Shortcomings of Quantum and the usage of Classical Cryptography: A Review

Sahana Lokesh R [*, a], T.N Srikanth [b], H.S Saraswathi [c]
[a] Department of Computer Science, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
[b] Department of Computer Science, SaIT, Bangalore, India
[c] Department of Computer Science, Jain Institute of Technology, Davanagere, India

Article Info
Article history:
Received 2 February 2015
Received in revised form
20 February 2015
Accepted 28 February 2015
Available online 6 March 2015

Keywords
Cryptograph,
Quantum,
Classical

Abstract

Is the newly born quantum cryptography the ultimate solution for information security? A technique needs to be theoretically strong and also 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 resplendent capabilities in providing security.

1. Introduction

Quite recently, we witnessed an exhilarating 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. 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 to light the true potentials of classical cryptography which assures propitious 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 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. But consider the following example. ; Alice needs to send a letter to Bob. He must make sure that:

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

Corresponding Author,
E-mail address: sahana.lokesh@gmail.com

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.

All these are not taken care of by the laws of physics and thus one has to make sure that (1) and (2) have a solution before he can claim QC as the 'ultimate solution' for information security.

A few years ago the concept of Quantum Key Distribution (QKD) was proposed and we diagrammatically explain its working:

Important:

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

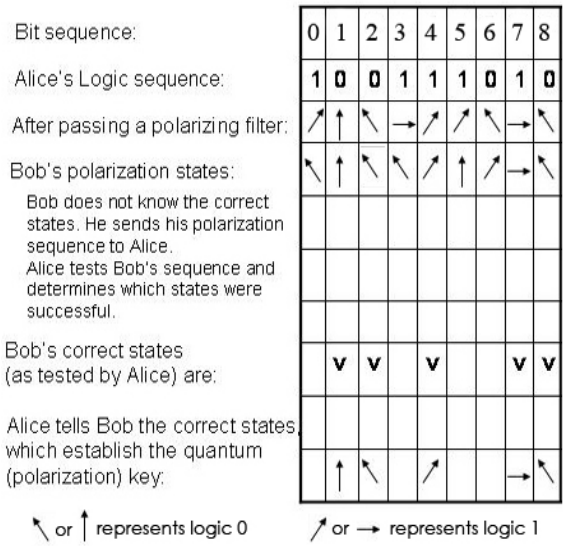

Fig: 1. Sequence of Operations

3. Limitations of Quantum Cryptography

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. A Flip-Flop is 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:

3.1.1. 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. If the ne and no are the refractive indices of the material due to the ordinary and extraordinary rays respectively and F is the birefringence,

$F= k|ne – no |$

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.

3.1.2. 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 waters, subway tunnels etc, paving way for the attacker to do his job. Just a paper clip is all that is needed. A paper clip when pinched onto the fiber causes the change in refractive index at that point leading to change in polarization which ultimately leads to wrong of interpretation of data. Imagine a city using such highly sensitive communication lines for its entire important links and a eavesdropper who wants to shut down the city's entire network! Job made easy, isn't it?

3.2. Dearth 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.

3.3. Predicament Due to the Source

A conspicuous 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.

3.4. Distance

The latest and the best distance that scientists have managed to get in QKD is 250 Km at a speed of 16 bits per second. But the satellites in air are at around 36000 Km from the earth surface, 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!

3.5. 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 light towards Alice captivating her to accept the message, causing him to get it back, coded. 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.

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.

3.6. 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. This may form as a blessing in disguise for the attacker who can just clone the bits while in channel.

3.7. Need of a dedicated channel

Exchanging information using single photon needs a dedicated channel of high quality. 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.

3.8. 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:

a) The number of trials required transmitting a photon without absorption or depolarization grows exponentially with length of channel
b) 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

4. Classical Cryptography (CC)

'Security through computational complexity' is the working rule for Classical Cryptography. It uses one way mathematical operations which makes the reverse process of finding the key or plain text an almost impossible job. But if eve is assumed to have infinite computational power, then CC backslides bringing around a disadvantage into this field.

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 Algorithms	Yes	Optional	No	Yes
One Way Hash Function	No	No	Yes	No
Message Authentication Codes	No	Yes	Yes	No

Briefing on a Couple of CC Algorithms

4.1. Public Key Cryptography

In 1976, Whitfield Diffie and Martin Hellman changed the paradigm of cryptography forever. 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 φ(n) = (p-1)(q-1)
   Φ(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 φ(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:

$c = m^e \bmod n = m^{17} \bmod 3233$.

The **private key** is ($n = 3233$, $d = 2753$). The decryption function is:

$m = c^d \bmod n = c^{2753} \bmod 3233$

For example, to encrypt $m = 123$, we calculate $c = 123^{17} \bmod 3233 = 855$

To decrypt $c = 855$, we calculate

$m = 855^{2753} \bmod 3233 = 123$

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. 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 are denoted by:

$E_K(M) = C$

$D_K(C) = M$

5. 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 and 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 security purely depends on the complexity of the algorithm, the data (key or cipher text) exchange can happen via any media where traditional means of communication is considered possible.

5.2. Identity

With millions of users along with thousands of hackers, one would like to know as to who is sending the information and whether it is from the expected person or not. Since algorithms can be implemented in CC, beautiful solutions like the Digital Signatures have been crafted to run-over this crunch.

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. Due to this an algorithm using a n-bit key which is proving secure now may not be safe in a few years from now.

This is seen as one of the biggest drawbacks in CC. But 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 it's not a pitfall for CC. All that is required to increase the key size is better and affordable computational power. Thus when its year 2030 one can expect key size of 16,384-bits or greater being processed at the same speed and cost thus ensuring 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 up-gradation.

Table: 2. A Few Examples

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

5.4. Colossal Communication Range

Distance of communication is not dependant on the CC algorithm and thus it promises secure communication over millions of kilometers. These days' space shuttles travelling deep into 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. 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. Key or cipher text exchange in complex networks

Considering any network in existence now; we will find that everything network is highly interlinked and one is having a need to communicate using a shared channel. Key exchange in such integrated networks using CC is a cake walk.

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. 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.

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

References

[1] C. Bennett, G. Brassard, IEEE, International Conference on Computers, Systems

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

[3] Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA) & Gilles Brassard (dept. IRO, Univ. de Motreal, H3C 3J7 Canada)

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

[5] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, Electronics Letters 34, 2116, 1998

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

[7] Purification of noisy entanglement and faithful teleportation via noisy channels,Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters

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

[9] 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.

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

[11] W. F. Ehrsam, C.H.W. Meyer, W. L. Tuchman, A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard, IBM Systems Journal, 17(2), 1978, 106–125.

[12] Information Security Management Handbook By Harold F. Tipton, Micki Krause