Contemporary Cryptography and Arguments for Classical Cryptography's Endurance alongside the Propitious Quantum Cryptography

[1]R.Sakthi Vignesh
Department of Electronics and Communication, Pre Final year
SSN College of Engineering
Chennai, India

[1]S.Sudharssun
Department of Electronics and Communication, Pre Final year
SSN College of Engineering
Chennai, India

[2]K.J.Jegadish kumar
Department of Electronics and Communication-Senior Lecturer
SSN College of Engineering
Chennai, India

ABSTRACT
Is the newly born quantum cryptography the ultimate solution for information security? A technique needs to be both theoretically strong and practically viable. But quantum cryptography comes to naught in the latter. We present here some of the quantum's theoretical weaknesses like lack of digital signatures (or any algorithm) along with its many real time implementation problems. We further pursue with the discussion about the potency of classical cryptography and its splendid capabilities in providing security.

Keywords
Cryptography, Quantum, Classical

1. INTRODUCTION
Quite recently, we witnessed an important advancement in data transmission that has its roots from quantum mechanics. This method, called Quantum Cryptography was first proposed in 1984.Since then there has been significant development in it and recently scientists have succeeded in transmitting data through a reasonable distance of 250 Km in free space but at a fruitless transmission speed of 16-bits per second [1]. General purpose use of it has not yet come as on date but we have an artifact in our hand, namely the classical which can do wonders when its potentials are brought to light.
The basic objective of the paper is to point out the vulnerabilities and impotency of transmission through quantum channel and to bring out the true potentials of classical cryptography which assures enhanced security along with a wide variety of salutary security tools.

2. QUANTUM CRYPTOGRAPHY(QC)

Quantum cryptography was first proposed in 1984 by Brennet and Brassard [2] based on the No-Cloning theorem. They proposed that this way of sending messages could prove to be the most secure because the eavesdropper cannot read or clone the bits as it would change the state the photons polarization thus raising an alarm. The crucial part of quantum computation is that the quantum system has "qubits" which not only has two states i.e. '0' or '1' but also a superposition of both. The SECOQC White paper of 2007 has proved past regret that QKD is a reliable courier.The following steps are done for a QKD session

Authenticate. Over an open communication line, Alice confirms she is talking to Bob, and Bob confirms he is talking to Alice.
Use a quantum protocol. The protocol dictates how Alice is to encode her random bit stream as a quantum state of a single photon. Bob measures photons according to the protocol.
Construct the sifted key. Alice and Bob use an open line to discover which photons were sent and measured in the same basis. The bit values associated with that subset of photons form the sifted key.
Construct the reconciled key. Over the open line, Alice and Bob find and remove errors from the sifted key to make the reconciled key.
Construct the secret key. Alice and Bob use privacy amplification to construct a secret key from the reconciled key. An eavesdropper has essentially no information about the bits in the secret key.
Save some bits. A few secret bits are retained to enable authentication in the future.

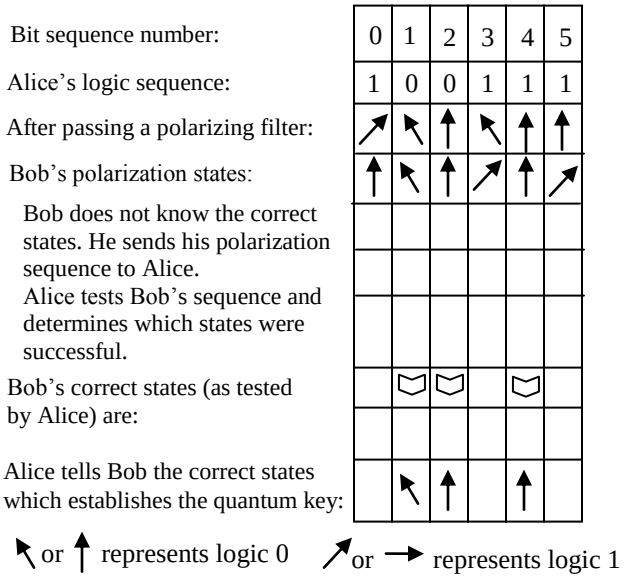

Figure 1: Diagrammatic representation of the quantum session

But consider the following example. Alice needs to send a letter to Bob. He must make sure that:

i) There is no one in Alice's room who can possibly leak the contents of the letter which she is writing.
ii) Charlie, the human courier is honest at the receiving moment from Alice.
iii) Charlie does not leak the information while carrying the information from Alice to Bob,

Considering Charlie as a quantum courier, (3) is not at all a problem as it is taken care of by the laws of physics. But what about (1) and (2) ? Eve may be spying on Alice through a camera while she is writing. Or Alice may commit mistakes while she drafts her letter. There is also a possibility for the contents of the letter to get corrupted due to improper handling while it is being transported.
One has to make sure that (1) and (2) have a solution before he can claim QC as the 'ultimate solution' for information security.

Important: In this paper we view Quantum Cryptography (QC) as a technique for secured communication using the laws of physics and Quantum Key Distribution (QKD) as an application based on QC.

3. REAL TIME PROBLEMS OF QUANTUM CRYPTOGRAPHY (QC)

It's important to note that implementation of algorithms using QC is not viable if one wants to have the security intact. It can only be used to share keys using Quantum Key Distribution (QKD). Distribution of keys is just a part of securing information. Proper encryption and decryption are equally important for preventing Eve from guessing the key. But even QKD has a lot to overcome before it's perfectly safe and practically useful. Here are a few things that laws of physics don't take care of.

3.1 The Need for a Non-Quantum Channel

In QKD, just before the key is finalized, there is a two way communication between Alice and Bob, using a normal channel. Here they discuss and conclude on the correctly decoded states, which makes up the key. However, during this communication, a man in the middle attack can be enforced. In such a case, Eve hears to Bob's polarization sequence, and passes it on to Alice. When Alice sends the sequences numbers of correctly decoded states, Eve passes that information on to Bob, after making note of the sequence numbers. Bob and Alice cannot detect Eve (the channel is normal) during this transaction and thus proceed with the transfer of data. However, Eve now knows the key (the sequence numbers of the correctly decoded states are known to Eve) and can thus decode the packets. This proves that QKD is not completely safe, it only appears to be.

3.2 Change in Polarization:

While traveling through the channel, say optical fiber or through air (wireless), there is always a possibility of change in polarization of photon. The various causes of the same could be:

3.2.1 Action of Birefringence:

The Birefringence is the process of splitting of beam of light into the ordinary and extraordinary rays when passed through certain materials. This effect can occur when the structure of the medium is anisotropic.The reason for birefringence is the fact that in anisotropic media the electric field vector and the dielectric displacement can be nonparallel (namely for the extraordinary polarisation), although being linearly related.If the n_e and n_o are the refractive indices of the material due to the ordinary and extraordinary rays respectively and F is the birefringence,

$$F= k|n_e – n_o| \quad [3]$$

Pooling this idea with quantum, we find that the message that is transferred due to photon polarization may change its state (change in polarization) while traveling through a medium. So, one must make sure that the medium is a perfectly homologous one with respect to the refractive index. But this is practically ambitious and leads to changes in the polarization of the photon which leads to misinterpretation by Bob.

3.2.2 Paper Clip. A paper Clip?

We need to remember that the eavesdropper may not only be a kleptomaniac but also cause cataclysm in the transfer of bits. One such example is the paper clip inkling. The fiber cable may go through rough paths such as the underground pipes, sea water, subway tunnels etc, paving way for the attacker to do his job. Just a paper clip is all that is needed. A paper clip, pinched onto the fiber is enough to cause enough change in refractive index at that point leading to change in polarization. This ultimately leads to wrong interpretation of data.[4] Imagine a city using such highly sensitive communication lines for all it's important links and a eavesdropper who wants to shut down the city's entire network! Job made easy, isn't it?

3.3 Lack of Digital Signatures:

The digital signatures are those which demonstrate the authenticity of the digital data to the receiver. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. The digital generation scheme consists of three algorithms namely key generation, signing, key verification. But we know that algorithms cannot be implemented in QC very easily. Therefore QC lacks many vital features like digital signature, certified mail and thus the ability to settle disputes before a judge.[5]

3.4 Predicament Due to the Source:

A basic point to be taken care of while designing the source is the laser pulses' coherence in phase. It is essential that all the photons emitted should be having varying phase coherence. This requires a very sensational design of phase modulator that changes the phase of the successive photons in a rapid fashion. And the attenuated laser pulses are not single photons and the multi-photon components are important [6]

3.5 Distance and Free Space Communication:

The latest distance that scientists have managed to get in QKD is 250 Km at a speed of 16 bits per second and that too through guided medium [7]. However, the satellites in air are at around 36000 Km from the earth surface separated by free space, which makes it incomparable to the former data. So Quantum in wireless is far from reach. One may suggest Quantum repeaters but the number of such repeaters required makes it costlier than the actual

system itself! And we need to comprimise on the distance for speed and vice versa. Researchers have been trying to implement ground-Satellite communications for so many years.
Proposals have already been given that one can use the weak laser pulses instead of single photon for free space communication as a single photon when sent through the turbulent atmosphere, would lead to errors even during nights.

We know that when a signal has to be transmitted to satellite it must pass through the ionosphere layer that cotains many sub-layers within itself, containing several ions.The short wavelength photons are absorbed by these materials that splits up a neutral atom into an electron and a companion. Altogether the photon that is sent is lost. However the theory of background rejection and immunity to the Faraday rotation has lead to succcessful proposal of this theory, taking an advantage that the atmosphere is non-birefringent in optical wavelengths. Still there are many more implementation problems that are needed to be considered.Some of which are

i) The background radiation rejection and the non-birefringent atmosphere work only for normal atmospheric conditions. One cannot expect such conditions throughout the year. The main challenge is that the above method does not give secure and reliable communication for all weather conditions.

ii) The Denial of Service (DoS): The DoS is simply an attempt to make the resource unavailable for its intended users. For a transmission to be reliable it must be resistant to the Denial of Service attacks. However till date, the extent to which the free space comunication has the immunity towards DoS remains very low.

Furthermore, till date the maximum possible distance that has been demonstrated is 10Km in day light and 23Km in the night (In Free Space).The main parameters such as the quantum physics implementation maturity, classical protocol implementation maturity, key transfer readiness, practical security, network and encrypor readiness has not yet been fully satisfied even for short distance communication and none of the above has been satisfied for long distance transmission (>70Km).

3.6 Trojan Horse Attack

While considering the plug and play systems, Alice's device is open to receive photons So Eve in the middle may send in a light pulse towards Alice's polarizer, this light gets reflected from the polarizer and leaks vital information to Eve[8]. Other attacks such as the time-shift attack, has been successfully used to crack commercially used quantum key distribution system. This is the first successful demonstration of hacking in a quantum channel.[15]Presently hackers are not having much to gain by spending their resource in hacking the sparsely used a quantum channel. But as QC users increase one can expect more such unexpected innovative attacks which are unthought-of till date.

3.7 No Cloning of Qubits?

One of the fundamental features of quantum information is that it is impossible to generate perfect copies (or `clones') of an unknown quantum state input. However, it was later found that stimulated emission is in fact an optimal approximation to perfect quantum cloning. This insight was quickly followed by the first experimental realizations of optical quantum cloning using parametric optical amplification. Recently, it has also been discovered that the bunching properties of light fields can be used to obtain optimal clones by post-selecting the output of a beam splitter. In general, optical cloning methods thus exploit the natural wave-particle dualism of light to clone the quantum coherence of photons by manipulating the (classical) optical coherence of the light field.
In order to get the field properties of photons, one must measure the quadrature components $\hat{\mathbf{w}}$ and $\hat{\mathbf{y}}$ of the complex field amplitude $\hat{\mathbf{a}} = \hat{\mathbf{w}} + \mathbf{i}\hat{\mathbf{y}}$. This obviously can be used to get the polarization state of the photon as the polarization merely depends upon the two complex amplitudes, $\hat{\mathbf{a}}_{\mathbf{H}}$ and $\hat{\mathbf{a}}_{\mathbf{V}}$ of a pair of orthogonal polarizations H and V. For a single-photon input, the measurement of the two complex amplitudes $\hat{\mathbf{a}}_{\mathbf{H}}$ and $\hat{\mathbf{a}}_{\mathbf{V}}$ by homodyne detection is indeed equivalent to a quantum mechanically precise detection of the photon in the polarization defined by the measurement results obtained for the amplitudes. A particularly simple cloning scheme could thus be realized by measuring the complex amplitudes of the input photon and modulating a coherent laser beam to emit multiple photons with the same polarization amplitudes.The schematic figure of the optimal cloning set-up is shown in the following figure.[10]

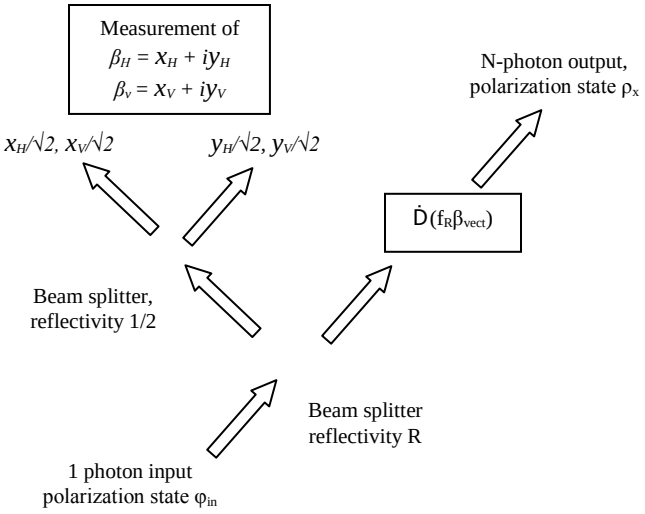

Figure 2: A Schematic of the optimal cloning set-up

The one-photon input state $|\psi_{in}\rangle$ is split at a beam splitter of reflectivity *R*. The reflected part is split once more to allow the simultaneous uncertainty limited measurement of the four quadrature components $\dot{\mathbf{x}}_{\mathbf{H}}$, $\dot{\mathbf{x}}_{\mathbf{V}}$, $\dot{\mathbf{y}}_{\mathbf{H}}$ **and** $\dot{\mathbf{y}}_{\mathbf{V}}$ by homodyne detection. The measurement result is then transmitted to an optical modulation setup that displaces the transmitted field amplitudes by a feedback of f_R times the measured amplitudes.Thus we can say that if advancements in quantum communication take place so is the developments in countering basic properties of quantum like No-Cloning of bits.

3.8 Need of a dedicated channel:

Exchanging information using single photon needs a dedicated channel of high quality in order to achieve high speed communication. It is impossible to send keys to two or more different locations using a quantum channel as multiplexing is against quantum's principles. Therefore it demands separate channels linking the source with the many destinations which

implies high cost. This is a major disadvantage faced by quantum communication especially through optical channel.

3.9 Tolerable error:

For channels such as an optic fiber, the probability for both absorption and depolarization of the photon stretches exponentially with the length of the fiber. This may cause the following problems:

i) The number of trials required to transmit a photon without absorption or depolarization grows exponentially with length of channel

ii) Even when a photon arrives, the fidelity of the transmitted state decreases exponentially with length of channel.
The tolerable error probabilities for transmission are less than 10^{-2}, and for local operations they are less than 5×10^{-5}. This seems to be far away from any practical implementation in the near future [10]

4 CLASSICAL CRYPTOGRAPHY (CC)

'Security through computational complexity' is the working rule for Classical Cryptography. It uses one way mathematical operations to provide security. That is these computations are easy in the forward direction where as they are computationally demanding if performed in the reverse e.g. discrete logarithms. In encryption and decryption process the information coding using the key is a easy forward process while the reverse process of finding the key or plaintext from the cipher text is almost impossible. From the above discussion we can clearly see that the security of CC depends on Eve's computational weakness. So if eve is assumed to have infinite computational power, then CC backslides, which is considered as a major disadvantage.

There are a lot of algorithms available in CC, each of them serves for a different purpose. Some are used for key exchange while some are used for encrypting and decrypting the message. A few of those has been listed in the table shown below. Even the revolutionary concept of digital signature is a part of the classical family.

Table 1:Popular Algorithms and their Features:

Algorithm	Confidentiality	Authentication	Integrity	Key Management
Symmetric Encryption	Yes	No	No	Yes
Public Key	Yes	Yes	No	Yes
Digital Signature	No	Yes	Yes	No
Key Agreement Algorithm	Yes	Optional	No	Yes
One Way Hash Function	No	No	Yes	No
Message Authentication Code	No	Yes	Yes	no

We discuss below a few popular Classical Cryptography algorithms.

4.1 Public Key Cryptography:

In 1976, Whitfield Diffie and Martin Hellman changed the paradigm of cryptography forever [12]. They used two different keys, one public and the other private. It is computationally hard to deduce the private key from the public key. Anyone with the public key can encrypt a message but not decrypt it. Only the person with the private key can decrypt the message. It is as if someone turned the cryptographic safe into a mailbox. Putting mail in the mailbox is analogous to encrypting with the public key; anyone can do it. But opening the mailbox (a strong vault) and reading the content is easier for the one with the key rather than the one with a hacksaw. There are many algorithms which use this concept but the most popular and cogent one is the RSA Algorithm.

RSA Algorithm with example:

1. Choose two prime numbers (p, q)
   E.g. $p = 61$ and $q = 53$
2. Compute $n = pq$: n = 61 x 53 = 3233
3. Compute the totient $\varphi(n) = (p-1)(q-1)$
   $\Phi(n) = (61-1)(53-1) = 3120$
4. Choose $e > 1$ co-prime to 3120: $e = 17$
5. Compute d such that $de \equiv 1 (\text{mod } \varphi(n))$
   e.g., by computing the modular multiplicative inverse of e modulo $\varphi(n)$:
   $d = 2753$ since $17 \cdot 2753 = 46801$ and mod (46801, 3120) = 1 this is the correct answer.

Thus
The **public key** is ($n = 3233$, $e = 17$). For a padded message m the encryption function is:
$c = m^e \text{ mod } n = m^{17} \text{ mod } 3233$.

The **private key** is ($n = 3233$, $d = 2753$). The decryption function is:
$m = c^d \text{ mod } n = {}^{2753} \text{ mod } 3233$

For example, to encrypt $m = 123$, we calculate
$c = 123^{17} \text{ mod } 3233 = 855$
To decrypt $c = 855$, we calculate
$m = 855^{2753} \text{ mod } 3233 = 123$

4.2 Symmetric Key

Symmetric algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely [11]. The security of a symmetric algorithm rests in the key, divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key must remain secret. Usually Public Key or any other key management algorithms are used to exchange the keys before the communication takes place.

Encryption and decryption with a symmetric algorithm is denoted by:

$$E_k(M) = C$$
$$D_K(C) = M$$

4.3 Digital Signatures

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message. A valid digital signature enables a recipient to believe that the message was created by a known sender, and that it was not manipulated by anyone. Digital signatures are commonly used for protecting duplication of software (software licensing), financial transactions, and in cases where it is important to detect forgery and tampering.

The important features of digital signature are its authentication and integrity and these two go hand in hand. In most cases, the sender and receiver expect some means by which they can be confident that the message has been crafted by the expected person and that it has not been altered during transmission. Though encryption hides the contents of a message, it is quite possible to change the encrypted message even without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signing will spoil or disintegrate the signature. Further, there is no efficient way to modify a message and its signature to produce a new message without invalidating the signature.

5 THE VERSATILITY OF CLASSICAL CRYPTOGRAPHY

It is condemned that CC's strength depends upon Eve's computational weakness and this criticism has been on the rise ever since the arrival of quantum cryptography.

So will CC lose its place with the upcoming of QC? Or will QC be able to sustain on its own? 'Definitely not', here are the advantages that CC holds over QC which assures it a permanent place in the future.

5.1 Non Dependency on the Medium:

Since CC's the security is purely based on the strength of the algorithm and not on the method of implementation it can be implemented on any practically proven technique of digital communication. This is one of the major advantages that CC holds. In future one can expect many new methodologies being introduced in the field of digital communication which promises better quality or range. For all these, quantum cryptography may not be able to assure security as its security is provided sole by the courier (message carrier). However CC can assure information security for all present and future ways of communication.

5.2 Identity:

With millions of users and thousands of hackers sharing the same communication channel, one would like to know as to who is sending the information and as to whether it is from the expected person or not. To cater to this issue there are beautiful solutions in CC, like the Digital Signatures which have been crafted to run-over this crunch.

Public keying is an example of digital signature. That is, only the person with the public key (n,e) can send a valid encrypted data to the destination, which can be usefully decrypted. By this the receiver can be sure that the message is being sent by the authorized person with the pubic key. Such algorithms are very handy as they can provide security and signature.

5.3 Life Expectancy:

Moors law states that computational power doubles approximately every 18months and we also see that the cost of computation is reducing drastically with time. This means the computational power available in future will keep growing unbound and one has to ensure proper security at all times. CC fully depends on the computational complexity, and providing security alongside growing processing power is a major disadvantage that CC has to overcome if it has to stay impressive. To get a better picture, we list below the life expectancy of a few CC algorithms.

Table 2: Life Expectancy of CC algorithms

Algorithm	Bit Length	Expected Lift Time
Triple Key DES	112	Through 2030
256-bit AES	256	Beyond 2030
DSA(p=7680,q=384)	192	Beyond 2030
DSA(p=2048,q=224)	128	Through 2030
SHA-512	256	Beyond 2030
SHA-224	112	Through 2030

We see that an algorithm using an n-bit key which is proving secure now may not be safe in a few years from now.

So, how to overcome this?

With a proper futuristic view one can infer that increased computational power is not only in the hands of Eve, but is also available to Alice and Bob. Thus with some gumption we can say that increasing computational power is not a pitfall for CC. Thus to increase the complexity one needs to increase the key length and to do that all that is required is affordable computational power. Thus when its year 2030 with predicted available computational power one can expect key size of 16,384-bits [13] or greater which ensures security at least till year 2050, and this will go on. Processors at any time can do the forward 'one way' mathematics much faster than the reverse process and thus life time of an algorithm can be increased quite indefinitely, the only problem being the need for regular hardware up-gradation.

5.4 Colossal Communication Range:

Distance of communication is mostly dependant on the technique of communication and not on the security algorithm. Thus CC promises secure communication over millions of kilometers. At present space shuttles travelling into deep space use CC to have secured communication with the base station (i.e.) without leaking important data to rival base stations. It's stiff to even imagine doing the same using a quantum channel.

5.5 Multiple Platforms for Implementation:

Both hardware and software implementation is possible when CC is used to for security. Hardware implementation is widely used for speeding up communication and also to make the algorithms tamper free. It also enables various other use, like the one demonstrated by IBM. They came up with innovative tamper proof cryptographic hardware modules to hold the keys [9]. Software implementation is extensively used to prevent software privacy or for user management. Software implementation for communication is slow but has the flexibility of changing the key size at will. Such security

especially security through software can only be handled using CC algorithms.

5.6 "I don't need a reliable courier"- CC :

Courier reliability is not an issue in CC because its security bets only on the computational complexity. Thus even with full information of what is being sent, Eve will have to downtime and compute for thousands of years before he gets to know the plain text. This removes the need for exorbitant secure channels.

5.7 Communicating in complex networks:

Considering any network in existence now; we will find that every network is highly interlinked and one is having a need to communicate using a shared channel. Information exchange in such integrated networks is very much possible in CC.

5.8 What if Quantum Computing Becomes a Reality? :

It is estimated that a 1024-bit RSA key could be broken with roughly 3000 qubits. Given that current Quantum Computers (QCmp) have below 10 qubits, public-key cryptography is safe for the foreseeable future, but this is not an absolute guarantee [14]. So what happens when a 3000-qubit QCmp becomes a reality?

This issue is analogous to the one discussed under the 'Life Expectancy' i.e. use the computational resource of a QCmp to implement complex algorithms to make cracking difficult for another QCmp. Example, if Alice is using RSA Algorithm, then he can generate very large primes (there is no upper limit for primes) and process them quickly to exchange the cipher text with Bob. These primes having been generated by a QCmp will be large enough to trouble another QCmp try to crack the information. It's a well known fact that multiplying two primes is always easier than factoring the product. In fact with the upcoming of faster processors, new computationally demanding algorithms may be discovered and implemented in future without the worry of slowing down the communication process.

6 CONCLUSION

From our discussion it's clear that Classical Cryptography (CC) is having a definite upper hand over Quantum cryptography (QC) at present. This is largely due to the implementation problems and lack of algorithms in QC. In future one can expect most of the implementation problems in QC to be overcome. Even that being is the case; QC's application will be restricted to Quantum Key Distribution (QKD) which plays an important but rather a small part in the protection of data. This restriction is basically due to the fact that algorithms cannot be implemented in QC without sacrificing on security. Thus we can conclude that CC with so many proven strengths can never be written off and will always demandingly occupy a major territory in the world of information security.

We consider the paper's objective to be accomplished if it had been of any use in the following ways.

i) Induce a speck of clarity to the reader and to the industries working in this field.
ii) Serve as a word of encouragement for those pursuing their research in Classical Cryptography.
iii) Help in pointing out the short comings in QC which needs to be overcome in order to ensure it a future.

7 REFERENCES

[1] A Los Alamos National Laboratory http://www.physorg.com/news86020679.html

[2] C. Bennett and G. Brassard, in Proceedings of IEEE,International Conference on Computers, Systems

[3] Eric Weisstein's World of Science on Birefringence http://scienceworld.wolfram.com/physics/Birefringence.html

[4] Identifying vulnerabilities of quantum cryptography in secure optical data transport Stamatios V. Kartalopoulos, PhD,Williams Professor in Telecommunications Networking, The University of Oklahoma

[5] Quantum Cryptography: Public Key Distribution And Coin Tossing: Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA) & Gilles Brassard (dept. IRO, Univ. de Motreal, H3C 3J7 Canada)

[6] N. Lutkenhaus, Phys. Rev. A 61, 052304 (2000);
G. Brassard, N. Lutkenhaus, T. Mor, B.C. Sanders, Phys. Rev. Lett. 85, 1330 (2000).

[7] Los Alamos National Laboratory http://www.physorg.com/news86020679.htmlC. Bennett and G. Brassard, in Proceedings of IEEE,International Conference on Computers, Systems

[8] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, Electronics Letters 34, 2116 (1998)

[9] W.F. Ehrsam, C.H.W. Meyer, and W.L. Tuchman, "A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard," *IBM Systems Journal*, v. 17, n. 2, 1978, pp. 106–125.

[10] Optimal cloning of single-photon polarization by coherent feedback of beam splitter losses Holger F Hofmann and Toshiki Ide

[11] Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth) Author(s): Bruce Schneier

[12] W. Diffie and M.E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, v. IT–22, n. 6, Nov 1976, pp. 644–654.

[13] R.L. Rivest, "Dr. Ron Rivest on the Difficulty of Factoring," *Ciphertext: The RSA Newsletter*, v. 1, n. 1, Fall 1993, pp. 6, 8.

[14] Information Security Management Handbook By Harold F. Tipton, Micki Kraus

[15] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo: "Experimental demonstration of time-shift attack against practical quantum key distribution systems", arXiv:0704.3253