The View of a Better Implementation of Prctical - Quantum Cryptographic Architecture

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

G.Srinivasa Rao
Sr.Faculty of Computer Science
Dept. Computer Science
Key Soft Computer Education
Mehdipatnam,

B.Sujatha
Asst.Prof.EngineeringCollege,
Dept. Computer Science
Osmania University
Hyderabad.

ABSTRACT:

Quantum Key Distribution (Q.K.D.) provides us a protected communication channel. In present days we have some latest problems existing in Quantum key distribution. Let us look in to the Quantum key distribution Research analysis which provides us the Information about BB84 Protocol, using reducing laser light is used as a Photon Source, Protected keys could not be generated. The reason is it's weakness towards a Photon Number Splitting (PNS) attack which we call it as Sequential Unambiguous State Discrimination (USD) attack. We need to generate the keys with more secured mechanism.

KEY WORDS:

Quantum Key Distribution (Q.K.D.), Bennet and armour plate Protocol (BB84 Protocol), Photon Number Splitting (PNS), Unambiguous State Discrimination (USD), Differential Phase Shift Quantum Key Distribution (DPS-QUANTUM KEY DISTRIBUTION), Protected Key Rate (PKR), General Collective Attacks (GCA), Specific Collective Attack (SCA), Photon Number Splitting (PNS), Quantum Non-Demolition Measurement (QNDM), Projective Measurement (PM), Electro-Absorption Modulator(EAM), Dispersion Shifted Fiber (DSF),

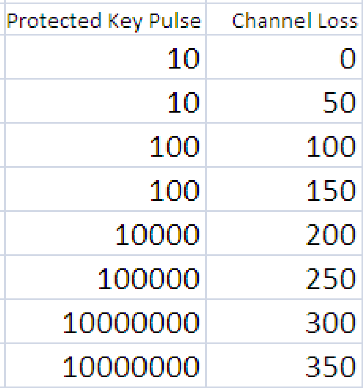
I.INTRODUCTION:"ALICE, BOB AND THE INTRUDER 'EVE' ":

Let us consider 2 people about whom we need to discuss, the 1st One is Alice (the sender), and the 2nd one is Bob (the receiver) and third one is Eve (the intruder).

Alice and Bob Approach every other:

(1) Currently allow us to imagine 'Alice' (The Sender) sends an encrypted key within the approach of 'polarized photons' that ar entangled. (2)'Bob' (Who is that the receiver) then receives them and checks the key using the calculations of the polarization.(3) currently once the Bob (Receiver) sends back the calculated key that sets the polarization values, (4) Alice (The Sender) then sends the premise on each and every Photon was polarized in (5) Recipient sends the premise on it every photon's polarization was measured in (6) Alice checks the values of these single photons that every the Alice and Bob used the same basis to form and live the polarization. Any Intrusion in these values warns them that there would be a placing intrusion presence by 'Eve' (The Intruder) so the method is left and a replacement process begins. During this case this approach utilizes the 'photons' to send as a key. Because the keys sent, Communication is enabled in between the Alice and Bob. Here the no-cloning principle it makes the Eve to live the key incorrectly. This can be as a result of the involvement of Eve that changes the direction of polarized photons. This polarization of photon will permit us only 1 'Bit' of data that may be sent. Thus key generation rate is then restricted up. But it is generally prone to get PNS Attack. In Q.K.D provides us a protected communication channel. In present days we have some latest problems existing in Quantum key distribution. That Latest One is to get Quantum Key Distribution using a 40 dB channel loss. Let us look in to the Quantum key distribution Research analysis. In Quantum key distribution generally we use a 'protected keys' for its distribution on of 42 dB channel loss and 200 km of optical fiber. Differential Phase Shift Quantum Key Distribution (DPS-QUANTUM KEY DISTRIBUTION) protocol has to used, execute it using the help of a 10-GHz clock frequency, and Superconducting Single Photon Detectors (SSPD) support by NbN nanowire. The SSPD provides a very less Dark Count Rate (DCR) in some Hz of Frequency, and small timing jitter of 60 peco seconds full width at half maximum. These properties permit to build a 10-GHz clock QUANTUM KEY DISTRIBUTION environment. And therefore to spread protected keys within the channel loss of 42 dB. Apart of this, we will get a 17 kbit per second Protected Key Rate (PKR) in 105 km of optical fiber, which is two orders of magnitude higher than the previous record, and a 12.1 bit/s secure key rate over200 km of optical fiber, which is the longest terrestrial QUANTUM KEY DISTRIBUTION yet demonstrated. The keys created in this practical are secured from General Collective Attacks (GCA) and Specific Collective Attack (SCA) over the Unique and Multiple-photons. This process is called as Sequential Unambiguous State Discrimination (USD) attack**.** While the 1st QUANTUM KEY DISTRIBUTION research is done with the help of 1-m Free Space Transmission Line (FSTL) was described are done they are generally used in BB84. The Protocol which are using reducing laser light as a Photon Source, Protected keys could not be generated. The reason is it's weakness towards a Photon Number Splitting (PNS) attack. The Eaves-Dropper (Eve) considers Quantum Non-Demolition Measurement (QNDM) on each weak simultaneous pulse generated. Whenever Eaves-Dropper identifies greater than a single photon in one pulse, Eaves-Dropper puts apart a single photon in her Quantum Memory(QM) and sends the others to Bob(The Receiver) from beginning to end her lossless transmission line. As the moment Eaves-Dropper guessed the Measurement Basis (MB) with the help of the Public Communication Channel (PCC) among the sender and the receiver then the Eaves-Dropper could make 'Projective Measurement' (PM) for a stored photon, and then get the complete idea of the pulse. In this process Eaves-Dropper does not disturb/make change the Polarization of Photons. Therefore the BB84 Protocol which is also abbreviated as "Bennet and armour plate Protocol" of QUANTUM KEY DISTRIBUTION environment has got not completely successful and also crept in some loop holes for the security

issues. To prevent from this type of PNS attack we need to have a single photon source. This made everybody to re-think QUANTUM KEY DISTRIBUTION in terms of single-photons sources, the similar attempts are made in BB84 protocol but the Protected Key Rate (PKR) was very less. Another way to identify the new protocols which could be strong on the side of PNS attack is done with Decoy State Protocol-BB84 (DSP- BB84). Here Decoy Pulses(DPs) are arbitrarily put inside of whose Average Photon Number(APN) is greater than the Signal Pulses(SP).In Latest time 107-km Protected Key Distribution(PKD) with a Bit Rate(BR) of about 0.1 bit/s has been described in our Scientists latest Research analysis by the help of Superconducting Transition Edge Sensors (STES).Using the Differential Phase Shift Quantum Key Distribution protocol , the quantum state of a single photon is described on several pulses from a consistent laser source. Alice arbitrarily adjusts the each pulse phase which came out from the source by $\{0,\pi\}$. The pulse intensity is adjusted in such a way that an average photon number per pulse could be then more (or) less equal to one. Now Bob is ready with a 1-bit delayed Mach-Zehnder interferometer, whose two output ports are pursued by two single photon detectors. If the phase difference between two pulse contiguous is 0 (π), detector 0 (1) clicks. As because of the average photon number per pulse is lesser than one, Bob's detectors clicks once at a time. Bob announces time instances in that he observed the clicks to Alice using the Public Communication Channel (PCC), at the same time keeping in hand the detector information. Using the information of time instance and original modulation data, Alice knows which detector clicked in those time instances at Bob's site. Therefore, Alice and Bob can contribute to a similar bit string which could be utilized as one-time pad key. In view of the fact that QND measurement on two successive pulses divides the consistent of the multiple-pulse quantum state, whenever the PNS attack is made QND gives the Eves-dropper the bit errors. Eve can decrease the Error Probability (EP) by making it to grow the number of pulses at the same time observed by a QND measurement, even then probability of Eve getting the key information also reduces, as since the detector click, there it is the fall down of the wave function, which happens arbitrarily and non-deterministically for Bob's and Eve's wave packets. Let us assume that if Eves-dropper has some technology which could estimate such a PNS attack on an arbitrary number of time slots, then the 'information chunk' that Eve can obtain using a PNS attack could be denoted by using 2M, in which M is the Average Photon Number(APN)/ pulse. In this scenario Eve could also make an Optimal Quantum Measurement Attack (OQMA) on the photons fraction that has been sent to Bob. Let us denote that as pc_0 which is the collision probability. $P_{c0} <= 1-e^2 -(1-6e^2)/2$ →Equation (1) where for every bit is bounded. Where *e*- system's innocent bit error rate. At that moment, considering a two-fold Attack consist of a PNS attack and an optimal quantum measurement attack, the Upper bound of the collision probability of n-bit sifted key p_c could be written as… $P_{c0} <= P_{c0}{}^{n(1-2\mu)} = (1-e^2 -(1-6e^2)/2)^{n(1-2\mu)}$ →Equation (2) $\tau = -\log_2 P_c/n = -(1-2\mu)\log_2(1-e^2 -(1-6e^2)/2)$ → Equation (3) Then the Protected Key Rate R_{pro} will be decreasing from the shifted Key Rate R_{shift} as per the equation $R_{pro} = R_{shift}\{\tau + f(e)h(e)\}$ →Equation (4) Here $h(e) = -e\log_2 e - (1-e)\log_2(1-e)$ will be a binary entropy function, and *f(e)* characterizes the performance of the error correction algorithm.



Protected Key Pulse	Channel Loss
10	0
10	50
100	100
100	150
10000	200
100000	250
10000000	300
10000000	350

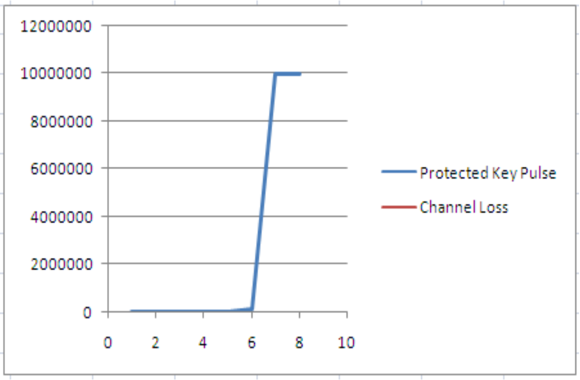
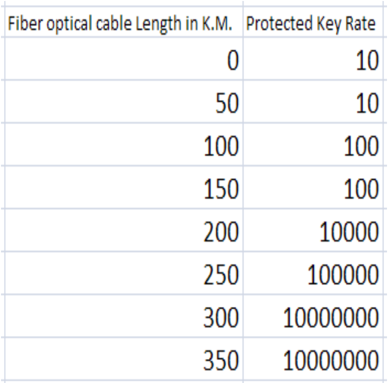


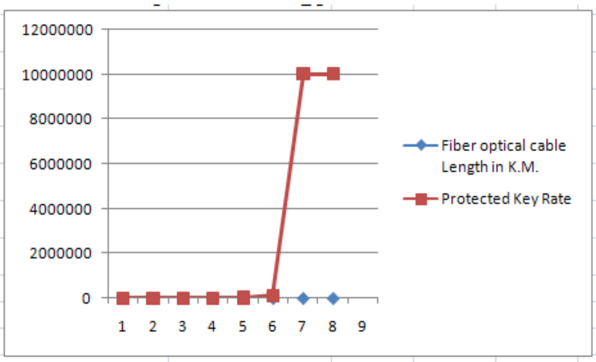
Fig 1: Protected Key Rates (PKR) vs. Channel Loss

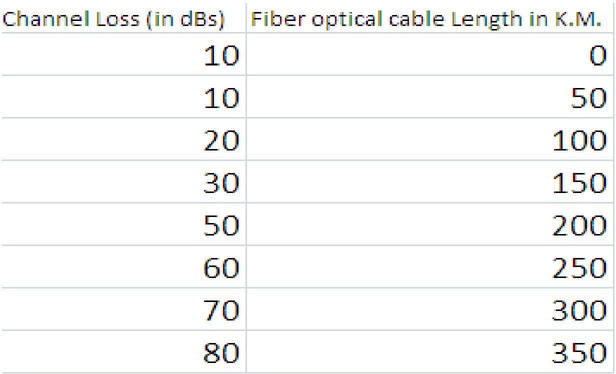
From the above graph … tells us the Protected Key Rates (PKR) vs. Channel Loss (CL) for DPS-QUANTUM KEY DISTRIBUTION with the help of standard consistent laser source and BB84 using single photon sources with various Properties. Herein, let us assume a same type of detector condition as in an experiment from our scientists Let the quantum efficiency be 1.4%, dark count rate 50 Hz, time window width 50 ps, and 36% decrease in effective quantum efficiency because of time window. Keeping in the view of BB84 Protocol environment, we consider an ideal execution, that is to say an active demodulation with no extra loss, so that Bob could use only two single photon detectors. The maximum channel loss of the DPS-QUANTUM KEY DISTRIBUTION system is greater than the BB84 system using a single Photon source with $g(2)$ (0) $=10^{-5}$ and an efficiency η =1 , that is highly above than the Available experimental research. From our earlier scientists researches the system configuration of the 10-GHz clock DPS-QUANTUM KEY DISTRIBUTION. A continuous wave result from a laser is transformed into a 10-GHz clock pulse train by an InGaAsP Electro-Absorption Modulator (EAM). We generated pulses with a full Width at half maximum of 15 ps. The phase of each pulse is modulated by a phase modulator driven by a 10-GHz pseudo random bit pattern from a high-speed pulse Pattern generator. The average photon number per pulse is adjusted to 0.2 by an optical attenuator. The quantum channel is a Dispersion Shifted Fiber (DSF) or a single Attenuator. Bob is equipped with a 1-bit delayed interferometer fabricated using planar light-wave circuit technology. The excess loss of the interferometer is 2.5 dB. Each Output port of the interferometer is connected to an SSPD. The packaged detector is housed in a closed-cycle cryogen-free refrigerator with an operating temperature of 3 K, for convenient use in quantum information experiments. The detector operates as follows: the superconducting wire is current-biased slightly below its critical current. When a photon hits the wire, a resistive hot spot is formed. Then the current density around the spot increases and eventually exceeds the critical current. As a result, a non-superconducting barrier is formed across the entire width of the wire, and a voltage pulse is formed. By discriminating the starting edge of the voltage pulses, we can measure the photon arrival time with a high timing resolution. The quantum efficiency and dark count rate of the SSPD vary when the bias current is changed. The single photon counting mechanism of an avalanche photodiode (APD) is complex (consisting of absorption, diffusion and avalanche), which results in excess dark counts and non-Gaussian timing jitter characteristics. On the other hand, the principle of SSPD is rather simple as explained earlier, which makes the dark count rate and timing resolution characteristics of the SSPD superior to those of an APD. We measured the timing jitter of the SSPD by launching 10-ps pulses. Figure 3(c) compares the obtained histogram of the photon arrival time with that of a single photon detector based on a frequency up-converter followed by a Si APD, which was used in our previous DPS-QUANTUM KEY DISTRIBUTION experiments. Here, the blue squares and the line denote the histogram for the SSPD, and the red line is that for the up-conversion detector. Even though the full width at half maximum (FWHM) of the jitter was approximately 60 ps, which is larger than that of the up-conversion single photon detectors, the histogram fits very well with Gaussian, and does not have a long tail, as observed in similar measurement for the up-conversion detectors. Therefore, we can reduce the error probability caused by inter-symbol interference by using SSPD. In addition, the dark count rate of the SSPD was measured to be <10 Hz (typically a few Hz) when the quantum efficiency was set at 0.7%, which is much smaller than that of the up-conversion detector operated in a similar quantum efficiency (350 Hz at 0.4% quantum efficiency).From our earlier scientists researches There should be (i) SSPD close-up image observed with scanning electron microscope (ii) Fiber alignment under optical microscope (iii) Histograms of photon arrival time of SSPD (squares and blue line) and up-conversion detector (red line) when 10-ps pulse is Input. We additionally a thin time window to the acquired time-instance data to decrease the contributions of the dark counts and the inter-symbol interference caused by neighboring signals. To show the effectiveness of this technique, we obtained here, the quantum efficiency and dark count rate of the SSPD were set at 0.7% and is less than 10 Hz of frequency, respectively, and the channel loss was 31.7 dB. We could observe that a signal pulse overlap caused by the detector timing jitter. However, the peaks were well separated when we employed a 10-ps time window.

In the QUANTUM KEY DISTRIBUTION research, we re-arrange the quantum efficiency, dark count rate and time window width at 1.4%, 50 Hz and 50 peco-seconds, respectively. The use of the time window decreased the effective quantum efficiency by 36%. The obtained protected key rates could be seen in below tables and graphs. The recent outcome majorly makes an impact on earlier QUANTUM KEY DISTRIBUTION analysis both in Protected Key Generation Rate (PKG) and Distribution Distance (DD). At 105 km, we could effectively generated Protected Keys at a rate of 17 k.bit per second, which is two times that of the magnitude higher than our earlier records which were 166 bit per second at 100 km. In a 200 km fiber optical cable signals sending analysis, we could be able to create a protected keys with a Bit Rate of 12 bits per second. The highest channel loss for protected key generation was 42.1 dB, which is higher than 20 dB higher than the earlier lengthy -distant QUANTUM KEY DISTRIBUTION researches. Up until now, we have considered the Protection with the help of GCA for Singular Photons. Moving further let us now consider the Protection from the sequential USD attack. Let us consider the bad scenario by thinking that Eves-dropper had a Local Oscillator (LO) which is ‘phase-locked’ to the consistent light source owned by Alice. Now with a prospect of $1^{-2\mu}$ Eves-dropper could un-doubted categorize whichever is the pulse modulated by 0 or π~ When Eve obtains *m (>M) with the* fruitful sequential measurement results, now the Eves-dropper builds ‘*m’* number of consistent pulses with phase modulations that is based on the measurement results, and sends them to Bob. When Eve gets *m (=M)* successful sequential measurement results, with a probability *p* then Eves-dropper re-sends ‘m’ number of consistent pulses with the related phase modulations, and with a probability of 1-*p ,and also* Eves-dropper resends a ‘vacuum’. Ultimately, if Eves-dropper gets ‘m’ *(<M) as a* successful sequential measurement results, she resends a vacuum. With this type of attack, no error occurs inside the pulses, but the border of pulse and vacuum becomes a reason for an arbitrary error. High channel loss gives the Eves-dropper an advantage because the number of consecutive successful USD attacks is needed not to be large. Therefore, this sequential USD attack could be a stronger threat when the channel loss is more. To examine the safety measurement of sequential USD attack, we should also estimate error threshold for this attack. The error threshold for a 200 km transmission using SSPDs with 1.4% quantum efficiency ,whereas with 36% reduction of effective quantum efficiency with the time window was 4.74%. With μ=0.2, the error threshold for generating keys that are Protect from GCA for individual photons is approximately 4.1%. This statement makes us to know that for our DPS-QUANTUM KEY DISTRIBUTION experiments with SSPDs, GCA on individual photons provides us a The Complete Protection around in comparison with sequential USD attack. As a result, the data and the graphs provide us the Protection from GCA, SCA attacks on singular photons and a sequential USD attack.



Fiber optical cable Length in K.M.	Protected Key Rate
0	10
50	10
100	100
150	100
200	10000
250	100000
300	10000000
350	10000000





Channel Loss (in dBs)	Fiber optical cable Length in K.M.
10	0
10	50
20	100
30	150
50	200
60	250
70	300
80	350

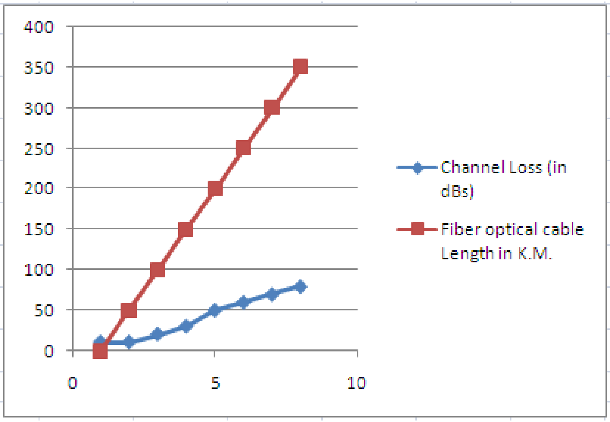


Fig 2: Protected Key Rate as a function of Fiber Optical Length

The above Graph Sheets Provides us the Information that:

Protected Key Rate as a function of Fiber Optical Length with 0.2 dB/km loss, and Protected Key Rates calculated tells us by 10-GHz and 1-GHz clock systems with SSPDs.

CONCLUSION:

As we explained a 10-GHz clock Differential Phase Shift (DPS) in Quantum Key Distribution experiment using SSPDs. The small dark count rate and small timing jitter of the SSPD allows us to produce Protected-keys with a 10-GHz clock system. So that we could distributed Protected Keys towards General Collective Attacks (GCA) for singular photons and a sequential USD attack on 200 km of fiber and with a 42.1 dB channel loss. Apart of this, we could obtain a 17 k.bit per second Protected Key Rate (PKR) at 105 km, which could be two times of the magnitude greater than the previous record. So that we could anticipate such as the result to constitute a major step towards understand simultaneously between the city and another city QUANTUM KEY DISTRIBUTION system implementation and Global QUANTUM KEY DISTRIBUTION system implementation using Geo-satellites. Here a note worthy information is that Geo-Synchronized-satellites generally which needs 30-35 dB channel loss which is enough for them.

REFERENCES:

[1] Code talker by Joseph Bruchac

[2] Cryptonomicon by Neal Stephenson

[3] Cryptonomicon by Neal Stephenson

[4] Top secret Ultra byPeter Calvocoressi

[5] U-571 by Max Allan Collins

[6] Super computers by Rajaraman

[7] A computer Laboratory Referral forDeploma by Jagadeesh,T.R

[8] A-Z Nano computer by Albert Shawn

[9] Advances in Computational Optimizationand its byKalyanmoyDeb

[10] Architecture,Programming and Application of vy A.K.Ganguly

[11] Basic Computation amd Principles and Computer by E.Balaguruswamy

[12] http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution

[13] http://gcn.com/articles/2013/10/29/how-quantum-key-distribution-works.aspx

[14] http://arxiv.org/abs/quant-ph/0012056

[15] http://iopscience.iop.org/1367-2630/4/1/341

[16] http://www.sciencemag.org/content/283/5410/2050.short

[17] http://en.wikipedia.org/wiki/Quantum_cryptography

[18] A Few Words on Secret Writing byEdgar Allan Poe

[19] http://www.newsfix.ca/2013/11/17/university-research-teams-new-approach-enhances-quantum-based-secure-communication

[20] http://arxiv.org/abs/quant-ph/0012056

[21] http://prl.aps.org/abstract/PRL/v91/i5/e057901

[22] http://iopscience.iop.org/1367-2630/4/1/341

[23] http://www.sciencemag.org/content/283/5410/2050.short

[24] http://www.pcadvisor.co.uk/news/security/3494723/quantum-crypto-standard-private-key-blended-for-first-time/

[25] http://www.scienceagogo.com/news/20131108232216.shtml

[26] http://news.idg.no/cw/art.cfm?id=AEA6F636-0149-5FB9-4E000A404DA37981

[27] http://www.poynter.org/how-tos/digital-strategies/234005/how-journalists-can-encrypt-their-email/

[28] http://www.prnewswire.com/news-releases/gridcom-technologies-unhackable-encryption-technology-named-in-popular-science-magazines-20-ideas-that-will-change-the-world-236538341.html