf(\epsilon)$ the expected gain is

$$E = 2np_{0\to 1}\left(1-(1-\frac{1}{2n})^{nf(\epsilon)}\right) \tag{17}$$

$$= 2np_{0\to 1}\left(1-e^{-\frac{f(\epsilon)}{2}}\right) \tag{18}$$

For BB84 and RUQB

$$p_{0\to 1} = \frac{1}{4},$$

$$f(\epsilon) = \left(\frac{1}{4} - \frac{h(\epsilon)}{4} - \frac{\log n}{\frac{2}{n}} - \frac{1}{n}\right),$$

where $h(\epsilon)$ is Shannon limit. In general, for no errors and large values of $n$, Equation (18) results in

$$E_{RUQB} = \frac{n}{2}\left(1-e^{-\frac{1}{8}}\right) \tag{19}$$

Which mean that the expected gain for BB84 using RUQB for large values of $n$ is

*Table 1. Average of 10 runs for each* $\boldsymbol{x}$ *without errors,* $n = 2^{12}$

| $x$ | $\bar{G}$ | $\bar{G}\%$ | $E$ | $E\%$ | $r$ | $x$ | $\bar{G}$ | $\bar{G}\%$ | $E$ | $E\%$ | $r$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | 236.5 | 5.70 | 240 | 5.87 | 0.02896 | **16** | 1738.8 | 42.45 | 1770 | 43.23 | 0.01804 |
| **2** | 450.9 | 11.00 | 453 | 11.06 | 0.00542 | **17** | 1765.6 | 43.10 | 1803 | 44.02 | 0.0209 |
| **3** | 615.7 | 15.03 | 640 | 15.63 | 0.03839 | **18** | 1785.0 | 43.57 | 1832 | 44.73 | 0.02593 |
| **4** | 797.7 | 19.47 | 805 | 19.67 | 0.01017 | **19** | 1814.2 | 44.29 | 1857 | 45.34 | 0.02316 |
| **5** | 916.1 | 22.36 | 951 | 23.23 | 0.03745 | **20** | 1835.6 | 44.81 | 1879 | 45.89 | 0.02353 |
| **6** | 1056.4 | 25.79 | 1080 | 26.38 | 0.02237 | **21** | 1843.9 | 45.01 | 1899 | 46.37 | 0.02933 |
| **7** | 1158.3 | 28.27 | 1194 | 29.15 | 0.03019 | **22** | 1877.3 | 45.83 | 1917 | 46.80 | 0.02073 |
| **8** | 1249.7 | 30.51 | 1294 | 31.61 | 0.0348 | **23** | 1898.5 | 46.35 | 1932 | 47.17 | 0.01738 |
| **9** | 1340.1 | 32.71 | 1383 | 33.76 | 0.0311 | **24** | 1881.8 | 45.94 | 1946 | 47.75 | 0.03791 |
| **10** | 1431.2 | 34.94 | 1461 | 35.67 | 0.02047 | **25** | 1920.7 | 46.89 | 1958 | 47.80 | 0.01904 |
| **11** | 1492.0 | 36.42 | 1530 | 37.36 | 0.02516 | **26** | 1922.1 | 46.92 | 1968 | 48.06 | 0.02372 |
| **12** | 1547.9 | 37.79 | 1591 | 38.84 | 0.02703 | **27** | 1957.2 | 47.78 | 1977 | 48.28 | 0.01036 |
| **13** | 1609.6 | 39.29 | 1644 | 40.15 | 0.02142 | **28** | 1947.6 | 47.54 | 1986 | 48.49 | 0.01959 |
| **14** | 1644.2 | 40.14 | 1692 | 41.31 | 0.02832 | **29** | 1969.3 | 48.07 | 1993 | 48.66 | 0.01212 |
| **15** | 1686.9 | 41.18 | 1733 | 42.33 | 0.02717 | **30** | 1975.0 | 48.23 | 1999 | 48.82 | 0.01209 |

$$E_{RUQB} \simeq 0.0588n \tag{20}$$

In Table 1 of Abu-ayyash and Ajlouni (2008) no errors where assumed, and $n$ was not a large value, therefore by using Equation (17) and solving for $b$ (gain percentage)

$$E_{BB84} = nb = \frac{n}{2}\left(1-(1-\frac{1}{2n})^{\frac{n}{4}-\log n-1}\right) \tag{21}$$

$$= \frac{n}{2}\left(1-\frac{e^{-\frac{1}{8}}}{(1-\frac{1}{2n})^{\log n+1}}\right) \tag{22}$$

$$= \frac{n}{2}\left(1-\frac{e^{-\frac{1}{8}}}{(1-\frac{1}{2n})^{\log n+1}}\right) \tag{23}$$

$$b \approx 0.0564 \tag{24}$$

This result is approximately similar to the results obtained by Abu-ayyash and Ajlouni (2008).

## P-RUQB Analysis

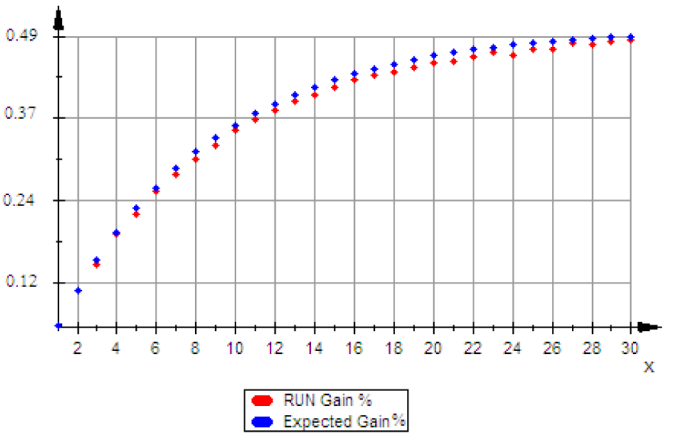
In Equation (14) replacing $m$ by $xnf(\epsilon)$, where $x$ is a multiplication factor that represents number of permutations to be used, will result in

$$E = 2np_{0\to 1}\left(1-e^{-\frac{xf(\epsilon)}{2}}\right) \tag{25}$$

From Equation (25), as the multiplication factor $x$ increase the gain $E$ increase, i.e.:

$$\lim_{x\to\infty} 2np_{0\to 1}\left(1-e^{-\frac{xf(\epsilon)}{2}}\right) = 2np_{0\to 1} \tag{26}$$

*Figure 2. Gain values for multiple P-RUQB iterations up to* $30$ *iterations for number of photons* $n = 2^{12}$ *See Table 1*




In this case the gain cannot be $2np_{0\to1}$; for which, an infinity permutations is used, while the maximum available permutations is only $l!$, also note that the gain do not increase linearly with the increase of the multiplication factor, see Figure 2.

Based on the assumption that the best (optimal) $\hat{x}$ value for the multiplication factor $x$ (integer value) can be found when the speed of change of gain $E$ at iteration $x$ is half the initial speed of change of gain (i.e., at $x = 1$). Differentiate Equation (25) with respect to $x$:

$$\frac{d}{dx}E = np_{0\to1}f(\epsilon)e^{-\frac{xf(\epsilon)}{2}} \tag{27}$$

Allow it to equal half the derivative at $x = 1$ and solve for optimal $x$

$$np_{0\to1}f(\epsilon)e^{-\frac{\hat{x}f(\epsilon)}{2}} = \frac{n}{2}p_{0\to1}f(\epsilon)e^{-\frac{f(\epsilon)}{2}} \tag{28}$$

$$\hat{x} = 1 + \frac{2ln2}{f(\epsilon)} \tag{29}$$

Note that the optimal value for $\hat{x}$ is dependant on the error $\epsilon$, in the following two subsections a discussion will be presented for running P-RUQB in two situations, the absence and presence of errors.

## P-RUQB without Errors

Assume that the quantum channel is error free, and Eve is not eavesdropping on the quantum channel, for BB84 value of $|F| = \frac{n}{2}$ then $f(\epsilon) \simeq \frac{1}{4}$, therefore the optimal value based on Equation (29) with no errors is

$$\hat{x}_{ne} \simeq 8\ln 2 + 1 = 7 \tag{30}$$

And the optimal expected gain $E$ is

$$\hat{E}_{ne} \simeq 2np_{0\to1}\left(1 - e^{-\frac{7}{8}}\right) \tag{31}$$

$$\simeq 1.17np_{0\to1} \tag{32}$$

BB84 and RUQB has $p_{0\to1} = \frac{1}{4}$ so the optimal gain is estimated as

$$\widehat{E}_{ne} \simeq 0.29n \tag{33}$$

See Figure 2. Table 1 lists an average of 10 runs for each selected $x$.

If Eve is eavesdropping on the quantum channel but still no errors is detected this may indicate that she is using a beam splitting (photon number splitting PNS) attack, where each pulse may contains two or more photons, the estimated bits leaked according to Bennett and Brassard (1992) is related only to the physical (and statistical) characteristic of photon pulse generator; the mean number of photons per pulse $\mu$, where the leak is $|F|\mu$ in addition to a suggested safe factor of *five* standard divination $5\sqrt{|F|\mu(1-\mu)}$, so the information gained by an eavesdropper is

$$I_e = |F|\mu + 5\sqrt{|F|\mu(1-\mu)} \tag{34}$$

a more comprehensive analysis done by Gilbert and Hamrick (2000), includes other physical parameters; the attenuation $\alpha$ of the quantum channel between Alice, Eve and Bob, in addition to Eve's controlling parameters $\rho$ and $u$ where they represent the degree to which she can adjust the transparency of the quantum channel and the number of photons that she chooses to remove from the multi-photon pulse for future use respectively, in addition to the efficiency of Bob detector $\eta$. The leak is related to the number of pulses containing more than two photons, and (decreased) by the non-efficient amount that is controlled by parameters $S(\alpha,\rho,u,\eta)$, so the information gained by an eavesdropper now is

$$I_e = \frac{M}{2}\left[1 - e^{-\mu}(1+\mu) - S(\alpha,\rho,u,\eta)\right] \tag{35}$$

Where $M$ is the total number of laser pulses. This leak is included in Equation (16). Back to Equation (29) the optimal multiplication factor of P-RUQB where $f(\epsilon) = \frac{1}{4} - \frac{I_e}{n}$ for BB84 is

$$\hat{x}_{ne\_I_e} = 1 + \frac{8ln2}{1 - 4\frac{I_e}{n}} \tag{36}$$

## P-RUQB with Errors

If the quantum channel is not error-free (but Eve is not eavesdropping on the quantum channel, and without paying attention to the physical properties of the equipments) then errors will be within the sifted key and they should be eliminated, error rate (percentage) can be estimated by comparing random bits of the key, Shannon theorem (Shannon, 1948) estimates the minimum number of bits to be eliminated by error correction as $\frac{|F|}{2}h(\epsilon)$, where

$$h(\epsilon) = -(\epsilon \log_2 \epsilon + (1-\epsilon)\log_2(1-\epsilon))$$

and $|F| = \frac{n}{2}$ for BB84, and for big value of $n$

$$f(\epsilon) \simeq \frac{1}{4}(1 - h(\epsilon)) \tag{37}$$

Therefore the optimal $x$ is

$$\hat{x}_e \simeq 1 + \frac{8ln2}{1 - h(\epsilon)} \tag{38}$$

And optimal expected gain $\widehat{E}_e$ is

$$\widehat{E}_e \simeq \frac{n}{4}\left(2 - e^{-\frac{1-h(\epsilon)}{8}}\right) \tag{39}$$

The effect of errors percentage $\epsilon$ on optimal $x$ and expected gain can be seen in

*Figure 3. The effect of error percentage $\epsilon$ on optimal $\hat{x}$*

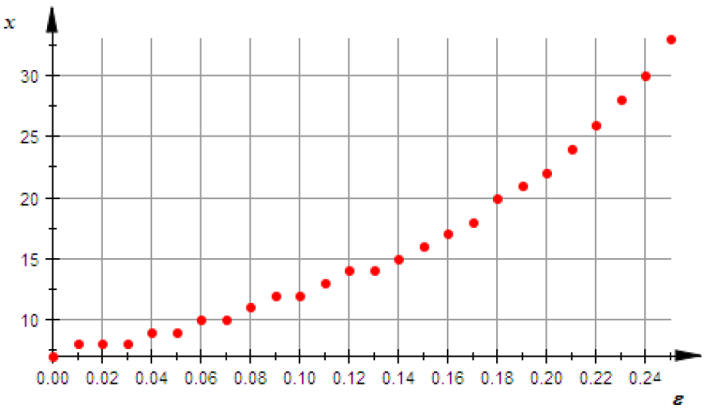



Figure 3 and Figure 4 respectively. Note that due to errors, optimal $x$ should be increased to maintain approximately the same expected gain percentage. In Gilbert and Hamrick (2000) a study to include the physical parameters of the devices in the estimation of errors without eavesdropping is

$$\epsilon_e \simeq \frac{M}{2}\left\{r_c(1-e^{-\mu\alpha\eta})+\frac{r_d}{2}\right\} \tag{40}$$

Where $r_c$ is intrinsic quantum channel error rate, $r_d$ is dark count rate by Bob detector.

Due to Bennett and Brassard (1992) if Eve is eavesdropping on the quantum channel and the channel is not error free (using only $\mu$ and $\epsilon$ ), then

$$I_e = \left|F\right|\left(\mu+2\sqrt{2}\epsilon\right) +5\sqrt{\left|F\right|(\mu(1-\mu)+(4+2\sqrt{2})\epsilon)} \tag{41}$$

This value should be used in Equation (36), a more comprehensive analysis can be found in Gilbert and Hamrick (2000).

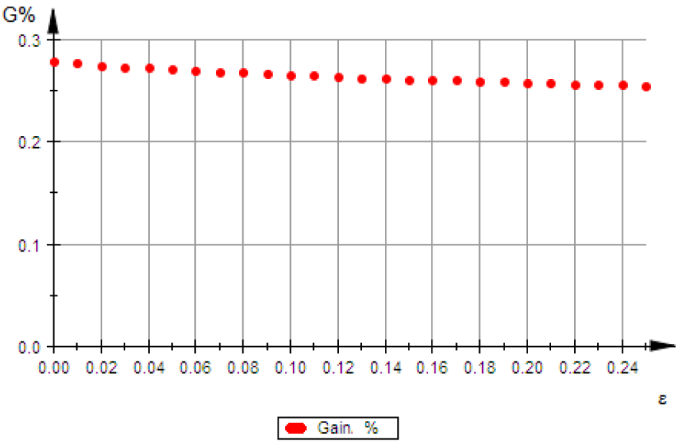
## SECURITY ANALYSIS

It is necessary to identify whether P-RUQB causes more information to be leaked than RUQB regarding both initial and final keys. Assuming that both RUQB and P-RUQB techniques allows Eve to be in possession of all sets $L_p$ that contains the indexes of the locations within the initial key, such sets will contribute to more bits within the final key. In this research RUQB security analysis will be discussed then it will be compared to P-RUQB.

### RUQB Security Analysis

In the RUQB algorithm an eavesdropper will be able to get the list of indexes that Alice sends to Bob, let $L=\{i_1,i_2,\cdots,i_s\}$ denote the list of indexes, $x_{l_j}$ denote the new bit value calculated based on the list $L$ starting at index $i_j$ using a maximum of $l$ sequential bits and $l_j$ be the calculated location for $x_{l_j}$, then an eavesdropper will be able to construct the following system of equations

*Figure 4. The effect of error percentage $\epsilon$ on gain percentage*




$$x_{l_1} = x_{i_1} \oplus x_{(i_1+1)} \oplus x_{(i_1+2)} \oplus \cdots \oplus x_{(i_1+l-1)}$$

$$l_1 = x_{i_1} 2^0 + x_{(i_1+1)} 2^1 + x_{(i_1+2)} 2^2 + \cdots + x_{(i_1+l-1)} 2^{l-1} \bmod n$$

$$x_{l_2} = x_{i_2} \oplus x_{(i_2+1)} \oplus x_{(i_2+2)} \oplus \cdots \oplus x_{(i_2+l-1)}$$

$$l_2 = x_{i_2} 2^0 + x_{(i_2+1)} 2^1 + x_{(i_2+2)} 2^2 + \cdots + x_{(i_2+l-1)} 2^{l-1} \bmod n$$

$$\vdots$$

$$x_{l_s} = x_{i_s} \oplus x_{(i_s+1)} \oplus x_{(i_s+2)} \oplus \cdots \oplus x_{(i_s+l-1)}$$

$$l_s = x_{i_s} 2^0 + x_{(i_s+1)} 2^1 + x_{(i_s+2)} 2^2 + \cdots + x_{(i_s+l-1)} 2^{l-1} \bmod n$$

Note that the size of the list is $|L| = s = gn$, where $g$ is the RUQB gain (every element within the list contribute to a bit of gain), from the above system of equation the number of equation $\mathcal{E}$ is

$$\mathcal{E} = 2s \tag{42}$$

Were each element in list $L$ results in two equations; one for location $l_j$ and the other for result $x_{l_j}$, the number of variables $\mathcal{V}$ in the system of equation is

$$\mathcal{V} = s(2 + dl) \tag{43}$$

Were each element in list $L$ results in two variables on the left hand side of the equations plus on average $dl$ variables for each equation, where $l = \log n + 1$, $d$ is a percentage depends on the distance between elements of $L$ and can be calculated as,

$$d = \begin{cases} \breve{d} & \text{if } \breve{d} < 1 \\ 1 & \text{if } \breve{d} \geq 1 \end{cases} \tag{44}$$

Where

$$\breve{d} = \frac{1}{l(s-1)} \sum_{k=1}^{s-1} (i_{k+1} - i_k) \tag{45}$$

And it has a maximum value of 1, see Equation (44), denoting that there is no intersection between the variables used by each equa-

tion. The ratio $R$ between the number of equations to the number of variable shows the ability for an eavesdropper to solve this system of equation to gain full knowledge about the original key and the gained bits, so

$$R = \frac{\mathcal{E}}{\mathcal{V}} \tag{46}$$

$$= \frac{2}{2 + d(\log n + 1)} \tag{47}$$

since $d$ depends on the distance between the elements of the list $L$ it is never 0 since at least each element is different than the other by one location, also it is uncommon to have the value of 1 since then all elements are far away from each other, so $0 < d \leq 1$ and the limit of the ratio as $n$ reach for infinity is 0 (i.e., the number of variables is far more than the number of equation and hence the eavesdropper will not be able to solve the system of equations).

## P-RUQB Security Analysis

For P-RUQB the number of equation is far more than RUQB, applying the same analogy, if the list of indexes is $L_j$

$$L_j = \{i_{1j}, i_{2j}, \cdots, i_{sj}\} \tag{48}$$

Then the number of equation is

$$\mathcal{E} = 2\sum_j \mid L_j \mid = 2g^{'}n \tag{49}$$

Where $\mid L_j \mid$ is the length of the list $L_j$, $g^{'}$ is P-RUQB gain, the number of variables used also

$$\mathcal{V} = h\frac{\mid F \mid}{2} + 2\sum_i \mid L_j \mid = h\frac{\mid F \mid}{2} + 2g^{'}n \tag{50}$$

Where $\mid F \mid$ is the initial sifted key size, and $h$ is the percentage used from the initial key $0 < h \leq h$, so the ratio is

$$R = \frac{\mathcal{E}}{\mathcal{V}}$$

$$= \frac{2g^{'}n}{h\frac{\mid F \mid}{2} + 2g^{'}n} \tag{51}$$

And the limit of $R$ as $n$ reaches infinity is dependent on $h$ and since $\mid F \mid = \frac{n}{2}$ for BB84 then the limit

$$\lim_{n\to\infty} R = \frac{8g^{'}}{8g^{'} + h} \tag{52}$$

And since $g^{'}$ for BB84 and P-RUQB is 0.29 then the limit is

$$\lim_{n\to\infty} R = \frac{2.32}{2.32 + h} \tag{53}$$

based on $h$, the ratio $R$ range from 0.6987 (for $h = 1$ ; i.e., all initial key bits are used) to 0.958 (for $h = 0.1$ ; only 0.1 of the initial key bits are used), in practice approximately all initial key bits will be used, so the ratio is 0.7 since this will give an eavesdropper more information than RUQB but still not enough to solve the system of equations for large values of $n$ . So if an eavesdropper has any or both of the following conditions hold:-

1. All the locations within the initial key that happen to be within $L_j$ are known (i.e., specific 11% of the initial key is known by Eve).
2. A known sequence of $l$ or more bits within the initial key and the start of this sequence must be within $L_j$ (i.e., with a probability of 11% this sequence contribute to new bit).

Then the system of equation begins to solve.

## Randomness Effect

Both algorithms (RUQB and P-RUQB) depend on the interpretation of the sequence of bits that contribute to the initial key (the original key). The higher the randomness of bits generated, the higher would be the expected gain obtained. This is due to the fact that randomness will cause the probability of any location to be interpreted equal, see Equation (11); where both $p_{0\to1}$ and $D$ are constants and dependent on randomness; the former is QKD protocol dependent, while the latter is only randomness dependent (the randomness of the generated bits) and equal to $\frac{1}{n}$.

If the bits are not completely random, then some interpretations (for new locations) are more likely than others, which results in redundancy in interpretation, and hence, degradation in gain obtained. Back to Equation (11), both $p_{0\to1}$ and $D$ will be degraded by the same redundancy factor (percentage) $r = [0..1]$ (where 0 is for no redundancy in location interpretations, and 1 is for full redundancy, i.e., all interpretations are for the same location, in general $r$ is close to 0 not 1), so

$$p_{i\to i+1} = \left(1-r\right)\left(p_{0\to1} - \frac{i}{n}\right) \tag{54}$$

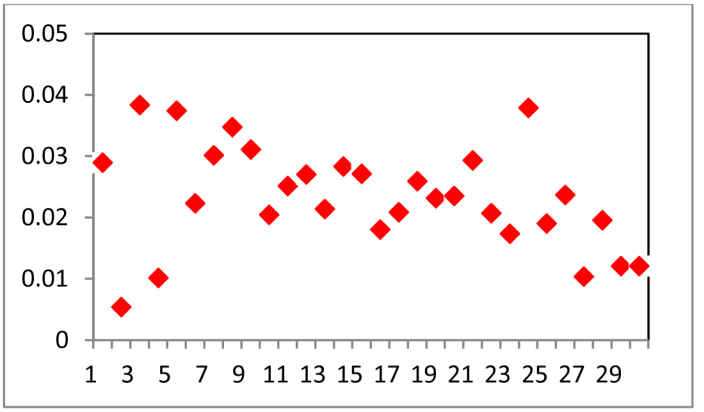
Replacing $\left(1-r\right)$ by $c$, and recalculating the expected gain (Equation (12)) will results in same factor to be included in the expected gain. This is given by

$$E_r = 2cnp_{0\to1}\left(1-\left(1-\frac{1}{2n}\right)^m\right) \tag{55}$$

Where $c$ is the inverse of the redundancy factor (i.e., 0 is for full redundancy and 1 is for no redundancy; now $c$ is close to 1 not 0). Note that in Table 1 and Figure 2 as it can be seen there is a small difference between calculated, and the actual gain obtained; $r$ varies between 0.0054 and 0.0384 with average of 0.0234. See Figure 5.

Randomness is used for security improvement, however gain is affected by randomness, at the same time the number of both variables and equations are also affected (degraded). As a source of randomness some QKD schemes and implementations are using entanglement (ERP Based) quantum states as a source for both information carrier and randomness, while Pironio, et al. (2010) noted that random numbers

*Figure 5. Calculated* ***r*** *based on the difference between expected and calculated gain as a result of randomness for each* $x$



(generated and used during QKD protocol using EPR states) can be certified based on the violation of Bell's inequalities (Bell, 1964; Gerhardt et al., 2011) showed that this certification can be refuted experimentally if the violation was not *loophole-free*, i.e., there is no classical communication between communicating parties used to fake results and there is no kind of shared randomness between communicating parties; both will result in statistical violation of Bell's inequalities, hence false sense of randomness and security. Another research (Bouda et al., 2012) showed that security of QKD will ruined if an eavesdropper is in position of partial and limited access to the source of randomness that is used by the protocol.

## CONCLUSION

QKD protocols uses quantum phenomena as a source of randomness to generate bits or qubits, sometimes, QKD protocols suffers from a gain problem; In this research it was found that P-RUQB achieved an enhancement over RUQB by recovering around 50-60% from the unused bits which is equal to around 30% gain, which means that some quantum lost bits are recovered.

The recovery is achieved by re-examining the initial 50% of the bits assumed to be lost. This is based on the process of finding relationships between the random bits generated.

A comprehensive analysis for both the gain and the security for both algorithms (RUQB and P-RUQB) were discussed; it was shown that P-RUQB achieves higher gain than RUQB, while the latter maintains better security. Both RUQB and P-RUQB are randomness dependent and the higher randomness the higher the gain. The complexity of P-RUQB was shown to be

$$O\left(\frac{\hat{x}\left|F\right|\log n}{2}\right);$$

while for BB84 a near optimal number of permutations 8. The algorithm is of the order $O\left(n\log n\right)$.

## REFERENCES


Abu-ayyash, A. M., & Ajlouni, N. (2008). QKD: Recovering unused quantum bits. In *Proceedings of the 3rd IEEE International Conference on Information and Communication Technologies*, Damascus, Syria (pp. 1-5).

Abu-Ayyash, A. M., & Jabbar, S. (2003). Fraction integer method: Calculating multiplicative inverse. In *Proceedings of the 7th World Multi-conference on Systemics, Cybernetics and Informatics*, Orlando, FL (pp. 49-53).

Barrett, J., Hardy, L., & Kent, A. (2005). No signalling and quantum key distribution. *Physical Review Letters*, *95*, 010503. doi:10.1103/PhysRevLett.95.010503

Bell, J. S. (1964). On the Einstein Podolsky Rosen Paradox. *Physics*, *1*, 195.

Bennett, C. (1992). Quantum cryptography using any two non orthogonalstates. *Physical Review Letters*, *68*(21), 3121–3124. doi:10.1103/PhysRevLett.68.3121

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, System, and Signal Processing*, Bangalore, India (pp. 175-179).

Bennett, C. H., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. *Journal of Cryptology*, *5*, 3. doi:10.1007/BF00191318

Bostrom, K., & Felbinger, T. (2002). Deterministic secure direct communication using entanglement. *Physical Review Letters*, *89*, 187902. doi:10.1103/PhysRevLett.89.187902

Bouda, J., Pivoluska, M., Plesch, M., & Wilmott, C. (2012). *Weak randomness, completely trounces the security of QKD*. Retrieved from http://arxiv.org/abs/1206.1287

Chou, C. W., Polyakov, S. V., Kuzmich, A., & Kimble, H. J. (2004). Single-photon generation from stored excitation in an atomic ensemble. *Physical Review Letters*, *92*, 213601. doi:10.1103/PhysRevLett.92.213601

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*, 644–654. doi:10.1109/TIT.1976.1055638

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, *47*, 777–780. doi:10.1103/PhysRev.47.777

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, *67*, 661–663. doi:10.1103/PhysRevLett.67.661

Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Scarani, V., Makarov, V., & Kurtsiefer, C. (2011). Experimentally faking the violation of Bell's inequalities. *Physical Review Letters*, *107*, 170404. doi:10.1103/PhysRevLett.107.170404

Gilbert, G., & Hamrick, M. (2000). *Practical quantum cryptography: A comprehensive analysis* (Tech. Rep.). Bedford, MA: Mitre.

Groblacher, S., Jennewein, T., Vaziri, A., Weihs, G., & Zeilinger, A. (2005). Experimental quantum cryptography with Qutrits. *New Journal of Physics*, *8*, 75. doi:10.1088/1367-2630/8/5/075

Hwang, W. Y., Koh, I. G., & Han, Y. D. (1997). Quantum cryptography without public announcement bases. *Physics Letters. [Part A]*, *244*(6), 489–494. doi:10.1016/S0375-9601(98)00358-2

Kak, S. (2006). A three-stage quantum cryptography protocol. *Foundations of Physics Letters*, *19*, 293–296. doi:10.1007/s10702-006-0520-9

Kanamori, Y., Yoo, S.-M., & Al-Shurman, M. (2005, March 18-20). A quantum no-key protocol for secure data communication. In *Proceedings of the 43rd Annual Southeast Regional Conference*, Kennesaw, GA (pp. 92-93).

Kuang, L.-M., & Zhoul, L. (2004). *Generation of atom-photon entangled states in atomic Bose-Einstein condensate via electromagnetically induced transparency*. Retrieved from http://arxiv.org/pdf/quant-ph/0402031.pdf

Lucamarini, M., & Mancini, S. (2004). Secure deterministic communication without entanglement. *Physical Review Letters*, *94*(14), 140501. doi:10.1103/PhysRevLett.94.140501

Menezes, A., van Oorschot, P., & Vanstone, S. (1997). *Handbook of applied cryptography*. Boca Raton, FL: CRC Press.

Pironio, S., Acín, A., Massar, S., Boyer de la Giroday, A., Matsukevich, D. N., & Monroe, C. (2010). Random numbers certified by Bell's Theorem. *Nature*, *464*, 1021–1024. doi:10.1038/nature09008

Price, W., Chissick, S., & Heisenberg, W. (1977). *The uncertainty principle and foundations of quantum mechanics: A fifty years survey*. New York, NY: John Wiley & Sons.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and publickey cryptosystems. *Communications of the ACM*, *21*, 120–126. doi:10.1145/359340.359342

Santori, C., Fattal, D., Vuckovic, J., Solomon, G. S., & Yamamoto, Y. (2004). Generation of single photons and correlated photon pairs using InAs quantum dots. *Fortschritte der Physik*, *52*(11-12), 1180–1188. doi:10.1002/prop.200410188

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, *27*, 379–423, 623–656.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, *28*, 656–715.

Tisa, S., Tosi, A., & Zappa, F. (2007). Fully-integrated CMOS single photon counter. *Optics Express*, *15*(6), 2873–2887. doi:10.1364/OE.15.002873

Vernam, G. S. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the IEEE*, *55*, 109–115.

Wiesner, S. (1983). Conjugate coding. *Sigact News*, *15*(1), 78. doi:10.1145/1008908.1008920

Yang, C.-N., & Kuo, C.-C. (2002). A new efficient quantum key distribution protocol, quantum optics in computing and communications. In *Proceedings of the SPIE Conference* (Vol. 4917).

*Abdulla M. Abu-ayyash is currently the information security officer at CBJ, has both BSc and MSc in computer science from Jordan University in 1987 and 1999 respectively, and PhD in CIS from Arab Academy - Jordan in 2008. Formally was responsible for the design and implementation of the initial internal and external network structure, and for establishing and managing the technical team at CBJ, published some papers in conferences related to cryptographic key generation and QKD; member of IEEE, ACM, and IEEE Computer society.*

*Naim Ajlouni is currently the Chairman of Assuit University Program in Jordan and Palestinian territory. Dr. Ajlouni obtained a BSc in Electrical from Bolton University, UK, in 1983 and Electronics Engineering, MS in Robot Control from Salford University, UK in 1992, and PhD in Intelligent Control from Salford University, UK, in 1995. Dr. Ajlouni worked for a company called Dextralog Ltd. in UK as project manager (1983 to 1991) and in a number of educational institutes including Salford University, Applied Science University, Amman Arab University, Al Balqa' Applied University. Dr. Ajlouni has held a number of academic positions including Head of Department, Dean Vice President, and President. Dr. Ajlouni published 35 papers in International refereed journals and 43 papers in international conferences and is a member of IEEE, and International Affairs Council – Jordan.*