Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Emergence of Horizons in the Field of Quantum Technology

Rani Danavath
Research Scholar
Dept. of CSE
Osmania University
Hyderabad, India

Dr. V. B. Narsimha
Asst, Professor
Dept. of CSE
University College of Engineering
Hyderabad, India

K. Prem Chander
Lecturer in Computers
Dept. of Computers
S.R.R.Govt.Arts & Science College
Karimnagar, India

Abstract: ***As per the Survey "internet world stats" by Minimarts marketing group published 2012, it has given that The total number of Internet Users worldwide are as follows: Asia-44.8% of the World, Europe 21.5%, North America 11.4%, Latin America and Carob 10.4%, Africa 7.0%, Middle East 3.7% and Australia 1.0%. And in the total number of email users as per the radiate group, Inc. A technology market research firm (Email Statistics Report, 2013-2017). The basic reason why this operations are done because of a belief that "No 3rd party may be able to look in to the contents and the Information remains secured as we all trust. This confidential Information is many times is made several attempted by several hackers and a considerable number of times they could succeed around the world. But it should be noted this scenario is with present available Technology. As The Time floats Technology grows with in a Geometric Progression. Then the Information in this present Technology may not be suitable. As a guess says nearby future of 2020 Hardware implementations of present day technology may achieve by a computer microprocessor Chip may be able to get a resize of reduction 1.10 nano meters. The Information generally converted into Cryptographic form such as the agencies could not be able to guess, and uses RSA Algorithm which uses CRAM (Challenge-Response Mechanism) of Largest Factorization, and implements on Neumannic Computers. Cryptography is not new to us one who has competent information about the windows and Ms Office packages probably know that they can encrypt any information in to unknown to the viewer. To do so…Ms Office Button → Prepare →Encrypt the Document →Enter the Password →Re-enter the Password → Press "OK" .When we want to open enter the password Challenges to our Information. The challenges could be arise if any Powerful Govt. in the World is attached a Super Computer to this field of guessing probably we are soup. If a Quantum Computer is attached to the internet probably we may not be in a safe zone. If any Govt. Sponsored Terrorists of any country make any one of the above (or) attaches a Quantum Computer probably we may have troubles and Confidentiality is in distrust.***

Key words: nano meter, CRAM (Challenge-Response Mechanism), Quantum Cryptography, hybrid technology, light weight Technology, Quantum Key Distribution (QKD), Hilbert Space.

I. INTRODUCTION

Quantum Cryptography is not possible to 'Crypt-analyze' and crack the information in any circumstances even by the Quantum Computer; in a situation we are going to use Quantum computers in coming to the near future. Coming to the point of Quantum Cryptography, in current days it is highly expensive and cannot be affordable. Then we have two options…One… is searching a way to make this cryptography cheaper and the second...Is using a hybrid technology which uses present day algorithms and computers and which makes no-effect in a situation they are replaced by the Quantum Computers (it is permitted by Quantum Cryptography to do so). Both sounds well but the Trials has to be made. At the First … Let us look in to the Quantum Cryptography which implements the technology…It is actually a Protocol Technology which creates a Key, it distributes the Key and Implements the Key over the Internet (it is possible also in Intranet). In the Second It is a light weight Technology possible to implement any where including in Mobiles, Tabs and laptops, Desktop systems and any other portable and non-portable systems. The Technology is safer because they establish a separate and secured Channel for the information to travel. This way of following of a method is called as Quantum Key Distribution (or) simply QKD. History of this Quantum Cryptography tells us that it is not a mathematical based cryptography but it is a real time cryptal application of Quantum Physics which is the Ultimate Technology that the science could achieve by the Human Mind as since turning the sparks of Human intelligence in to a gigantic flame, as we all know that invention of fire is the 1st step of beginning of the Human Intelligence.

For this dream of Quantum Cryptography case the Inventor must become a Philosopher rather than becoming a Mathematics and Computer Scientist. It is invented by Charles Floyd Bennett, Gilles plate armour and John Smolin in 1989.As explained earlier This system will have to travel…as like that of the other Cryptographic Systems, Creating of a Key , Key Distribution over the internet, And the Key Maintenance. We have two systems... One is as "Bennet and armour plate Protocol" and the other is "Eckert Protocol". We call to days our computers and protocols as digital as there is a possibility of only '1' and '0' which we call them as binary state digits. But here Quantum Cryptography takes the qualities from that of the Quantum Mechanics as like the '1', '0' and '1 and 0 both quantities at a time', this is a

probabilistic mechanism as we all know which mesmerizes the tracker (or) hacker. This Ternary number system is called as Quantum bit (or) Qubit.

II. PROBLEMS WITH QUANTUM CRYPTOGRAPHY

But the problem with this system is its Length capability one hundred fifty Km (Approx.93 Miles) are due to interference. And it uses' photons (particle of light') as to transmit a key. All angles of photon's spin represents one piece of data sometimes a one or a zero, for code.

Generally this undergoes such as…

1. Sender sends the encrypted key within the style of entangled polarized photons
2. Recipients receives the photons and measures the key worth by measurement the polarization
3. Recipient sends back the measured key worth id set the polarization values
4. Sender sends the premise on that every gauge boson was polarized in
5. Recipient sends the premise on that every photon's polarization was measured in
6. Sender compares the values of solely those photons that each the sender and receiver used a similar basis to form and live the polarization. Any discrepancy in these values suggests that there's a potential overhang dropping by a 3rd party and therein case the group action is aborted and is started anew.

III. MERITS OF QUANTUM CRYPTOGRAPHY

Quantum Key Distribution (Q.K.D.) generates a Secured One-Time Pad this is also called as Vernam Cipher. It uses NO CLONING Principle... This States "an eavesdropper if intercepts and tries to measure the Qubit eventually it modifies the content. Hence it can be detected". This Principle is also called as Avalanche Effect .Quantum Key Distribution uses Shores algorithm rather than that of the RSA algorithm as we use now. Fourier transforms are widely used in taking the input and other related aspects.

IV. KEY GENERATING ALGORITHM

Step: 1: choose any 2 Prime Numbers 'p', 'q' like p=q
Step: 2: Calculate n=p*q
Step: 3: Calculate Ø (n) = (p-1) (q-1)
Step: 4: choose Associate in whole number e wherever GCD (Ø (n), e) =1 like 1<e
Step: 5: Calculate d wherever d=e 1mod Ø (n)
Step: 6: Public key KU= {e, n}
personal Key KR= {d, n}

4.1 Factoring:

Resolution may be a terribly tough task for classical computers. It takes 240,000 pc hours to issue 174 digit numbers. All Secure web transitions are supported the idea that this downside is more durable to try and do thus. The most effective classical algorithmic rule takes time: o (exp (n 1/3)) Shore's Quantum algorithmic rule takes time o (n2 log n).This Shore's algorithmic rule is Associate in economical algorithmic rule for resolution that breaks the RSA public Key Cryptography.

4.2 Qubit Generation:

it's born-again into the hexa decimal code then into the binary decimal numbers, finds least little bit of 2 binary values and obtain the Quantum bit of 0's and 1's.

4.3. Quantum Key Generation:

Use Qubit and therefore the session key to get a quantum key. If the Qubit combination is …
If zero and zero then 1/0.707 (p [0] +p [1])
one and zero then 1/0.707 (p [0] +p [1])
zero and one then p [0]
one and one then p [I]

V. KEY DISTRIBUTION

The distribution original session key and Qubit to the sender for cryptography and conjointly distributes the Qubit and therefore the session key on receiver facet for the coding.

5.1. Working Mechanism:

Server In between Client (1). Produce a pulse light-weight and send it to Server victimization the fiber
(2). Server receives the weak pulse and sends it through electrical device that outputs the one gauge boson (3). Currently the Server sets the polarization of photons and sends it back to the server via fiber (4). Server and therefore the server compare their live employing a typical link. This permits them to extract the key & purity of the link .

5.2 Practical issues in Implementation:

During a wave length vary of 600-800nm single photons are accessible, and therefore the noise rate is 50Hz to

25Hz once cooled. In optical fibers zero.3dB/km accessible in semiconducting material & Indium-gallium compound (InGats) APAs, that detects the one photons regarding 100khz.The propagation distance, is in one kilometer solely QKD key generates is slower than optical device vital sign is 100 percent solely. The ninetieth of the optical device pulse contains no photons.

QKD is in economical of identification of 1 shared bit for four initial bits. however even helpful distance is restricted not most by the key rate as by the Bit error rate(BER) that should be but some threshold so as that attended may be detected. Error rate is interferometric visibility. Attributable to the amount of Photons inbound decreases with increasing distances noise contribution to BER will increase with distance.

In Associate in approach to change Shor-Preskill vogue unconditional security proof of QKDs. In Shor-Preskill's proof, the target QKD, BB84, is reworked into Associate in other QKD supported a trap distillation protocol (EDP), that is additional possible for direct analysis. We tend to formalized heir methodology as program transformation during a quantum artificial language, QPL. The rework is outlined as revising rules that are sound with relation to the protection within the linguistics of QPL. We tend to evidenced that revising continually terminates for any program which the traditional type is exclusive underneath applicable conditions. By applying the revising rules to the program representing BB84, we are able to get the corresponding EDP-based protocol mechanically. We tend to finally evidence the protection of the obtained EDP-based protocol formally within the quantum Hoare logic that may be a system for formal verification of quantum programs. We tend to show conjointly that this methodology may be applied to B92 by an easy modification.

Once creating a radical analysis to means to send the information during a secured way of causing mechanism, approaching to a Quantum Cryptography, has lead USA to form several style of applications are to be looked in. in reference of BB84 is being fail because the alignment of the Server and server was allowed to drift over time, arrangement freelance Quantum Key Distribution, could be ready to speedily endure noise by choice introduced to the communication link at a debilitating level.

One such try is created that creating an S/W development that gives the Key-Generation and Distribution makes us simple to realize our necessities.

VI. EQUIPMENT SOPHISTICATION

In Present situation we are available with the Latest Technological Equipments such as Multiple Transmitter-Receiver Multiplexing Analysis: for sending and receiving the data Data Recording De-multiplexing Constraints: for data recording High Pulse-Repetition-Frequency Lasers: for Photon calculations Synchronization Constraints: for data synchronization

VII. RECENT DEVELOPMENTS IN THIS FIELD

Development: 1 Nokia Mobile Company and the University of Bristol (UK) developed quantum cryptography for the use of a mobile phone. This promises a complete secrecy for the mobile users. In this Cryptography...QKD will use an easy, strong, cheaper chip that can be embedded with user's mobile. Nokia's New QKD uses a variant of QKD called referenced frames of independent QKD, (rfiQKD); this technology is development is done by Laing and several others of his colleagues. This saves from a problem of one strong control with conventional QKD methods: that they only work if Alice and Bob measure the properties of photon qubits – such as phase or polarization – relative to a fixed reference frame. The advantage of rfiQKD is that it allows for some twisting and turning – even if this relative motion is unknown. The technique works by having Alice and Bob each compute a specific combination of observables whereby the effect of the twisting angle cancels itself out. According to Laing, this "angle independent" value can be thought of as the purity of the quantum state exchanged by Sender and the Receiver. In a case this comes below a value, this people are warned about the Eves dropper's un-authorized looking in to the content. Jeremy Edna O'Brien, director of the CQP, believes that the system may ultimately create it attainable to use quantum cryptography to shield the growing quantity of non-public data, like passwords, that's transmitted victimization mobile phones. Cash machine machines, as an example, may well be started as rfiQKD servers and a user may merely purpose their phone at an optical system to receive a quantum key. Within the new system, Alice is represented as a server as a result of she sits in an exceedingly fastened location and performs all the fragile measurements needed for the rfiQKD. Bob is represented as a shopper as a result of he performs easy and strong actions that may be achieved employing a moveable device. First, the server creates a really weak pulse of sunshine that's sent to the shopper victimization AN fiber. The shopper takes the weak pulse and passes it through an electrical device, which outputs one gauge boson. The shopper then sets the polarization of the gauge boson and sends it back to the server via the fiber. The server then measures the polarization of the gauge boson. Then, the shopper and server compare their measurements employing a standard link that permits them to extract each the cryptography key and also the purity of the link. The team conjointly enforced a well known standard QKD protocol known as BB84 on its system. Whereas BB84 began to fail because the alignment of the shopper and server was allowed to drift over time, rfiQKD delayed. The team conjointly found that rfiQKD was able to chop-chop endure noise advisedly introduced to the communication link at a weakening level, whereas BB84 continued to fail.

Development: 2 GOOGLE & QCOMPUTER

Google Purchased a Quantum pc and in association with independent agency forming a Quantum computer science laboratory that focuses on Machine Learning that focus additionally on like facial or voice recognition, biological behavior, or the management of terribly massive and complicated systems. the foremost effective ways for victimization

quantum computation, Google aforementioned, concerned combining the advanced machines with its clouds of ancient computers.

D-wave an Yankee company that sold-out the Quantum pc to Google freelance man of science found that for a few forms of issues the quantum pc was three,600 times quicker than ancient supercomputers, it was 11,000 times quicker, however within the tougher fifty p.c, it was 33,000 times quicker. Within the prime twenty five p.c, it was 50,000 times quicker." interactions of 512 quantum bits, or qubits, to work out improvement.

Development: 3TOSHIBA & RE-SEARCH PAPER**:**

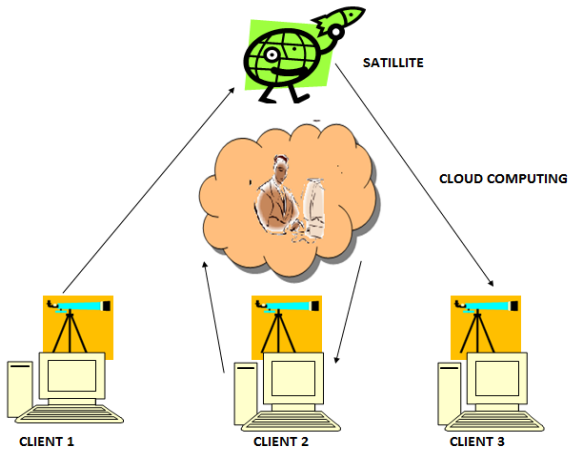
Toshiba Scientists created re-search paper in Nature Journal, explained "how to expand a point-to-point quantum network with solely 2 users into a "quantum access network" with up to sixty four users" the outline as follows...A quantum network uses specially polarized photons to encipher associate degree encoding key—a terribly long series of numbers and letters which will unlock a digital file. The photons are then sent down a fiber optic cable till they reach their destination, a gauge boson detector that counts them, and delivers the key to the supposed recipient. If the photons are interfered with, the individual packets of knowledge are forever altered and also the recipient will see the telltale signs of change of state. The Toshiba team targeted its efforts on up the gauge boson detector, and created a system that counts up to one billion photons per second, that makes it possible to feature additional folks to the network. They need developed associate degree design that's point-to-multipoint. This will increase the quantity of potential users within the network, and reduces prices. It prices aprox.30 Lakhs for sixty four users.

Development 4: Canadian team needs to require a budget

Microsatellite route to untraceable world communications

Development 5: United States intelligence agency seeks to make quantum pc that might crack most styles of encoding.

Proposed System Architecture:



Three Binoculars with formation and pointed towards satellite, that is capable of bouncing a beam pulse, on reaching the planet with one gauge boson. This single gauge boson can reach a QUANTUM CLOUD station that is connected to a number of the 'n' shoppers to its QUANTUM SERVER. Quantum wells area unit in wide use in diode lasers.... we will use Quantum Tunnels for the signals to create it transmit. Typically infra-red lasers in fiber optic transmitter's area unit exploitation currently this property.

They're conjointly accustomed create HEMTs (High lepton quality Transistors), that area unit utilized in low-noise natural philosophy. Quantum well infrared exposure detectors are supported quantum wells, and area unit used for infrared imaging. Quantum wells area unit fashioned in semiconductors by having a fabric, like metallic element compound sandwiched between 2 layers of a fabric with a wider band gap, like Al compound. (Other example: layer of atomic number 49 metallic element chemical compound sandwiched between 2 layers of metallic element chemical compound.) These structures will be full-grown by molecular beam epitaxial or chemical vapor deposition with management of the layer thickness right down to monolayer. Skinny metal films may support quantum well states, specifically, aluminiferous skinny over layers full-grown in metal and semiconductor surfaces. The lepton (or hole) is confined by the vacuum-metal interface in one aspect, and generally, by associate degree absolute gap with semiconductor substrates, or by a projected band gap with metal substrates.

VIII. CONCLUSION

Usage of Binoculars and a Satellite and with the assistance of optical device pulses will create our signal to achieve the Quantum Cloud Center, from here we will hook up with many alternative purchasers and at a less expensive rate we will offer it to the user. HEMTs of Quantum Wells will create our signals to possess noise less media to permeate the signal.

REFERENCES

[1] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M.Fejer, K. Inoue, and Y. Yamamoto, New J. Phys. 7, 232 (2005).

[2] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. 4, 41.1 (2002).

[3] C. Gobby, Z. L. Yuan, and A. J. Shields, Electron. Lett. 40, 1603 (2004).
[4] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature 419, 450 (2002).
[5] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. R.
[6] V. Y. Bazhenov, M. V. Vasnetsov, and M. S. Soskin, JETP Lett. 52, 429 (1990).
[7] A. Vaziri, G. Weihs, and A. Zeilinger, J. Opt. B: Quantum Semiclass. Opt. 4, S47 (2002).
[8] G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett, and S. Franke-Arnold, Optics Express 12, 5448 (2004).
[9] R. T. Thew, A. Ac´in, H. Zbinden, and N. Gisin, Phys. Rev. Lett. 93, 010503 (2004).
[10] M. Curty, L. L. X. Zhang, H.-K. Lo, and N. LÄutkenhaus, \Sequential at- tacks against di®erential-phase-shift quantum key distribution with weak coherent states," Quant. Info. Compu. 7, 665 { 688 (2007).
[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du·sek, N. LÄutkenhaus, and M. Peev, \A Framework for Practical Quantum Cryptography," arXiv:0802.4155 (2008).
[12] C. Gobby, Z. L. Yuan, and A. J. Shields, \Unconditionally secure quantum key distribution over 50km of standard telecom ¯bre," Electron. Lett. 40, 1603 (2004).
[13] W. Y. Hwang, \Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. 91, 057 901 (2003).
[14] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, \Practical Decoy State for Quantum Key Distribution," Phys. Rev. A 72, 012 326 (2005).
[15] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, \Experimental Quantum Key Distribution with Decoy States," Phys. Rev. Lett. 96, 070 502 (2006).
[16] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, \Unconditionally secure one-way quantum key distribution using decoy pulses," Appl. Phys. Lett. 90, 011 118 (2007).
[17] D. Mayers, \Unconditional security in quantum cryptography," J. of ACM 4

