An Efficient Implementation of Quantum Cryptography using a Hierarchical Structured Architecture

B. Sujatha
Asst.Prof Engineering College
Dept. of Computer Science
Osmania University
Hyderabad

S. Nagaprasad
Lecturer in Computers
Dept. of Computer Science
S.R.R.Govt. Degree College
Karimnagar

G. Srinivasa Rao
Sr. Faculty of Computer Science
Dept. of Computer Science
Key Soft Computer Eductaion
Hyderabad

ABSTRACT
The chief aim of information security is to protect an organization's precious resources, for instance information related to emails, passwords, ATM cards and Credit cards etc., Quantum key distribution (QKD) offers an unconditionally secured means of communication based on the laws of Quantum Mechanics. Let us look into the available information from our some of our scientists from their Reports that QKD experiments in which secured keys could be distributed over 42 dB channel loss and 200 km of optical fiber Cable Networks. Superconducting Single Photon Detectors Provides us a relatively Less dark count rate in a less Frequency and tiny Timing Jitter with 60 peco seconds full width at half maximum. Currently, a major challenge is to obtain a QKD system with a 40 dB channel loss, using World wide QKD Networks with the Help of Satellite Communications. This Property makes us to construct a 10-GHz clock QKD system and therefore distribute the Secured Keys on the channel loss of 42 dB. 'Qubits' are Quantum Bits which are the Binary Information digits in Ternary; they are safe and un-predictable data representation. Keys created in experiment are secured for General Collective Attacks (GCA), and a Specific Collective Attack (SCA) on single and multiple-photons. This protocol is Executed with 10-GHz clock frequency, and Superconducting Single Photon Detectors (SSPD) With the Support of 'NbN Nano-wire. This communication Hierarchical element adds the sender and the receiver in Quantum Cryptography. Therefore we are supposed to make a new algorithm for Throughput Optimization (TPO) in a Quantum Cryptography. Apart of this we they also obtained a 17 Kbit/s Secure Key Rate (SKR) over 105 km of Optical Fiber Cable, and also 12.1 bit/s Secure Key Rate (SKR) over 200 km of Optical Fiber Cable. Therefore we are required to create a new procedure to increase Throughput in Quantum Computers. These are the Key Elements of Quantum Cryptography in coming Quantum Computers. This Approximate Solution Algorithm (ASA) gives us a major reduction in computation time in contrast to available methods. They use the Quantum Key Distribution with Differential Phase Shift (DPS-QKD). This also provides reasonable size and large size of Computer related problems to solve. We need to obtain the fixed regular Qubits with the Help of "Approximate Solution". A Collection of Qubits could be effectively assigned to Hierarchical Structure at any throughput level. This is the longest World Wide QKD that can be established.

Keywords
QC (Quantum Cryptography), Quantum key distribution (QKD),Quantum Key Distribution with Differential Phase Shift (DPS-QKD),Superconducting Single Photon Detectors (SSPD),General Collective Attacks (GCA),Specific Collective Attack (SCA),Throughput Optimization (TPO),Approximate Solution Algorithm (ASA), Protocols Layered System(PLS),Application-Specific Networking Methods (ASNM),Transport Layer (TL),Transit Networks (TN),Link Layer (LL),Local Network Link(LNL),Internet Protocol (IP),Routing Tables (RT),Border Gateway Protocol (BGP),Quantum Cryptographic hierarchical structure(QCHS).

1. INTRODUCTION:
In the Internet…When we enter the data, it is analyzed through a 'Protocol Stack (PS)'; all new layers append a 'sum up (encapsulation)' at the time sending to the server.At the middle level, relays will remove and add a new link encapsulation for retransmission, and check the IP Layer for Routing purposes.Internet communications system will have Hardware devices and software Layers to administer different architectural parts. The will be Data is sending in the link level, from left to right.IT IS A CONTINUES PROCESS SUCH AS SECURITY UP GRADATION EXAMINATION CHECKING IN A WAY TO ACHIEVE STATE-OF-ART-TECHNOLOGY.When the server receives it reverses the obtained 'encapsulation stack'.

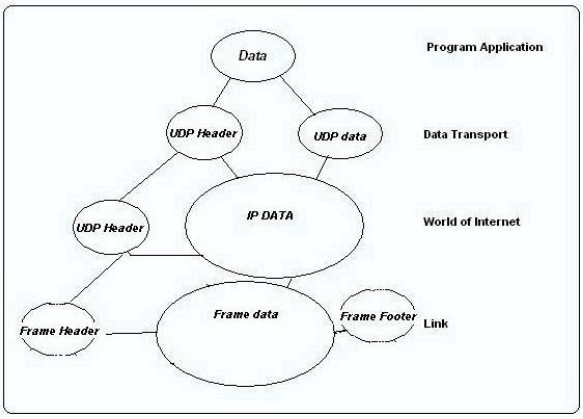

Fig.1 Data in the Internet

Finally, in the last level of the design the Link Layer (LL), permits us to connect in between the servers using the Local Network Link(LNL).We call them as TCP/IP Protocol, it's architecture is does not co-inside with the Hardware. The internet layer permits our computers to 'recognize' and 'find the Location' of every Computer using the 'IPAddresses', and permits those computers to attach one computer with the other computer using the Transit Networks (TN). Under it, there could be a Transport Layer (TL).This Transport Layer attaches the Software Applications over many types of servers using the network with the suitable data exchange Procedures. The Internet standards makes it clear that to follow Internet protocol suite Framework(IPSFW).It is an design to follow and gives us to follow into a Protocols Layered System(PLS).They are RFC 1122, RFC 1123. 1) The Important Procedures of networking is

… it permits the Internet to use Request for Comments (RFC) s that include the Internet Standards.The important element of the Internet architecture is the Internet Protocol (IP) that permits us to use IP Addresses.IP Addresses allows internet-Networking .IP Version is architected to address up to 109 Internet servers at a time.In the software applications, on above the application layer, we place the Application-Specific Networking Methods (ASNM).2) Here the layers will communicate to the Services Operational Environment (SOE).3) These two layers are the fundamental Networking Technologies.

2. ROUTING:

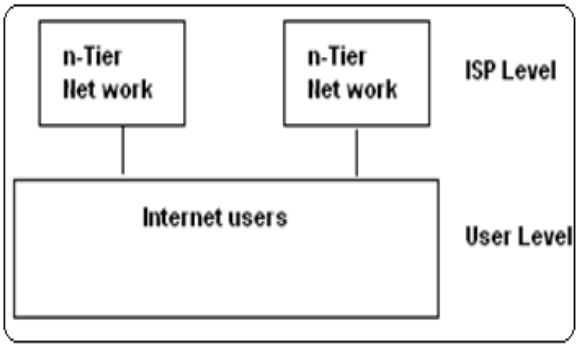

Fig.2 Routing in the Internet

End-nodes use a default route which targets at an ISP showing its way, at the same time ISP routers utilize the Border Gateway Protocol (BGP) to create the significant routing surrounding the typical Physical and Hierarchical Internet connections. In the 2nd level of routing hierarchy, some networks purchase Internet passage.ISP could use a unique upstream provider to connect. These ISPs are attached to the users, which are at the lower level of the routing hierarchy; in the 1st level of routing hierarchy many Telecommunications swap their internet passage. Packet Routing (PR) in Internet is done in n-tier of Internet Service Provider (ISP) s. Computer Systems and Routers will use Routing Tables (RT) to point towards IP packets to the next-leap router…. Internet exchange points are significant traffic exchanges with connections to many ISPs connected. This also suggests the Qubits Optimization problem formulation and that will tells us The Regular Qubits and approximation Algorithm. These Regular Qubits will attain a level of Throughput. Let the fixed regular Qubits, with an objective to provide 'permanent communication support for the regular Qubits. Routing tables are administered with the help of Routing Protocols by the Individuals. Hierarchical structure of this Network may be supporting for a betterment of the Quantum Cryptographic Architecture. Data taken from this are sent over the area either in free space/Fiber Optical Cables. Repeater Stations can cover big area. And to the next leap finally towards the targeted Place.

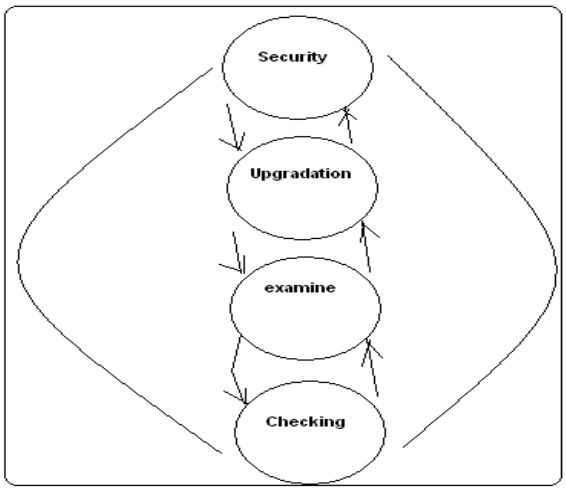

Fig.3 Security of the Data which we need to do

3. FRAMING THE PROBLEM:

The Problem is" many senders and receivers are connected in a hierarchical structure with fixed communication ranges are deployed to provide communication support for a set of fixed regular Qubits." Our requirement is to have the minimum number of Quantum Cryptographic hierarchical structure(QCHS) Qubits so that each regular Qubit is connected by at least one QCHS Qubits ,And where all the senders and receivers in Quantum Computers who are connected to each other. Let us think that the throughput (data rate) that can be obtained between a regular Qubit and a QCHS Qubits is a uniquely non-increasing function of both the distance between the two Qubits and the number of other regular Qubits that are also communicating with a particular QCHS Qubits. Therefore it will takes a separate way to construct a communication architecture, where two Qubits could communicate when they are within the communication range elsewhere they cannot do so. There could be two types of Qubits when the Quantum Computers are connected to the internet. At the same time our outcomes will be valid for every throughput function which is uniquely non-increasing. Generally we are using the multi-layer hierarchical Network architecture in the Internet. This communication makes interference.

This will be a noteworthy to identify a particular example.Let us denote throughput 'τ' In between i, j which are Qubit and **QCHS Qubit**

Then it could be such as …

$(A_j,d_{ij})=1/|A_j|(1-1/|A_j|)(1/|A_j|-1)(1/d_{ij}^{\alpha})$

→Equation (1) In this here we are with…

$|A_j|$-Number of regular nodes assigned to Quantum Cryptographic hierarchical structure Qubits j,

d_{ij} - Distance between regular Qubit i and QCHS Qubit j, and α is the path loss exponent. Then the through put could be then….

$$\tau \quad (A_j,d_{ij}) \sim 1/e.\ |A_j|.d_{ij}^{\alpha} \rightarrow \textit{Equation (2)}$$

As we make this Architecture, we will get QCHS Qubits optimization problem "When A set of N regular Qubits are distributed in a plane, we need to re-arrange into K QCHS Qubits, in a random locations, at the same time assigning the regular Qubits to the hierarchy design, then so the network capacity could be increased.

Once the QCHQ Qubits have been placed in their selected locations, regular Qubits have a finite amount of data available to

send, and QCHQ Qubits must move around the network and collect data.

Our Aim is to increase the number of regular Qubits which can obtain the throughput at least min where each regular Qubit can be attached to a single sender (or) receiver.

We limit our self thinking that regular Qubits assigned to one sender (or) receiver does not come across any interference from regular Qubits assigned to other sender (or) receiver.
Let us consider QCHQ Qubit placement and regular Qubit assignment, they can be placed anywhere in the plane, then the Question of Identifying an optimal placement is, list of all KN possible assignments is not possible, and random assignment cannot be done.

In way the capacity is calculated with the help of number of regular Qubits that achieve throughput at least min.
It lets us the regular Qubits positions are known, with the satellite connection establishment.

Hence our hypothesis permits us to accommodate a satellite uplink for regular Qubits.

We will make the network optimization at the same time of placement and assignment.

To do so we will keep one sender(or)receiver in one "Block" with a different Frequency that should not match with the other, and no need to connect each other.

Then the efficiency of the network is increased.

This is an instantly created Network.

$$\max F_{\tau} \ (R,M,A, \tau_{min})$$

M,A

Where M_i belongs to R^2 ,i=1…..K and A belongs to A where Regular Qubits are stationary. Let R_i be The Regular Qubits Locations, i = 1…N, and τ_{min} is the Minimum Throughput Level, Let τ is a Throughput Function, and M_i is Decision Variables in the selected locations of the QCHQ Qubits ranging from i=1……up to K, and A be the assignment of regular Qubits to QCHQ Qubits……From the above A is the set of valid assignments $F_{\tau}(\mathbf{R},\mathbf{M},A,\tau_{min})$ is the number of regular Qubits that achieve throughput level. τ_{min} Is the number of regular Qubits that achieve throughput level. As since … τ_{min} given Qubit placements R and M, assignment A, and throughput function τ although the QCHQ Qubits can reside in arbitrary locations, they can be restricted to a small number of areas without leaving the optimality. For throughput functions that are uniquely non-increasing in distance, each QCHQ Qubit can be located at in an optimal solution. K QCHQ Qubits are located anywhere in the plane, each regular Qubit is assigned to at most one QCHQ Qubit, and each assigned regular Qubit achieves throughput at least τ_{min} Let A_k be the Regular Qubits set assigned to QCHQ Qubit where k=1 ….,K, and let r_k be the distance from (QCHQ) Qubit to regular Qubit in. We are aware of…. $\tau(|A_k|,r_k) \geq \tau_{min}$ then, the distance from all regular Qubit in A_k to QCHQ Qubit k is no more than r_k. The distance from the QCHQ Qubit to the regular Qubit in A_k is r'_k we are aware of $\tau(|A_k|,r'_k) \geq \tau(|A_k|,r_k) \geq \tau_{min}$ as since τ is a non-increasing distance function. We may observe that restricting the feasible set of (QCHQ) Qubit locations to the set of 1- center locations of all subsets of regular Qubits does not reduce the maximum objective value that can be obtained. Although there is 2^N possible subsets of N regular Qubits, there are only $O(N^3)$ distinct 1-center locations. Although a particular 1-center location may correspond to multiple subsets of regular Qubits, it is uniquely defined by the regular Qubits that are most distant from it in all of these sets. Each 1-center location either coincides with a regular Qubit lies at the center of the diameter described by two regular Qubits, or lies at the circum-center of three regular Qubits.

$$\binom{N}{1}+\binom{N}{2}+\binom{N}{3}$$

For 1-center locations defined by a single regular Qubit, the associated 1- center radius is zero.1 the insight that (QCHQ) Qubits can be restricted to a relatively small number of locations without sacrificing optimality of the overall solution allows the (QCHQ) network optimization problem to be simplified. For 1-center locations defined by the diameter between two Qubits or the circum-circle of three Qubits, the 1-center radius is simply the radius of the associated circle. This radius, which we will denote as the 1-center radius, is the distance from the 1-center location to any of the defining regular Qubits. Therefore there are at most distinct 1-center locations, and they can be efficiently enumerated through enumeration of the possible sets of "defining" regular Qubits. Moreover, the maximum communication radius associated with each possible (QCHQ) Qubit location is easy to

$$\max F_{\tau} \ (R,M,A, \tau_{min})$$

compute.

M,A

Where M_i belongs to R^2 ,i=1…..K and A belongs to A Where C(R) denotes the set of 1-center locations of the regular Qubits, and |C| = O(N3).

Therefore, an approximation algorithm with computation time that is polynomial in the number of regular Qubits and the number of QCHQ Qubits is desirable. The approximation algorithm is based is the fact that … "Maximum number of regular nodes which could be assigned is a sub-modular function of the set of QCHQ Qubit locations selected. Given a finite ground set D={1,…..d} a set function f (S) defined for all subsets S of D is said to be sub-modular, if it has the property that **f(SU{i,j}-f(SU{i})<=f(SU{j})-f(S)**for all i, j belongs to D, i is not Equals to j and S is a subset of D \{i,j} In the context of the network design problem, this means that the maximum flow through the network is a sub modular function of the set of arcs incident to the sink that are selected. For maximization of a non-decreasing sub-modular set function f , where f (/0) = 0, greedy selection of elements yields a performance guarantee of

$1-(1-1/p)^p > 1-1/e$. Where p is the number of elements to be selected from the ground set and e is the base of the natural logarithm. This means that if an exact algorithm selects P elements from the ground set and produces a solution of value OPT, a greedy selection of P elements produces a solution of value at least $(1-(1-\frac{1}{p})^P)\cdot OPT$. For the network design problem considered in this paper, P = K (the number of mobile backbone nodes that are to be placed), and OPT is the number of regular nodes that are assigned in an optimal solution. Note that greedy selection of K arcs amounts to solving at most O(N3K) linear maximum flow problems on graphs with at most N+K+2 nodes. Thus, the computation time of the greedy algorithm is polynomial in the number of regular nodes and the number of

mobile backbone nodes. Furthermore, each of the maximum flow problems solved by the greedy algorithm is solved over a bipartite graph with node sets **NU{t} and {s}UK** where K is the set of nodes from M whose outgoing arcs are selected. Because maximum flow problems can be solved even more efficiently in bipartite networks than in general networks, the greedy algorithm is thus highly efficient. Further computational efficiency can result from exploitation of max flow/min cut duality.

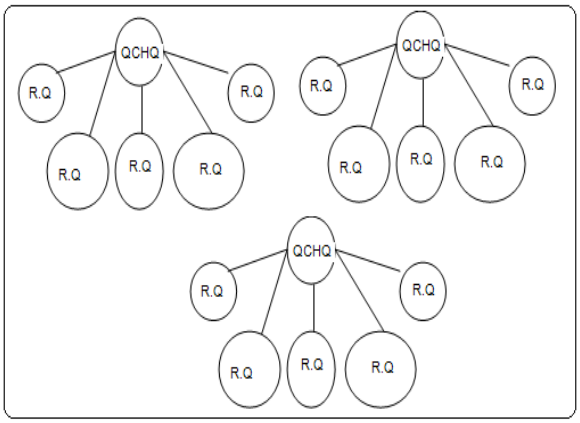

Fig.4 Hierarchical Structured Architecture

R.Q	Regular Qubits
QCHQ	QCHQ Qubits

4. ALGORITHM:

S← Ø

MaxFlow ←RQ

For k=1 to K do

For m=1 to M do

If f(S U {m})>= maxflow then

Maxflow ← f(S U {m})

$m^{QCHC} \leftarrow m$

end if

end for

$S^{QCHC} \leftarrow S \cup \{m^{QCHC}\}$

end for

return S

5. CONCLUSION:

As a Collection of Qubits those could be effectively assigned to Hierarchical Structure at any throughput level in Quantum Computers using Quantum Cryptography. Therefore with the Optimization algorithm for Throughput Optimization (TPO) in a Quantum Cryptography is possible to make.

6. REFERENCES:

[1] **AppliedQuantumCryptography**
Volume 797 of Lecture Notes in Physics, ISSN 0075-8450

[2] Quantum Cryptography and Secret-Key Distillation

By Gilles Van Assche

[3] Ryszard Horodecki, Sergei Ya Kilin, J. Kowalik

IOS Press, 01-Jan-2010 - Political Science

[4] Dirk Bouwmeester, Artur K. Ekert, Anton Zeilinger

Springer, 2000 – Computers

[5] Giuliano Benenti, Giulio Casati, Giuliano Strini

World Scientific Pub., 2007 – Computers

[6] Noson S. Yanofsky, Mirco A. Mannucci

Cambridge University Press, 11-Aug-2008 – Computers

[7] Julian Brown

Simon and Schuster, 05-Apr-2002 – Computers

[8] Sir Roger Penrose

Oxford University Press, 04-Mar-1999 – Computers