Enforcing Communication Security in Times of Quantum Computers
Quantum Cryptography, Overview

Mag.edu.inf Valter Popeškić
University of Rijeka
Department of Informatics, Rijeka, Croatia
v@lter.biz

Abstract - This work will try to justify the efforts invested in the development of advanced techniques which make quantum cryptography work. It does it in a way that will describe the trends in the development of quantum computers and their impact on current cryptographic systems.

Effects of quantum mechanics are starting to be applied within different technologies. Today more and more advanced systems are emerging that are leveraging quantum mechanics to build enhanced solutions from legacy technology.

This work is a review of Quantum Cryptology. The motivation behind this work lies in the beauty and simplicity of the idea that powers Quantum Cryptology as a technique that enables Quantum Key Distribution. This work will try to engage the reader to dive deeper into technology that exploits quantum characteristics of small particles and uses those characteristics, which at first look as weaknesses, as a main advantage.

With theoretical quantum cryptography in the main focus, this work will explore even further and try to explain Quantum Cryptography, Quantum key distribution and further details of their usage.

Keywords: Quantum Key Distribution, Quantum Cryptography, Key Generation, Interception Detection

I. INTRODUCTION

In computer systems today, almost everything we have and use is based on Electrodynamics. Deeper understanding of the world of small, under-atom particles is the next step for physicist of our time to explore. Huge steps are already taken and we today know so much about quantum mechanics. First ideas, emerged in the last 50 years, about exploiting quantum mechanics are starting to give results. First Quantum Cryptology systems are already available today.

Quantum mechanics explores quantum size particles known as quanta. It further explores characteristics of quantum particles and their entanglement as special way of interaction at a distance.

Technologies like cryptography are the first and more advanced examples of quantum mechanics effects in use. In order to perform cryptographic tasks and enhance cryptographic systems quantum effects are leveraged and we already have first commercial Quantum key distribution (QKD) products available. Quantum key distribution is the most known and most studies example but is surely not the only one. Many more applications are emerging today and some of the examples include random number generators, delegated quantum computation and secure multiparty computation systems.

Quantum Cryptography takes the advantage from fairly negative set of rules from quantum physics. Quantum physics states that we are unable to measure the system without perturbing it. It is further impossible to accurately measure the position and the momentum of a particle simultaneously. It is also not possible to measure photon polarization in both vertical-horizontal and diagonal basis. It is possible to measure only one of the basis, after that we used the photon and cannot make another measurement. Quantum state in a system is impossible to duplicate.

It is hard to imagine that all this negative rules could be used to make something so simply functional like Quantum Key Distribution. In this work we will try to show how it is possible.

Quantum Cryptography is based on standard cryptography principles which are enhanced by usage of Quantum key distribution system. Quantum key distribution technique enables Quantum Cryptography by employing basic quantum mechanics principles listed above.

On the other side, Quantum Cryptography today is trying to examine and possibly take advantage of other quantum mechanics limitations. This includes the impossibility of quantum bit commitment, the issue with quantum rewinding and the definition of quantum security models for classical primitives.

Modern cryptology needs to be enhanced in a way that prevents future quantum computers or similar future calculation systems to break current crypto systems.

As we will have the chance to see in the next chapter, current crypto system are mostly based on prime integer factorization or similar mathematical problem with no known efficient solution. No known efficient solution is good enough for today's systems as todays computer

systems need huge number of calculation steps (CPU cycles) to calculate one prime number out of factorized two big primes.

Creation of quantum computers that can get to the result of that calculation in dramatically decreased number of steps will enable them to break current popular RSA or similar crypto algorithms in the time shorter that the key life time.

Today Quantum Cryptology's most developed application is surely Quantum Key Distribution. Quantum Key Distribution is making the enhancement to crypto key distribution systems in a way that solves the issues mentioned above. Quantum Cryptology principle is mostly based on quantum mechanics rule which defines that is impossible to take a measurement of a quantum system state without perturbing that system. There is an exception when the quantum state is compatible with the measurement but we will see further in this work that that's the reason behind long key size generation in exchange process.

II. Quantum Cryptography

A. New Technique

Quantum cryptography as a new technique of securing communication channels is not using some new kind of advanced mathematic algorithm to make keys that are impossible to inverse engineer like asymmetric encryption is trying to do. Quantum cryptography is rather a new technique of exchanging secret keys in a way that makes it impossible to misuse those keys from reading secure messages. When exchanged using quantum key distribution, secret keys will be used with current symmetric encryption and current communication links to encrypt the data.

Quantum cryptography uses photons to transmit secret key to a receiver using an optic communication channel. The mechanism is not only transmitting the key using photon polarization but the process of sending polarized photons is actually the process which sends and, in the same time, generates the key in that process.

The whole process of generating key, using quantum mechanics characteristics on a photon, is making the quantum cryptography work. The communication channel is actually not really quantum, it's basically normal optical line. Photons as information qubits are only quantum pieces of quantum crypto puzzle.

To be able to go in deep with quantum cryptography we will shortly list modern cryptology types used today.

B. Types of Cryptography

Cryptography can be categorized as:

- Symmetric Cryptography
- Asymmetric Cryptography

Symmetric Key Cryptography is sometimes known as Secret Key Cryptography. Main characteristic of this type of cryptography is the same key usage in encryption of data, and the decryption of that same data. Every change in the secret key will cause data decryption failure.

Asymmetric Key Cryptography is known as Public Key Cryptography. Main characteristic of this type of cryptography is usage of two sets of keys which are generated for the process. One key is public and other is private key. Public key encrypts the data and we can only decrypt that data using appropriate private key. The best part of asymmetric cryptography is that is giving us a technique to share encrypted data and enable the receiver to decrypt that data without the need of sending the decryption key across unsecured network.

It is a magic process in which you share public key with the whole world and every sender can encrypt the data that it is sending to you with your public key. You will then be the only one in the world to have the private key that can decrypt that message and that key was never sent to anybody.

The disadvantage of Public Key Cryptography is in the situation where you lost private key or it leaked, or somebody used a quantum computer to brute force your key. In that moment you will have to generate a new pair of public and private keys to be able to continue secure message sending.

C. How Asymmetric Key Cryptography works

From technical perspective, every cryptographic algorithm in asymmetric key cryptography is based on mathematical problem with no known efficient solution. Some of the most common examples are integer factorization, elliptic curve relationships or discrete logarithm usage. The base of the technical functionality is comprised of easy technique for a public and private key pair generation and their usage for encryption and decryption alternately. The main strength is in highly mathematically/computationally complicated way to calculate the private key from its corresponding public key.

That enables the system to publish the public key without affecting security. Security then depends on keeping the private key secure.

III. Why a New Cryptography System?

A. Symmetric Cryptography Issues

There are few major issues with symmetric encryption that are becoming main motivators for scientists to investigate the possibilities of a better encryption system.

The major issue with traditional symmetric cryptography is the secret key which is both encrypting and decrypting the message. If somebody else than sender and receiver comes into possession of that secret key, it means that he could snoop on private communication by decrypting messages between trusted parties.

It usually doesn't stop there. When somebody, except sender and receiver, has the secret key, that device or person is able not only to read the message but also alter the content without trusted parties knowing about the

changes. He is able to decrypt the message, change the content, encrypt again and forward it towards the receiver.

Second issue with symmetric crypto is in selecting the secret key properly. What would be the best mechanism to generate and then decide if the secret key selected is secure enough so that nobody on the way could guess it or brute force it in limited time-frame.

One more issue with the secret key is the mechanism of distributing the key to the receiver. Taking the facts that sender will generate the key, use the key to encrypt the message, taking into account that we are looking at symmetric system, the same key would need to be available at receiver side in order for him to be able to decrypt and read the content of the message. If sender is in Croatia and receiver is maybe in Sri Lanka. It is easy to see that the communication with which the key will be send also needs to be secure. This can easily be seen as catch 21.

In order to secure the communication channel, used to exchange secret keys, asymmetric encryption is used. Usage of asymmetric encryption, like described in previous section, provides, to date, secure technique of encryption without the need of sending the private key (used for decryption) to receiver.

B. Asymmetric Cryptography Possible Future Issues

Asymmetric crypto is still considered secure so it is not here listed as another issue which justifies the need for new cryptography mechanism. In this case the issue is in increasing computer calculation speed. Today's supercomputers will still need years to generate the right private key from public key. Giving the fact that Moore's law is still more or less right in the statement that computers CPU number of transistor will double every 18 months, it is clear that few years to break asymmetric key can easily become few days or even few minutes in near future.

If we start to think of new cryptology methods at that time, it will surely be too late to bring bank systems and similar secure communication dependent systems back online in time.

In this section after listing all the issues and issues that are on the horizon, we can clearly see why we need quantum cryptology. It is clear that all issues above describe problem with keys in current cryptographic mechanisms and their security in transmission.

Quantum cryptography solves exactly that piece of cryptography using basic quantum mechanics features.

IV. QUANTUM KEY DISTRIBUTION

A. How Quantum Cryptography Key Distribution Works

Quantum cryptography actually does the magic only on key distribution part of cryptographic system. Every other part of this new cryptography mechanism is same as in cryptography techniques currently used. By using quantum particles which behave under rules of quantum mechanics, keys can be generated and transferred to receiver in completely safe way. Quantum mechanics principle which describes the base rule which is protecting the exchange of keys is Heisenberg's Uncertainty Principle.

Heisenberg's Uncertainty Principle states that it is impossible to make a measurement of speed and current position of some particle in the same time. It furthermore states that the state of observed particle will change if and when measured. This fairly negative axiom which says that measurement couldn't be done without perturbing the system is used in positive way in quantum key distribution.

It a real communication system it will mean that, if somebody or something tries to intercept photon-powered communication, that eavesdropper will need to squeeze photons through its polarization filter. As soon as it tries with wrong filter it will send forward the wrong photon. Sender and receiver will notice the disparity and interpret it as detection of interception. They will then restart the process of generating key.

B. Photon, and how it is used?

1) Photon

Smallest particle of light is a photon. It has three types of spins horizontal, vertical and diagonal which can be imagined as right to left polarization.

2) Polarization

Polarization is used to polarize a photon. Polarize the photon means to filter the particle through polarization filter in order to filter out unwanted types of spins. Photon has all three spin states at the same time. We can manipulate the spin of a photon by putting the filter on its path. Photon when passed through the polarization filter has particular spin that filter lets through.

3) Spin

The Spin is usually the most complicated property to describe. It is a property of some elementary particle like electron and photon. When they move through a magnetic field, they will be deflected like they have same properties of little magnets.

If we take classical world for example, a charged, spinning object has magnetic properties. Elementary particles like photons or electrons have similar properties. We know that by the rules of quantum mechanics that elementary particles cannot spin. Regardless the inability to spin, physicists named the elementary particle magnetic properties "spin". It can be a bit misleading but it helps to learn the fact that photon will be deflected by magnetic field. The photon's spin does not change and it can be manifested in two possible orientations.

4) LED

LEDs - light emitting diodes are used to create photons in most quantum-optics experiments. LEDs are creating unpolarized (real-world) light.

Modern technology advanced and today is possible to use LEDs as source of single photon. In this way string of photons is created which will then be used in quantum channel for key generation and distribution in quantum key distribution process between sender and receiver.

Normal optic networking devices use LED light sources which are creating photon bursts instead of individual photons. In quantum cryptography one single photon at a time needs to be sent in order to have the chance to polarize it on the entrance into optic channel and check the polarization on the exit side.

C. Data Transmission Using Photons

Most technically challenging part of data transmission encoded in individual photon is the technique to read the encoded bit of data out from each photon. How it is possible to read the bit encoded in the photon when the very essence of quantum physics is making the measurement of quantum state impossible without perturbations. There is an exception.

We attach one bit of data to each photon by polarizing each individual photon. Polarizing photons is done by filtering photon through polarization filter.

Polarized photon is send across quantum channel towards receiver on other side.

Heisenberg's Uncertainty Principle come into the experiment with the rule that photon, when polarized, cannot be measured again because the measurement will change its state (ratio between different spins).

Fortunately, there is an exception in Uncertainty Principle which enables the measurement but only in special cases when measurement of the photon spin properties is done with a device (filter in this case) whose quantum state is compatible with measured particle.

In a case when photons vertical spin is measured with diagonal filter, photon will be absorbed by the filter or the filter will change photon's spin properties. By changing the properties photon will pass through the filter but it will get diagonal spin. In both cases information which was sent from sender is lost on receiver side.

The only way to read photons currently encoded bit/spin is to pass it through the right kind of filter. If polarized with diagonal polarization (X) the only way to read this spin is to pass the photon through diagonal (X) filter.

If vertical filter (+) is used in an attempt to read that photon polarization, photon will get absorbed or it will change the spin and get different polarization as it did on the source side.

List of spin that we can produce when different polarization filter is used:

- Linear Polarization (+)
- Horizontal Spin (–)
- Vertical Spin (|)
- Diagonal Polarization (X)
- Diagonal Spin to the left (\)
- Diagonal Spin to the right (/)Tablica 1

D. Key Generation or Key Distribution

The technique of data transmission using photons in order to generate a secure key at quantum level is described in last section. This process is usually referred as Quantum Key Distribution process or shortly as Quantum Cryptography. Key Distribution/Generation using photon properties like spin is solved by Quantum Key Distribution protocols allowing the exchange of a crypto key with - laws of physics guaranteed - security. When finally generated, this key is absolutely secure and can be further used with all sorts of conventional crypto algorithms.

Quantum Key Distribution protocols that are commonly mentioned and mostly in use in today's implementations are BB84 protocol and SARG protocol. BB84 is the first one invented and it is still commonly used. It is the first one to be described in the papers like this one which are trying to describe how Quantum key exchange works. SARG was created later as an enhancement which brought a different way of key sifting technique which is described later in this paper.

1) Attaching Information bit on the photon – Key Exchange

Key Exchange phase, sometimes referred as Raw Key Exchange giving the anticipation of future need for Key Sifting is a technique equal for both listed Quantum Key Distribution protocols BB84 and SARG. To be able to transfer numeric (binary) information across quantum channel we need to apply specific encoding to different photon states. For Example, encoding will be applied as in the Table 1 below making different photon spin carry different binary value.

Table 1- Encoding of Photon States

SPIN	VALUE
HORIZONTAL SPIN(–)	0
VERTICAL SPIN(|)	1
LEFT DIAGONAL SPIN(\)	0
RIGHT DIAGONAL SPIN(/)	1

In the process of key distribution, first step is for sender to apply polarization on sent photons and take a note of applied polarizations. For this to be an example, we will take the Table 2 below as the list of sent photons with their polarization information listed.

Applied Polarization	X	+	X	X	X	X	X	+	X	+	+	+	+	+	X	+	X	+	+	+
Spin	\	|	\	\	\	\	\	|	\	-	|	|	|	-	\	|	\	-	|	|
Value	0	1	0	0	0	0	0	1	0	0	1	1	1	0	0	1	0	0	1	1

Sender sent binary data:

0 1 0 0 0 0 0 1 0 0 1 1 1 0 0 1 0 0 1 1

If the system will work with integers this data can be formatted in integer format:

Table 3- Binary to Decimal Conversion Table

Binary	**0 1 0 0 0 0 0 1 0 0 1 1 1 0 0 1 0 0 1 1**
Decimal	267155

Sender sent a key 267155 but it is just the start of the key generation process in which this key will be transformed from firstly sent group of bits to the real generated and secured key.

2) Reading Information bit on the receiver side

The question arises on how can we use above described properties of photon and still be able to actually read it on the receiver side. In the above step, photons with the information attached to them were sent to the receiver side.

The next step will describe how quantum key distribution, and with that the whole quantum cryptography, works. While sending, a list was made, list containing each sent photon, sent from sender to receiver and polarized with specific spin (encoded a bit of information on each photon).

In optimal case, when sender sends a photon with vertical spin and receiver also applies vertical filter in the time of photon arrival, they will successfully transfer a bit of data using quantum particle (photon). In a less optimal case when a photon with vertical spin is measured with diagonal filter the outcome will be photon with diagonal spin or no photon at all. The latter will happen if the photon is absorbed by the filter. In this case, transferred bit of data will later get dumped in the phase of key sifting or key verification.

3) Key Verification – Sifting Key Process

Key sifting phase or Key verification is a technique made differently with listed Quantum Key Distribution protocols BB84 and SARG.

In the last section, a less optimal case when a photon with vertical spin is measured with diagonal filter was described. The outcome of that photon, which is sent with vertical spin, measurement done with diagonal spin will give to the receiver a photon with diagonal spin or no photon at all.

Key verification come into play now and it is usually referred as **Key Sifting process**.

In BB84 protocol receiver will communicate with sender and give him the list of applied filters for every received photon. Sender will analyze that list and respond with a shorter list back. That list is made by leaving out the instances where sender and receiver used different filters in single photon transfer.

In SARG protocol receiver will give to sender the list of results he produced from each received photons without sending filter orientation used (difference from BB84). Sender then needs to use that list plus his applied polarization while sending to deduce the orientation of the filter used by receiver. Sender then unveils to the receiver for which transfers he is able to deduce the polarization. Sender and receiver will discard all other cases.

In this whole process, sending of polarized photons is done through special line of optical fiber cable.

If we take BB84 for example, Key sifting process is done by receiver sending to the sender only the list of applied polarization in each photon transfer. Receiver does not send the spin or the value he got as a result from that transfer. Having that in mind, it is clear that communication channel for key verification must not be a quantum channel but rather a normal communication channel with not even the need to have encryption applied. Receiver and sender are exchanging the data that is only locally significant to their process of deducing in which steps they succeeded to send one polarized photon and read the photon one bit of information on the other side.

In the end of Key Sifting process, taking that no eavesdropping happened, both sides will be in possession of exactly the same cryptographic key. The key after sifting process will be half of the original raw key length when BB84 is used or a quarter with SARG. Other bits will be discarded in the sifting process.

E. Communication Interception – Key Distillation

1) Interception Detection

If a malicious third party wants to intercept the communication between two sides, in order to read the information encoded, he will have to randomly apply polarization on transmitted photons. If polarization is done, this third party will need to forward photons to the original sender. As it is not possible to guess all polarizations correctly, when sender and receiver validate the polarizations, receiver will not be able to decrypt data, interception of communication is detected.

On average, eavesdropper which is trying to intercept photons will use wrong filter polarization in half of the cases. By doing this, state of those photons will be changed making errors in the raw key exchange by the emitter and receiver.

It is basically the same thing which happens if receiver uses wrong filter while trying to read photon polarization or when the same wrong filter is used by an eavesdropper.[1]

[1] If we look at quantum channel, Observer who wants to read a bit of data prom polarized photon is unable to do that without using polarization filter of that photon. By doing that, all photons that he tries to read with wrong filter will be dropped in key verification process as they will appear different on sender and receiver side. If he applies the right filter he will succeed to read that one bit of that. Observers issue is in the key generation and verification process itself. After reading the bits from photons, he will still be unaware of which bits will get dropped by sender and receiver and which bits will get accepted and become a part of quantum crypto generated key.

In both cases, to prove the integrity of the key, it is enough that sender and receiver are checking for the errors in the sequence or raw key exchange.

Some other thing can cause raw key exchange errors, not only eavesdropping. Hardware component issues and imperfections, environmental causes to the quantum channel can also cause photon loss or polarization change. All those errors are categorized as a possible eavesdropper detection and are filtered out in key sifting. To be sure how much information eavesdropper could have gathered in the process, key distillation is used.

2) Key Distillation

When we have a sifted key, to remove errors and information that an eavesdropper could have gained, sifted key must be processed again. The key after key distillation will be secured enough to be used as secret key.

For example, for all the photons, for which eavesdropper used right polarization filter and for which receiver also used right polarization filter, we do not have a detected communication interception. Here Key Distillation comes into play.

First out of two steps is to correct all possible errors in the key which is done using a classical error correction protocol. In this step we will have an output of error rate which happened. This error rate estimate we can calculate the amount of information the eavesdropper could have about the key.

Second step is privacy amplification which will use compression on the key to squeeze the information of the eavesdropper. The compression factor depends proportionately on the error rate.

V. Real-life Implementations

Key advantage of Quantum Key Distribution over other new techniques in communication systems is that it can use existing optical infrastructure. New devices making Quantum Key Distribution work need to be implemented and are already implemented in some high end security solution IT systems. Existing fiber optic cable infrastructure is adequate for performing Quantum Key Distribution with few existing solutions which helped make the whole implementations possible at this point of time.

From different sources it is possible to gather vague information which shows that this new technology already has several companies offering solutions in form of hardware devices for single photon detection which makes QKD technique possible.

Quintessence Labs and Toshiba Research[2] are two of them that offer devices at this point in time. Technology currently can cost around 150K $ for implementation of one link. Devices are fairly big because they need to contain parts like attenuated laser, detector and other electronics.

Giving those facts, banks and government are currently most likely users and information on who is using it is not publicly available. This is the first proof that security through obscurity is taking place even when quantum physics is securing the system.

Current research is lead by University of Geneva together with NASA. They are focusing on a method called the Ekert Protocol, method where encryption key is transmitted between the photon emitters and detectors by means of quantum teleportation. This type of transfer is extending the maximum distance of a single link through which individual photon is able to travel.

This is actually the biggest issues which all current QKD solutions are facing. It is in the photons ability to travel for a limited distance before it is likely to be absorbed by the optic cable. Photon generated at sender side can only travel for approximately 100km before being absorbed by the optic cable.

Robert Young of Lancaster University founded Quantum Base, a firm which, with Prof. Young and his colleague's expertise, designed a technique for usage of quantum filters for third parties interception attempts detection. They are also working on equipment miniaturization which will consequently cause significant cost reduction in the future making the technology feasible for numerous implementations.

In an article on the next stage in quantum key distribution[3], Prof. Young stated that current technology development at their labs will get results within two years, giving to the world a functional QKD system with reduced dimensions and reduced cost.

It states further that approximately 20 years will be needed for wide deployment of this technology, quenching critics who are still saying that QKD is an unfeasible technology.

VI. Conclusion

Privacy and data security is of utmost importance to people communicating across networks. With quantum cryptography, secure transmission of data is guaranteed, and chances of it being intercepted and altered are close to none. QKD technology has been implemented in some high importance systems like banking and government. More feasible and economically acceptable solutions using QKD is still under deep research before being widely implemented.

The security solutions offered by Quantum Key Distribution systems are providing a next generation protection of data on the telecommunications networks against the next generation threats these systems face. Computer increasing computation power and ability to

[2] http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution/Toshiba-QKD-system/

[3] Computerweekly.com - The next stage in quantum key distribution - http://www.computerweekly.com/feature/The-next-stage-in-quantum-key-distribution

brute-force ever more complex cryptographic mathematical functions is threatening current networking systems security.

At some point in the near future QKD hardware devices enabling its wide usage will get to market. The prospects about security of currently deployed crypto systems will have big impact on development of these devices. It is surely justified and reasonable investing huge efforts into developing QKD systems who will be the only remedy standing in between our secret data and unwanted observers in the moment when one of quantum computer implementations becomes available and capable to calculate our private keys in hours.

There are actually no valid reasons why not to implement system like this once they get finally out.

VII. Appendix

A. Asymmetric Key Cryptography Example

1) Modular Arithmetic

In modular mathematics numbers are going until the modulus. They are never bigger than the modulus. Imagine the clock for example, clock in a great example of "mod 12". There are no numbers after 12. There is no 13, 14, 15. After 12 you start back at 1.

Calculating the modulus is dividing the number with modulus and taking the remainder.

17 mod 3 = (3 * 5 + 2)mod 3 = 2

The reason to use modular mathematics is to get manageable numbers even if we make really complex stuff like high-end encryption. The thing is that you can always cut the number if it is bigger that the modulus and keep thing manageable.

Look at this one:

22^17 mod 77 = 662499529219459433152512 mod 77
= 22

2) Successive Squaring

Successive squaring helps computers to calculate integer powers of a number more quickly. It does that by diminishing the number of steps it takes to calculate it and thus diminishing processing cycles needed to calculate integer to the power of a number.

So if you take a fairly basic example of 3^14 we can see that by normal means we would need 14 multiplication steps to get the result:

3^14 = 4.782.969

3^14 = 3 * 3 * 3 * 3 * 3 * 3 * 3 * 3 * 3 * 3 * 3 * 3 * 3 * 3

Successive squaring is making the process shorter by squaring x so many times until the current power of x exceeds y:

We take 13 which is 1110 in binary:
1110 = 14 = 8 + 4 + 2
and we make the next steps.

Calculation example:

- 3^1 = 3 we don't use this one as it is 0 in binary number 14 (1110), we take the next three:
- 3^2 = 9
- 3^4 = 9^2 = 81
- 3^8 = 81^2 = 6561
- 9 * 81 * 6561 = 4782969

So we calculated the thing in 4 steps and not in 13, it's better and faster indeed.

3) Diffie Helman

This process is really ingenious. Two computers are exchanging plain text information between them and everyone can see what they are speaking about. After a while, both of the computers share a secret key called shared secret that they could use to encrypt future communication.

We can imagine a publicly known key that is composed of two prime numbers x and y. This key K(x,y) is a public key that everyone on the Internet knows. Sender and receiver are each calculating a secret number which will be used to encrypt the communication between each-other. They are using public key K(x,y) to calculate the shared secret key that needs not to be known to anyone else but them.

1. One of them comes up with two prime numbers x and y and tells it to the other. They are send in plain text so everybody can see those numbers crossing the network.
2. Sender picks a secret number a and calculates A = x^a mod y.
He then sends the result "A" to the receiver on other side.
3. Receiver does the same. He picks a secret number b and the computed number B in the same way, B = x^b mod y
and sends the result to sender.
4. Now, Sender received number B and receiver received number A. They calculate the secret key by doing this:
   a. Sender calculates secret S = B^a mod y.
   b. Receiver calculates secret S = A^b mod y.

This math is crazy. It enables both sender and receiver to generate the same secret key S by using values a and b which are newer sent across the network by using modulo exponents rules below:

(g^a mod p)^b mod p = g^a*b mod p

(g^b mod p)^a mod p = g^b*a mod p

VIII. REFERENCE

A. Science Work

[1] Bourennane, M., et al. "Experiments on long wavelength (1550nm)"plug and play" quantum cryptography systems." Optics Express 4.10 (1999): 383-387.

[2] Gisin, Nicolas, et al. "Quantum cryptography." *Reviews of modern physics* 74.1 (2002): 145.

[3] Bennett, Charles H., et al. "Experimental quantum cryptography." *Journal of cryptology* 5.1 (1992): 3-28.

[4] Bennett, Charles H. "Quantum cryptography using any two nonorthogonal states." *Physical Review Letters* 68.21 (1992): 3121.

[5] Bennett, Charles H. "Quantum cryptography using any two nonorthogonal states." *Physical Review Letters* 68.21 (1992): 3121.

[6] Bennett, Charles H., Gilles Brassard, and N. David Mermin. "Quantum cryptography without Bell's theorem." *Physical Review Letters* 68.5 (1992): 557.

[7] Bennett, Charles H., Gilles Brassard, and N. David Mermin. "Quantum cryptography without Bell's theorem." *Physical Review Letters* 68.5 (1992): 557.

[8] Bienfang, J., et al. "Quantum key distribution with 1.25 Gbps clock synchronization." *Optics Express* 12.9 (2004): 2011-2016.

[9] Yuan, Zhiliang, and A. Shields. "Continuous operation of a one-way quantum key distribution system over installed telecom fibre." *Optics Express* 13.2 (2005): 660-665.

[10] Deutsch, David, et al. "Quantum privacy amplification and the security of quantum cryptography over noisy channels." *Physical review letters* 77.13 (1996): 2818.

[11] Sharbaf, Mehrdad S. "Quantum cryptography: a new generation of information technology security system." *Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on*. IEEE, 2009.

[12] Migdall, Alan, and Jonathan Dowling. Introduction to the Journal of Modern Optics Special Issue on Single-Photon: Detectors, Applications, and Measurement Methods. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD, 2004.

[13] Scarani, Valerio, and Christian Kurtsiefer. "The black paper of quantum cryptography: real implementation problems." *arXiv preprint arXiv:0906.4547* (2009).

[14] Jacobs, B. C., and J. D. Franson. "Quantum cryptography in free space." *Optics Letters* 21.22 (1996): 1854-1856.

[15] Yanofsky, Noson S., Mirco A. Mannucci, and Mirco A. Mannucci. *Quantum computing for computer scientists*. Vol. 20. Cambridge: Cambridge University Press, 2008.

B. Web Resources

[16] Gomes, Lee. "A Beautiful Mind from India is putting the Internet on Alert." Wall Street Journal Online. 4 Nov. 2002. URL: http://www.iitbombay.org/misc/press/wsj100402.htm (13 Jan. 2003).

[17] Gottesman, Daniel & Lo, Hoi-Kwong. "From Quantum Cheating to Quantum Security." Physics Today. Nov. 2000. URL: http://www.aip.org/web2/aiphome/pt/vol-53/iss-11/p22.html (29 Oct. 2002).

[18] Reuters Group PLC. "Keys for Deciphering Code Sent Record Distance." 2 Oct. 2002. Technology News – Reuters. URL: http://emoglen.law.columbia.edu/CPC/archive/crypto/news_article%5BStoryID=1526934%5D.html (13 Jan. 2003).

[19] Junnarkar, Sandeep. "Noisy Light is New Key to Encryption." CNET News Online. 15 Nov. 2002. URL: http://news.com.com/2100-1001-965957.html?tag=fd_top (10 Dec. 2002).

[20] Lo, Hoi-Kwong. "Quantum Cryptology." Hewlett-Packard Labs. 17 Nov. 1997. URL: http://fog.hpl.external.hp.com/techreports/97/HPL-97-151.pdf (12 Dec. 2002).

[21] Meystre, Pierre. "Future Issues in Theoretical Quantum Cryptography." 15 Feb 1995. URL: http://www.aro.army.mil/phys/proceed.htm#Future%20Issues (10 Nov. 2002).

[22] Thomson ISI. "Quantum Privacy Amplification and the Security of Quantum

[23] Cryptography Over Noisy Channels." 31 May 2001. URL: http://www.esitopics.com/enc/interviews/Dr-David-Deutsch.html (17 Dec. 2002).

[24] Walton, Z., et al. "Performance of Photon-Pair Quantum Key Distribution Systems." URL: http://arxiv.org/PS_cache/quant-ph/pdf/0103/0103145.pdf (10 Dec. 2002).

[25] http://www.bbn.com/networking/quantumcryptography.html (21 Oct. 2002).

[26] DeJesus, Edmund X. "Quantum Leap." Information Security Online. Aug. 2001. URL: http://www.infosecuritymag.com/articles/august01/features_cryptо.shtml (10 Nov. 2002).

[27] Dwyer, Jeffrey. "Quantum Cryptography." URL: http://www.cyberbeach.net/~jdwyer/quantum_crypto/quantum1.htm (23 Oct. 2002).

[28] Fisher, Dennis. "Turning the Key on Data." eWEEK Magazine 18 Nov. 2002: 89

[29] Reuters Group PLC. "Notre Dame Math Whiz Cracks Certicom Code Contest."

[30] The Mercury News Online. 6 Nov. 2002. URL: http://zdnet.com.com/2100-1104-964798.html (10 Dec. 2002).