I.J. Mathematical Sciences and Computing, **2017, 2, 11-21**
Published Online April 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2017.02.02

Available online at ***http://www.mecs-press.net/ijmsc***

Revisited Quantum Protocols

Shyam Sihare [a], Dr. V V Nath [b,*]

[a] *Gujarat University, Dr. APJ Abdul Kalam Govt. College, Silvassa-396235, India*
[b] *Nirma University of Institute of Management, Ahmedabad-380001, India*

Abstract

Quantum cryptography is marches towards secure communication by using quantum protocols. Number of quantum protocols has been evolved based on an entanglement in three decades; similarly during this meanwhile non-entanglement based protocols have been evolved within the same period also. Among number of different protocols a torch bearer was BB84 protocol. Even though different quantum communication protocols exist, the BB84 protocol proved its application by initial experiments whereas most of the other protocols are theoretical which marches towards the practical application yet. But in quantum mechanics principle, cryptography based on an entanglement and superposition of entangled particle. Furthermore, challenges ahead are development and design high sensitive equipments for measurement of an entangled particle position at output end. Particle entanglements open a new door for computation worlds such as speedup, security. In this article, we discuss quantum protocols, their challenges, and applications based on above discussion.

Index Terms: BB84 (Bennett and Brassard Protocol), Cryptography, Entanglement, Quantum Protocols, Superposition.

1. Introduction and Related Works

Communication is a mechanism depends on words juxtaposition with corresponding similar words. In electronic world, it is define as in trivial form, pulses modulation as per requirement. A notable classical communication protocol is RSA protocol of a conventional system in perspective of cryptography. Most of the classical system protocols have had enough strength to establish secure communication with a presence of third party. Due to processing incapability of classical system, it seems hard to decode in polynomial time. Coming days also give guarantee about RSA algorithms strength. Hence, this algorithm used most of the commercial transaction like banking, industries, governmental, defense etc. Next, public or private key decryption needs at most exponential or higher time.

* Corresponding author.8000642070
E-mail address: shyams_sihare1979@rediffmail.com

Consider, A(lice) as a sender and B(ob) as a receiver of a network then $A \xrightarrow{key(x)} B$ path established, where *key(x)* is a key, either public or private. A quantum computer protocols application based on the Quantum Key Distribution (QKD), this was first time proposed by Brassard and Bennett as BB84 protocol in 1984[1]. The BB84 protocol significantly focuses on sharing of a quantum key from a sender (Alice) to a receiver (Bob). It applies single photon for secure communication from one entity (Alice) to other entity (Bob) with a presence of a third entity (Eve). It is a secure quantum communication protocols since a public and a private key sharing in a presence of eavesdropper Eve. At both ends deterministic or un-deterministic Turing machine could be used for this application. Later Arthur Eckert proposed E91 [2] protocol which uses particle entanglement on both sides (i.e. from Alice to Bob and vice versa and an Eve in between of Alice and Bob). An entangled particle gives guaranteed about secure quantum communication, it used in number of quantum protocols. This protocol based on BB84, B92 features; hence it is more sophisticated in terms of security. Addition of this, superposition exhibited in some extends into these protocols by which a state is in unpredictable in an initial phase. An entangled particle measurement is carried out to know basis states of a Hilbert space.

Next, a quantum teleportation protocol [4] use a guided media as well as an unguided media for teleporting quantum bits from a source to a destination; whereas an unguided media use the open space for teleporting qubits of a state space. Obviously, entangled states principle based on EPR paradox [5]. So qubit teleportation carried out from a source to a destination not more than the speed of light because quantum communication use deterministic/non-deterministic Turing machine.

All of these we look into Section-3 in details. However, most of the quantum protocols use photon entanglement, with that photon behavior follows quantum mechanics fundamental principle. Furthermore, it seems uncomfortable to apply completely Einstein entanglement principle in quantum communication protocols due to "*spooky action as a distance*".

Form above we can say that, photon entanglement effect gives guarantees about complete security during communication. Hence, it finds new cryptography mechanism which call quantum cryptography. It could be apply into classical Turing machine (deterministic or probabilistic Turing machine) or quantum Turing machine.

Today, open space quantum communication seems hard for long distance due to unavailability of quantum technologies. Open space quantum communication is too complex for reality at present. However, 2-7 qubits open space communication experiments show some extends successful. But, we could not confidently mention that it is commercially viable. Because following factors severely affect on open space quantum communication are–

- Superposition and entanglement properties of qubits.
- Quantum mechanics Heisenberg's uncertainty principle.
- Single photon readout equipments.
- Most modern technologies are deterministic Turing machine oriented.
- Nostalgic towards quantum algorithms and technologies during three decades.
- Nostalgic on quantum mechanics fundamentals conceptualization framework.

These points are specific concepts of quantum mechanics. Due to that these, create problems for commercial quantum computer developments. With that, various quantum protocols attempt to develop with the help of BB84, E91, dense coding (super-dense coding), and quantum teleportation. Enhancements of fundamental quantum protocols might be more secure protocols.

2. Quantum Communication Protocols

2.1 BB84 protocol

It was proposed by Brassard and Bennett in 1984. It acts as quantum cryptography by using quantum key

distribution (QKD). QKD first phase used quantum string $P_A(x)$, where *A* stand for A(lice) and *x* as a binary string encode into qubits. Afterword, imply public quantum key $K_1\ (P_A(x))$. The Second phase used private key $K_2\ (P_A(x))$ to transform sophisticated cryptography. Obviously, if public to private implication implies on the classical channel on qubits then Eve presence evidently visible and further communication stopped for a while.

$a = K_1(P_A(x))$, where *a* is a set of qubits encoded by a classical channel for sharing public key K_1.
$b = K_2(P_A(x))$, where *b* is a set of qubits further encoded by a classical channel for sharing private key K_2.

Clearly,

$$a.b = K_1(P_A(x)).\ K_2(P_A(x)) \tag{1}$$

If consider $P_A(x) = t_1$ then eq. (1) re-write

$$a.b = K_1(t_1).K_2(t_1) \tag{2}$$

$$a.b = K_1(K_2(t_1)) \tag{3}$$

$$b.a = K_2(K_1(t_1)) \text{ by commutative law} \tag{4}$$

But, $a.b \neq b.a$ since qubits properties of quantum mechanics does not permit commutative equality. The *a* and *b* encoded by a Alice end, as *b* as a private key and *a* as a public key, *c* qubits determine by the B(ob) end as qubits bases.

So, $c = a.b \oplus b.a$ plus any superposed qubits of *a.b* or *b.c*.

Nevertheless, there is no effect on secure transmission or quantum cryptography by commutative in a presence of Eve. But, before transmission from *A* to *B*, special treatment carried out by *A* or *B* such as change polarization angle for particle momentum.

Alice sends qubits by a classical channel i.e. encode $x \in \{0\}$ and $y \in \{1\}$ bits into a qubit $|\Psi_x\rangle$ and $|\Psi_y\rangle$ respectively

$$|\Psi_x\rangle = |\uparrow\rangle \text{ if } x \in \{0\} \tag{5}$$

$$|\Psi_y\rangle = |\downarrow\rangle \text{ if } y \in \{1\}$$
$$|\Psi_x\rangle + |\Psi_y\rangle = |\uparrow\rangle + |\downarrow\rangle \text{ if } x \in \{0\}, y \in \{1\} \tag{6}$$
$$|\Psi_x\Psi_y\rangle = |\uparrow\downarrow\rangle^1$$

$$|\Psi_{xy}\rangle = |\uparrow\downarrow\rangle \tag{7}$$

Eq. (6) claim that, particle in a superposition vector, which is represented as $|\uparrow\downarrow\rangle$ and interchange vector orientation which is represented by a reverse sign from + (plus) to – (sign).

Hence,

$$|\uparrow\downarrow\rangle \neq |\downarrow\uparrow\rangle \tag{8}$$

Eq. (8) claim that, tow particles orientation not equal to the base of amplitude amplification magnitude α and β. Eq. (4), (5), (6) and (7) could be represented as vector orientation in a Bloch Sphere (fig. 1).

[1] consider either $|\uparrow\downarrow\rangle$ or $|\downarrow\uparrow\rangle$ as $(|\uparrow\rangle \pm |\downarrow\rangle)/\sqrt{2}$

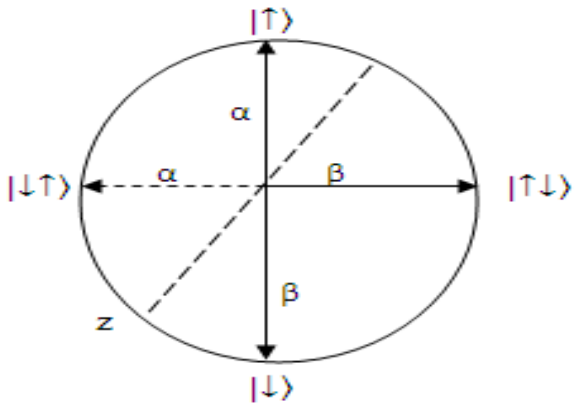

Fig.1. Bloch Sphere Representation of Different Vector and Its Corresponding Amplitude α and β

Eq. (4) and (5) are non-orthogonal, whereas eq. (6) and (7) are orthogonal. Hence, BB84 protocol mixed of both.

Further,

$$c= \begin{cases} |\Psi_x\rangle = |\uparrow\rangle \oplus |\downarrow\rangle, \text{if } x \in \{0,1\} \\ |\Psi_y\rangle = |\downarrow\rangle \oplus |\uparrow\rangle, \text{if } y \in \{1,0\} \\ |\Psi_{xy}\rangle = |\uparrow\downarrow\rangle \oplus |\downarrow\uparrow\rangle \oplus |\uparrow\rangle \oplus |\downarrow\rangle, \text{if } x \in \{0,1\}, y \in \{1,0\} \\ |\Psi_{xy}\rangle = |\downarrow\uparrow\rangle \oplus |\uparrow\downarrow\rangle \oplus |\downarrow\rangle \oplus |\uparrow\rangle, \text{if } x \in \{0,1\}, y \in \{1,0\} \end{cases} \quad (9)$$

Eq. (2), (3) and (9) indicate that $ab \neq ba \neq c$ after measurements.

On the meantime, Eve attempt to intercepts communication channel. By which get disturbed polarized vectors, on such condition an Eve captured superposed $|xy\rangle$ states where $x \in \{0,1\}^2, y \in \{0,1\}^2$ means superposition of 2^2 as 4 states.

Next, c states gets determine by a Bob. This happened on condition of Eve intercepted on a communication channel. Hence $c' = \varphi.c$ states receive at Bob end where φ represent as Eve operational effect on c. Hence measurement effect by Eve and Bob is $c' \not\approx c$. So, it become as $c' = \delta.c$, where δ represent vectors errors rate between Eve and Bob, obviously $\delta > 50\%$ at Eve end comparative of Alice or Bob vector measurement. If it is not as such way then discard communication and start again after a while. As such fashion Alice and Bob perform measurement operation at their respective end. In fact, through this we know a presence of Eve δ, on the basis of δ value Alice and Bob take further appropriate action.

2.2 B92 Protocol

It was proposed by Charles H. Bennett in 1992. The B92 protocol used 2 basis vectors for communication while BB84 used 4 basis vectors for communication from A(lice) to B(ob). Next, B92 protocol used two basis vectors $|0\rangle$ and $|1\rangle$ while BB84 protocol used basis vectors $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$. Basis vector $|0\rangle$ transferred from *A* to *B* without any superposition whereas $|0\rangle$ basis vector transferred in superposition states.

That is, Alice vector represents as

$$|\Psi_{x_1}\rangle = |\uparrow\rangle, \text{if } x \in \{0\} \quad (10)$$

$$|\Psi_{x_2}\rangle = \frac{(|\uparrow\rangle \pm |\downarrow\rangle)}{\sqrt{2}}, \text{if } x \in \{1\} \tag{11}$$

Eq. (10) and (11) are measurement effect at Bob ends

$$|\Psi_{y_1}\rangle = |\uparrow\rangle, \text{if } y \in \{0\} \tag{12}$$

$$|\Psi_{y_2}\rangle = |\uparrow\rangle \pm |\downarrow\rangle, \text{if } y \in \{1\} \tag{13}$$

Resultant of eq. (10) and (12) are

$$|\Psi_{x_1}\rangle \cong |\Psi_{y_1}\rangle \tag{14}$$

$$|\Psi_{x_2}\rangle \ncong |\Psi_{y_2}\rangle \tag{15}$$

Eq. (15) as in superposition state hence basis state may be either $|0\rangle$ or $|1\rangle$. Next, on x_2 and y_2 carried out measurement publically and compare between *A* and *B* with a presence of Eve. After *A* to *B* communication successive measurement being performed by *B* and *A*

$$|\Psi_{x_2}\rangle = \alpha|\Psi_{y_2}\rangle, |\Psi_{y_2}\rangle \text{ become a superposition state at a } B \tag{16}$$

An arbitrarily amplitude at Bob end is α. An error rate of $|0\rangle$ state at Bob after measurement probable value would be δ_1 whereas measurement of superposed vector $|1\rangle$ at Bob assume δ_2. Apparently, $\delta_1 \lll \delta_2$ at Bob side and this probability may be at Eve side also. The probability of error distribution might be $30\% \leq \delta_2 \leq 100\%$ if $\delta_2 \geq 50\%$ then discarding further communication since an eavesdropper presence visible in a classical communication channel. Discarding further communication resume after a while. At last, variation of δ_2 at Bob and Eve are the base of B92 cryptography secure communication.

2.3 E91 (EPR or Eckert) Protocol

It was used particle entanglement as pair or *n* number of particles. Alice and Bob share *n* number of particles[1]

$$\frac{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle}{\sqrt{2}} \tag{17}$$

Eq. (17) known as EPR pair of qubits applies on Bell's states

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(\uparrow_A\downarrow_B - \downarrow_A\uparrow_B) \tag{18}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(\uparrow_A\downarrow_B + \downarrow_A\uparrow_B) \tag{19}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(\uparrow_A\downarrow_B - \downarrow_A\uparrow_B) \tag{20}$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(\uparrow_A\downarrow_B + \downarrow_A\uparrow_B) \tag{21}$$

The Bell's different entangled states $|\psi^-\rangle$, $|\psi^-\rangle$, $|\phi^-\rangle$ and $|\phi^+\rangle$ used for testing photons entanglement between Alice and Bob. Hence, measurement of bases states is based on the Bell's states.

Suppose Alice generate number of qubits entangled pairs

$$|\Psi\rangle = |\Psi_1\rangle|\Psi_2\rangle|\Psi_3\rangle \ldots |\Psi_n\rangle \tag{22}$$

Where

$$n \in I^+ \text{ and } |\Psi_n\rangle = \frac{|\uparrow_{A_n}\rangle \otimes |\downarrow_{B_n}\rangle}{\sqrt{2}}$$

Let

$$|\Psi_A\rangle = \frac{|\uparrow_A\rangle \otimes |\downarrow_B\rangle}{\sqrt{2}} \tag{23}$$

Similarly Bob end state would be

$$|\Psi_B\rangle = \frac{|\uparrow_B\rangle \otimes |\downarrow_A\rangle}{\sqrt{2}} \tag{24}$$

Eq. (23) represents the entangled state at Alice end while eq. (24) represent at Bob end. Its measurement performed at the both ends

$$|\Psi_A\rangle = |\psi^-\rangle \otimes |\psi^-\rangle \otimes |\phi^-\rangle \otimes |\phi^+\rangle \tag{25}$$

$$|\Psi_B\rangle = |\psi^-\rangle \otimes |\psi^-\rangle \otimes |\phi^-\rangle \otimes |\phi^+\rangle \tag{26}$$

Probability of eq. (22) and (23) reverse such as Bob to Alice or Alice to Bob

$$|\Psi_B\rangle \rightleftharpoons |\Psi_B\rangle \tag{27}$$

Furthermore, eq. (22) and (23) qubits measurement performed by Bell's different states $|\psi^-\rangle$, $|\psi^-\rangle$, $|\phi^-\rangle$ and $|\phi^+\rangle$.

Hence eq. (22) and (23) might be represents

$$|\Psi_A\rangle = |\psi^-\rangle \otimes |\psi^-\rangle \otimes |\phi^-\rangle \otimes |\phi^+\rangle = 1 \tag{28}$$

$$|\Psi_B\rangle = |\psi^-\rangle \otimes |\psi^-\rangle \otimes |\phi^-\rangle \otimes |\phi^+\rangle = 1 \tag{29}$$

So it is an orthogonal normalization as *+45°* or *-45°* of particles such as $|+\rangle$ or $|-\rangle$ states of quantum communication. Also, probability distribution of each Bell's states would be

$$|\psi^-\rangle \otimes |\psi^-\rangle \otimes |\phi^-\rangle \otimes |\phi^+\rangle = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1 \tag{30}$$

Eq. (30) imposed on the $|\Psi_A\rangle$ and $|\Psi_B\rangle$,

Hence,

$$|\Psi_A\rangle = \alpha|\Psi_A\rangle \tag{31}$$

$$|\Psi_B\rangle = \beta|\Psi_B\rangle \tag{32}$$

Where α and β are arbitrary amplitude which entangled particle of Alice end as well as Bob end or vice versa. Eq. (31) and (32) become

$$|\Psi_A\rangle + |\Psi_B\rangle = \alpha|\Psi_A\rangle + \beta|\Psi_B\rangle \tag{33}$$

Further, Alice's and Bob's measurement performed on qubits publically as –

$$|\Psi_A\rangle = b_{A_0}.b_{A_1}.b_{A_2}\ldots b_{A_{n-1}} \tag{34}$$

$$|\Psi_B\rangle = b_{B_0}.b_{B_1}.b_{B_2}\ldots b_{B_{n-1}} \tag{35}$$

Where b_i represents binary bits and i represents an integer.
If

$$|\Psi_A\rangle = b_{A_0}.b_{A_1}.b_{A_2}\ldots b_{A_{n-1}} = |\uparrow_A\rangle \oplus |\downarrow_A\rangle \oplus \left(\frac{(\nearrow+\nwarrow)}{\sqrt{2}}\right) \oplus \left(\frac{(\rightarrow+\uparrow)}{\sqrt{2}}\right) \tag{36}$$

then its pattern accepted otherwise rejected. Similarly, for $|\Psi_B\rangle$ measurement performed for particles to the corresponding bit pattern. In eq. (36), entangled particle might be represented at a receiving end such as –

$$\left(\frac{(\rightarrow+\uparrow)}{\sqrt{2}}\right) = (\rightarrow\oplus\uparrow) \tag{37}$$

and

$$\left(\frac{(\nearrow+\nwarrow)}{\sqrt{2}}\right) = (\nearrow\oplus\nwarrow)$$

An eq. (36) intercepted by an Eve and those qubits measurement reveal at Bob or Alice end.

$$|\Psi_A\rangle = \int_0^n b_{A_n} db_A \tag{38}$$

$$|\Psi_B\rangle = \int_0^n b_{B_n} db_B \tag{39}$$

if

$$\delta = |\Psi_A\rangle \otimes |\Psi_B\rangle \geq 50\% \tag{40}$$

then qubits de-coherence occurred due to Eve interception. On resultantly further communication either from Alice or Bob through away and re-transmission of particles carried out after a while.

A full utilization of quantum system resources for EPR communication not susceptible if the quanta of qubits are whole string. It is fine for quantum system resources to deal with a chunk of communicable particles either Alice or Bob end. Due to qubits string partition, the presence of Eavesdropper easily reveals in an initial

communication. Since, particle measurement at the end, it would be space and time consumption of quantum system resources. An eq. (22) re-writes

$$|\Psi\rangle = [\{S_1\}\{S_2\}\{S_3\} \dots \{S_n\}, \phi] \tag{41}$$

$$[S] = [S_1, S_2, S_3, \dots, S_n] \tag{42}$$

Means

$$\begin{aligned} S_1 &= \{|\Psi_0, \Psi_1, \Psi_2, \dots, \Psi_i\rangle\} \\ S_2 &= \{|\Psi_{i+1}, \Psi_{i+2}, \Psi_{i+3}, \dots, \Psi_j\rangle\} \\ &\vdots \\ S_1 &= \{|\Psi_{j+1}, \Psi_{j+2}, \Psi_{j+3}, \dots, \Psi_n\rangle\} \end{aligned} \tag{43}$$

First of all randomly select quanta from *S*, such as subset S_i. Selected subset S_i sends either Alice or Bob. Determine error probability rate at both ends (i.e. Bell's entanglement of particle measurement); if error rate δ_i of particles subset S_i not acceptable then further transmission through away since Eve presence reveal in this quantum communication.

Lastly, EPR communication has the further refinement of BB84, B92 protocols in quantum cryptography.

3. Result and Analysis of Quantum Protocols

Above discussed three quantum protocols are suitable for open space quantum. BB84 protocol applied for quantum key exchange from Alice to Bob, first private key exchange after that measurement publically private key from one ends to another end or vice versa. Its principle based on four qubits for secure communication between Alice to Bob and vice versa in a presence of Eve. The main characteristics of BB84 protocol are

i. It use $x_1 \xrightarrow{q_1} x_2 \xrightarrow{c} x_3 \xrightarrow{q_2} x_4$ (where q_1 and q_2 represent open space quantum communication while c as classical channel). Here x_1 and x_2 act as source and destination respectively. An x_1 to x_2 represent classical channel used bit string p_1. An x_2 to x_3 encoded the p_1 string as qubits string sequence after that x_3 to x_4 used classical bits string one more.
ii. This sequence use x_2 to x_3 as open space quantum channel for qubits transfer. An x_2 to x_3 sequence work on the principle of an EPR.

Above mentioned two points, exhibit stronghold of quantum cryptography communication rather than classical computer communication. An operation of BB84 protocol, operational limitation speed down due to classical as well as quantum communication combination.

Second, B92 protocol used the nearly same principle of BB84, contrast is two qubits implication and polarization of particles is orthogonal.

Some more characteristic of above protocols which based on an entanglement are no-cloning, intercept-send strategy, error correction privacy amplification and quantum growing, quantum distillation etc.

Fig. 2 indicate, comparative analysis Quantum Bit Error (QBE) rate of BB84, B92, and E91 quantum protocols. This result based on above discussed three quantum protocols.

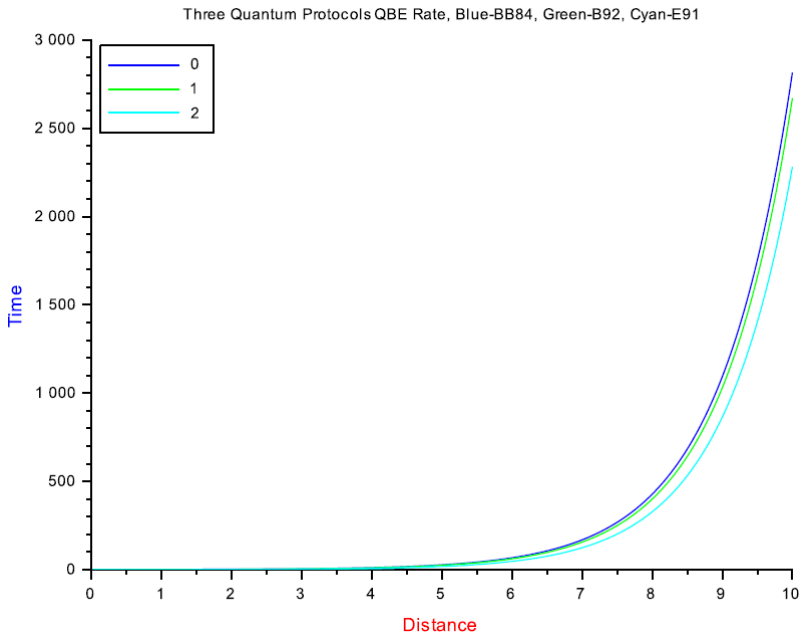

Fig.2. Comparative Analysis of Three Quantum Protocols QBE (Quantum Bit Error) Rate

4. Conclusion

BB84 quantum protocols experimentally tested for few km (kilometer). The testing done on ground based quantum communication channel. Its application quite more wide in near future for guided channel; whereas it is challenging for open space quantum communication due to quantum mechanics entanglement features. But, it is too early to say at this time. When we go back to the primary stage of quantum mechanics such as infancy stage of the 20^{th} century then quantum mechanics was just virtual realization, nothing more than that. Successively, quantum mechanics ripe into theory and its ripe juice tested by the world somewhat extent when Bell's inequality experiment stated that there were no local hidden variables that are based on quantum mechanics. Quantum mechanics notable characteristics are entanglement of states and superposition of states. By these, we see the future superior than deterministic or somewhat un-deterministic Turing machine.

Acknowledgement

Authors acknowledge DG & DY DG of Raksha Shakti University, Ahmedabad for allowing this research work at the aegis of Institute of R&D, Raksha Shakti University, Ahmedabad & we are grateful for their support and guidance.

References

[1] C. H. Bennett, G. Brassard: Quantum cryptography: Public key distribution and coin tossing. In Proceeding of IEEE International Conference on Computers, Systems, and Signal Processing, volume 175, page 60-111, New York, 1984.

[2] Ekert. A, Phys. Rev. Lett. 67, pp. 661-663 (1991).

[3] Chaung I., Nielson M.:Quantum Computation Information. 2000.

[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels. Phys. Rev. Lett. 70, pp. 1895–1899, 1993.

[5] Einstein A., B. Podolsky, N. Rosen: Can Quantum-Mechanical Description of Physical Reality be Considered Complete? Physical Review 47 (10), pp. 777–780, 1935.

[6] Bennett C., Wiesner S.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters **69** (20), 1992.

[7] Noson S. Yanofsky, Mirco A. Mannucci: Quantum Computing for Computer Scientists. Cambridge University Press, 2008.

[8] Brassard Gilles, Claude Crépeau, Jozsa Richard, Langlois Denis: A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties. IEEE, pp.362–371, 1993.

[9] Branciard Cyril, Gisin Nicolas, Kraus Barbara, Scarani Valerio: Security of two quantum cryptography protocols using the same four qubit states. Physical Review A **72** (3), 2005.

[10] Gerhardt I. et al.: Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Communications, 2011.

[11] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin: Experimental Quantum Cryptography. Journal of Cryptology vol.5, no.1, pp. 3-28, 1992.

[12] Z. Zhang, J. Liu, D. Wang, S. Shi: Quantum direct communication with authentication. Phys. Rev. A 75, 026301, 2007.

[13] G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders: Limitations on practical quantum cryptography. Physical Review Letters, 85(6):1330+, 2000.

[14] Meyer, D. A. Quantum strategies, Phys. Rev. Lett., 1999; 82(5):1052.

[15] Younis A. Shah, Irshad.A. Mir, Uzair M. Rathea, "Quantum Mechanics Analysis: Modeling and Simulation of some simple systems", International Journal of Mathematical Sciences and Computing (IJMSC), Vol.2, No.1, pp.23-40, 2016.DOI: 10.5815/ijmsc.2016.01.03.

Authors' Profiles

Shyam R. Sihare is the Ph. D. candidate in Raksha Shakti University, Ahmedabad, India. He took up his Master's degree in Computer Science at Nagpur University, Nagpur, India in 2003 and obtained M. Phil. in Computer Science at Madurai Kamraj University, Madurai, India. He cleared Professor Eligibility Test GSLET, Gujarat, India in 2011. He obtained MCA at IGNOU, New Delhi, India in 2011.

He is currently working as Asstt. Professor in Computer Science and Application in Dr. APJ Abdul Kalam Govt. College, Silvassa, Dadra & Nagar Haveli(UT), India. His research interests include Quantum Computer, Quantum Algorithms, Quantum Cryptography, and Classical Computer Algorithms.

Dr. V V Nath, earned his Doctor of Philosophy at North Gujarat University, Patan, Gujarat, India in 2012.

He currently works as a professor at the Nirma Institute of Management, Nirma University, Ahmedabad, India. He has 27 years experience in Industry before joining the Institute in June, 2003.His Industry experience spans across various Industry segments like Electronic, Pharmaceutical, Glass Manufacturing, Steel Manufacturing etc. He has been heading Information Technology Department at various Companies in his career with Industry. His Research interest includes Enterprise Systems and Information Security.

How to cite this paper: Shyam Sihare, V V Nath,"Revisited Quantum Protocols", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.3, No.2, pp. 11-21, 2017.DOI: 10.5815/ijmsc.2017.02.02