Proposed New Quantum Cryptography System Using Quantum Description techniques for Generated Curves

A. Dr. Hala Bahjat AbdulWahab[1] , **B. Dr.Abdul Monem S. Rahma** [2]
And C. Dr.Hilal M. Yousif Al-Bayatti[2]
[1]Computer Science Department, University of Technology, Baghdad, Iraq,
[2]Computer Science Department, University of Technology, Baghdad, Iraq,
And [2] University of Technology, Kingdom of Bahrain.

Abstract:-*The main goal of this paper is combining the curve security methods with quantum cryptography concepts in order to increase the capability of quantum cryptography methods that used for key distribution and increase the randomness for quantum cryptography protocols. This paper produced a new approach depend on the generate curve and descript this curve by using quantum cryptography concepts, the curve description will be sent to the other party to agree about the key depending on the suggested protocol that produced in this paper. Curve security involves the process of protecting the shape of the curve from reproduced and as a result, protecting the whole document from being regenerated by any counterfeiting person. On the other hand, the strength of quantum cryptography is based on the quantum behavior of the photons when it is measured in a different basis; it is resulted in a random value and information destruction. The combination of the two cryptography direction guaranteed that the resulted key have the required randomness. The key is tested using the different randomness tests, which prove the high randomness of the keys that are resulted with this approach.*

Keywords: Curve fitting, applied numerical analysis, quantum cryptography, key distribution, randomness tests.

1 Introduction

Every few years, computer security has to re-invent itself. New technologies and new application bring new threats, and force us to invent new protection mechanisms. One of the problems of the security systems is the key distribution. The secret keys are needed to be exchanged among the communicated parties safely; otherwise, the encrypted data will be in threats. One of the approaches of security systems depends on curve fitting. The forms produced by graphic systems are much harder to counterfeit, especially when the counterfeiter has no information about the design of the system .On the other hand, quantum cryptography is the promised approach of cryptography. It is exploit the properties of quantum mechanics to implement cryptography systems and protocols. There are many suggested quantum cryptography protocols such as The BB84 protocol, which invented in 1984 by Charles Bennett of IBM Research and Gilles Brassard of the University of Montreal [1]. In this work, a key distribution protocol is suggested which is used the concepts of curve fitting to generate a key then a quantum description approach is suggested to describe this curve and implement the required key. Therefore, a quantum information is transmitted between the two parties instead of traditional information [2] , in this paper produce a new quantum cryptography system with simple implementation to explain the proposed method .

2 Key Distribution

Cryptography is the art of rendering information exchanged between two parties unintelligible to any unauthorized person. Although it is an old science, its scope of applications remained mainly restricted to military and diplomatic purposes until the development of electronic and optical telecommunications [3] .

The key distribution problem is encountered by any two entities that wish to communicate using a cryptographically protected channel. If Alice and Bob want to use a traditional block cipher and message authentication code to protect their communications, they need to agree upon a shared key to use. This problem is currently solved using public-key cryptography. Alice and Bob each generate a public-private key pair and register their public key with a Certification Authority (CA). The CA then creates a certificate for each of them and distributes the certificate to the other party. Alice and Bob can now use their private keys and the public key contained in each other's certificate to agree upon a shared symmetric key to be used in the block cipher or message authentication code. A number of specific algorithms and protocols exist for doing this. These include Diffie-Hellman key agreement. Public-key cryptography is currently secure. Using key sizes currently in use, it appears infeasible for any attacker to be able to obtain a user's private key solely from his/her public key, which is what would typically be required to break these schemes. However, in theory, if sufficient

computing power existed or if a solution is found to the mathematical problem upon which the algorithm is based, then these schemes could be vulnerable to attack. There is no reason to believe that either of these outcomes are likely. However, since the security provided is computational, rather than absolute, some are searching for alternative approaches. Quantum cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of physics. This key can then be used with conventional cryptographic algorithms. One may thus claim, with some merit, that "quantum key distribution" may be a better name for quantum cryptography. Contrary to what one could expect, the basic principle of quantum cryptography is quite straightforward. It exploits the fact that according to quantum physics, the mere fact of observing a quantum object perturbs it in an irreparable way. If one encodes the value of a digital bit on a single quantum object, its interception will necessarily translate into a perturbation, because the eavesdropper is forced to observe it. This perturbation causes errors in the sequence of bits exchanged by the sender and recipient. By checking for the presence of such errors, the two parties can verify whether their key was intercepted or not. It is important to stress that since this verification takes place after the exchange of bits, one finds out a posteriori whether the communication was eavesdropped or not. That is why this technology is used to exchange key and not valuable information. Once the key is validated, it can be used to encrypt data. Quantum physics allows proving that interception of the key without perturbation is impossible [4].

3 Quantum Cryptography

The field of quantum cryptography was pioneered by Wiesner around 1970, by exploiting the use of quantum physics to accomplish the quantum computing and the quantum cryptography. The strength of this type of cryptography is based on the quantum behavior of the photons when it is measured in a different basis; it is resulted in a random value and information destruction [5].

Quantum Cryptograph features

- Ability to detect eavesdropping.
- Detection works only after the information was taken.
- Usually requires classical information channel for effective communication.

In figure (1) shown the quantum cryptography concepts.

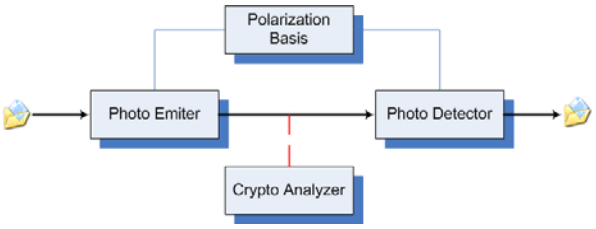


Figure (1): The quantum cryptography concepts.

3.1 Quantum Cryptography Protocols

Although several quantum cryptography protocols exist, a single quantum cryptography protocol will be discussed in this paper. This is sufficient to illustrate the principle of quantum cryptography. The BB84 protocol was the first to be invented in 1984 by Charles Bennett of IBM Research and Gilles Brassard of the University of Montreal. In spite of this, it is still widely used and has become a de facto standard. An emitter and a receiver can implement it by exchanging single-photons, whose polarization states are used to encode bit values over an optical fiber. This fiber, and the transmission equipment, is called the quantum channel. They use four different polarization states and agree, for example, that a 0-bit value can be encoded *either* as a horizontal state or as a –45° diagonal one. For a 1-bit value, they will use *either* a vertical state or a +45° diagonal one.

- For each bit, the emitter sends a photon whose polarization is randomly selected among the four states. He records the orientation in a list.
- The photon is sent along the quantum channel.
- For each incoming photon, the receiver randomly chooses the orientation – horizontal or diagonal – of a filter allowing distinguishing between two polarization states. He records these orientations, as well as the outcome of the detections – photon deflected to the right or the left.

4 Curves Security Techniques Development.

Curve security involves the process of protecting the shape of the curve from reproduced and as a result, protecting the whole document from being regenerated by any counterfeiting person. The shape of the curve is based on a set of control points that fundamentally describe its properties and its curvature. Thus if the intruder knows the set of control points, it may lead to discover the shape of the curves with a trial and error on the methods or algorithms that were originally used to produce the curve. In this paper B-spline curve algorithm is used as efficient example for curves generating. In the following an algorithm to generate B-Spline curve [6].

Algorithm-1: B-spline curve generation

Input: Given control points n+1 $v_i = (x_i, y_i), i = 0, \cdots, n$

Output: Interpolate the get new values for each of x and y to draw curve points.

Process:

Step1: Set $v_{-1} = v_{-2} = v_0$ and set $v_{n+1} = v_{n+2} = v_n$

Step2: For i=0 to n-1

Step3: For u=0 to 1 step 0.01

Step4:

$$X = (1-u)^3/6x_{i-1} + (3u^3 - 6u^2 + 4)/6x_i + (-3u^3 + 3u^2 + 3u + 1)/6x_{i+1} + u^3/6x_{i+2}$$

$$Y = (1-u)^3/6y_{i-1} + (3u^3 - 6u^2 + 4)/6y_i + (-3u^3 + 3u^2 + 3u + 1)/6y_{i+1} + u^3/6y_{i+2}$$

Step5: Plot(X,Y).

Step6: Next u

Step7: Next i

Step8: End.

5 Using curve generation technique in key distribution system.

A description of quantum protocol for key generation and distribution is presented in this section using curve-fitting techniques. The key is generated as steps on the curve. These steps are coupled with equalized period. Steps will be represented as the quantum photons polarized with different directions [7]. As an example, consider theB-spline curve shown in figure (2), Alice and Bob agreed previously about the value of time steps t and the number of the time steps N as parameters equal to the code refer to the quantum photons polarized with different directions schema that used. Then Alice will transform the curve to be as a sequence of photons of different polarizations. Therefore, the sequence of the photons will be as in figure (3).

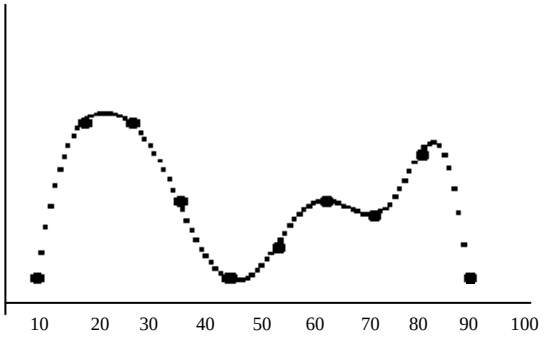


Figure (2-a): B-Spline curve generating according algoritm-1.

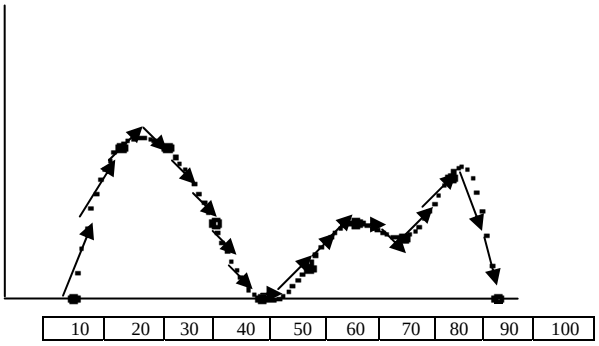


Figure (2-b) : B-Spline curve and its quantum description

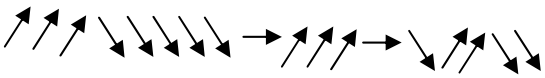


Figure (3): the sequence of the photons resulted from the quantum description of the curve.

5.1 Base Protocol

The protocol of key sending process will be as following steps: [7]

- Alice and Bob agreed previously about the polarized angles that considered as 0's and the polarized angles that are considered to be 1's (for example ↑ ↘ are considered to be 0's and are considered to be 1's) .
- Alice and Bob agreed previously about the number of photons between each two control points and the number of the control pointes .
- Alice invents a curve.
- Alice generates the key sequence as described in the previous section.
- Alice sends each photon with its specific direction.
- Bob will receive photons and measure them with different polarization.
- If Bob receive the photon properly, he will add this photon to the key.
- Bob will send the position of the properly received photons to Alice.
- Alice will send an agree message to Bob if the number of the received photons greater than or equals the required key length, otherwise they will repeat the steps 3 to 7 until the key is completed.

5.1.1 Example:

In this section simple example that help to explain the idea that produce in base protocol for quantum description for B_splin curve, and impelement the base protocol on the curve that shown in figure(2) .

- Bob will send the positions of the properly polarized photons
  1 3 4 6 7 9 10 11 12 14 15 16 18
- If the number of the properly received photons greater than or equals the length of the required key the Alice will send an agree message to Bob, otherwise more photons will be sent and the steps 3 to 7 are repeated until the whole key is completed.
- The Key will be as follows:
  0011110001001…….

5.1.2 The Key Randomness Tests

The resulted key that obtained in section 5.1.1 in order is test the randomness for the base protocol output. The results as follows[8]:

1- FREQUENCY TEST

Pass value 0.067 with freedom degree "1"
must be <=3.84

2- ***RUN TEST***

Pass value TO= 0.615 with freedom degree " 2 "
must be <= 5.702
Pass value T1 =2.982 with freedom degree " 3 "
must be <= 7.531

3- POKER TEST

Pass value 3.267 with freedom degree " 5 "
must be <=11.1

4- ***SERIAL TEST***

Pass value 0.833 with freedom degree "3 "
must be <= 7.81

5- ***AUTO CORRELSTION TEST***

Shift No. 1>--> Pass value 0.000
Shift No. 2>--> Pass value 0.077
Shift No. 3>--> Pass value 0.000
Shift No. 4>--> Pass value 0.818
Shift No. 5>--> Pass value 0.000
Shift No. 6>--> Pass value 0.111
Shift No. 7>--> Pass value 0.500
Shift No. 8>--> Pass value 0.143
Shift No. 9>--> Pass value 0.667
Shift No. 10>--> Pass value 0.200
With freedom degree "1" must be <= 3.84

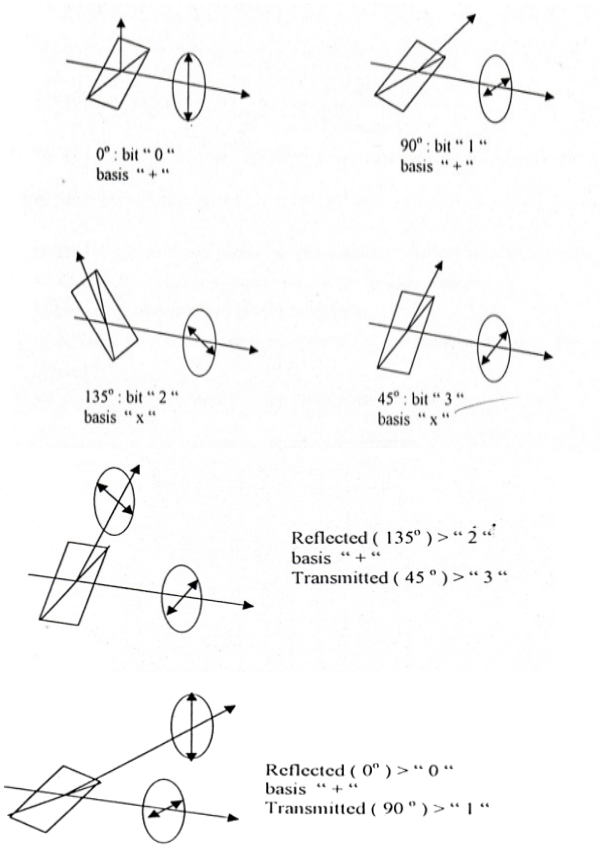
6 Modification on Base Protocol.

The proposed modification on base protocol is differs in the *polarized angles that used in quantum description are encoded in four different"basis", (0,1,2,3), instant of (0,1)* and the output description used *polarized states* angles according the table(1).

The protocol as in the following stages[9]***:***

Stages 1: Alice sends random "states" (0,1,2,3) encoded in four different "basis"

Stages 2: Bob randomly chooses either the (+) or the (x) basis and records the transmitted and reflected photons (giving "1 "or "0" if basis ok) .



Stage 3: Bob announces openly his choice of basis (but not the result!) and Alice answers (ok) or (no). States with different basis are discarded.

Stage 4: The remaining state gives the key.

The states assignment for these bullies is shown in the table below:

polarization states	Assignment state
0	0
45	1
90	2
135	3

Table (1): polarization states that used in the proposed protocol.

Stage 5: manipulation ciphers transfer plaintext into cipher text by altering the actual state pattern of each character through the use of a logical operator (#). The (#) has the following truth tables in figure (4):-

# 0	0	1	2	3
0	3	2	1	0
1	2	3	0	1
2	1	0	3	2
3	0	1	2	3

#1	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

# 2	0	1	2	3
0	2	3	0	1
1	3	2	1	0
2	0	1	2	3
3	1	0	3	2

# 3	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

figure (4): 4- truth tables for(#) operator.

6.1 manipulation bits process [9].

In this paper produce new quantum cryptography system aim to use deception for curve generation as a tool in quantum description for polarization states that illustrated in (section 6), the proposed protocol help to increase the security and key space ,that make more robust on the intruder. In other hand, this new cryptography protocol required adds new manipulation bits process because the traditional binary process (XOR) work on (0, 1) bits only. where the proposed second modification protocol (see5.2) used different truth table for manipulation bits process work on 4-states (0,1,2,3) , In this paper, symbol # refer to the operator that execute this process use truth tables that shown in figure (4).

Example-1:

In the following simple example shown the manipulation bits process with four states of bits (0,1,2,3) and execute XOR process two bits (0,1) , with (0,1,2,3), truth table (#1) is used:

001101	(plain text)	
132013	(key)	**(Encryption process)**
213212	ciphertext	

Note: the key(132013) in above example represent the index truth table (#1) . (i.e the first bit in plaintext (0)as row XOR with (1) as column in truth table (#1) and the output is obtained from the conjunction which equal(2), and so on.

213212	ciphertext	
132013	(key)	(**Encryption process)**
001101	(plaintext)	

6.2 Generalization for manipulation bits process.

In this paper produce the method that combine fourth the truth table in each encryption process, by make the states(12,3,4)used as index for the tables and execute the same process that shown in example-1 , in the following example-2 illustrated The generalization manipulation process .

Massage:	**1110011010111**
Key:	0231011300102
Output:	2122232……

Note: key bits refere to index for the 4-turth table, (i.e 0 mean go to the #0 and perform the XOR (row,col) and the output according #1 is 2.

7 Proposed new approach to modify quantum cryptography system.

The proposed approach aim to combine between two protocols (base and modification protocol),that illustrated in section (5) ,the proposed quantum cryptography system work according the following steps:

1- ***Secret key***: Alice and Bob agreed previously about the secret key that consist from (curve generation algorithm (like B-spline), control points coordinates (x,y), and polizreed angles that used in base protocol where used (0,1) bits only for description (see section 5-1)).

2- Public keys: each Alice and Bob has public key s that represent as (control points, curve generation algorithm).

Note : the 4- tables must be secret between both Alice and Bob.

3- Sending Process:

- ***Alice want send massage to Bob***

  ❖ Alice used public key from Bob (Generate curve and represent using quantum description and porlized according the proposed protocol-2 (see 5 .2).

*****Encryption process:***

❖ Alice used two keys(the secret key represent as (0,1) and Bob public key represent as(0,1,2,3) , with plain text according the manipulation bits process, in the following simple example that shown the process:

Example for encryption process:

** Public key used as index refer to the 4-tables(#0,1,2,3) .

public key : 0231011300102
Secret key : 0011110001001
Massage: 1110011010111

Ciphertext: 2122232……

The cipher text sent in quantum obtical channel to Bob using polizerd using (four states).

4- Receiving Process:

Bob will receive photons and measure them with four states polarization.

- For each bit, the emitter sends a photon whose polarization used four states according second protocol, which represent the public key that Alice used. Bob records the orientation in a list.
- Received the cipher text from optical public channel.
- Bob used secret key and public key with ciphertext

*****decryption process:***

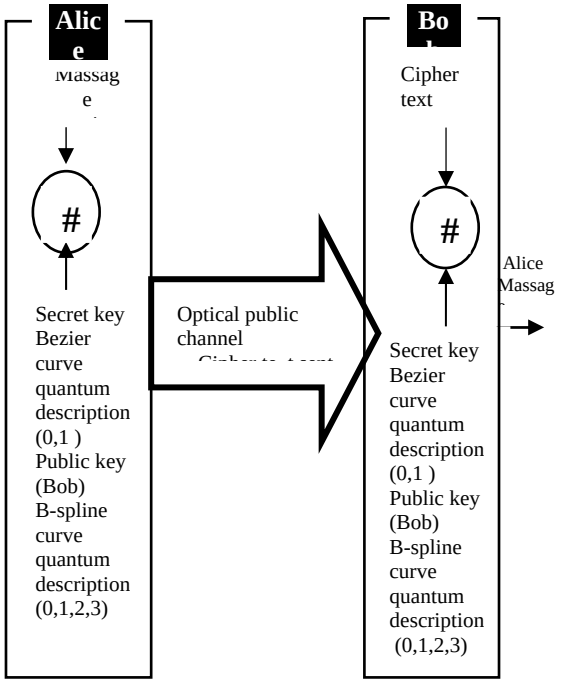
Note: **Bob can verify the correct element for by regenerate the curve and the description for the curve.*

Public key : 0231011300102
Secret key: 0011110001001
Cipher text: 2122232……

Massage: 1110011010111

- Bob received the correct message from Alice.

5- End.



The proposed Quantum cryptography System

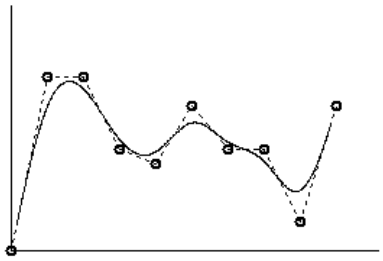
8 *Application*

In this section shown complete example that show implement of the proposed quantum cryptography system in each step:

Stage 1 : initialized the required keys for Alice and Bob:

- **The secret key** : is the same between Alice and Bob (B-spline curve), generate using (10) control points and coordinate as (x,y):
  (25,220),(50,100),(75,100),(100,150),(125, 160),(150,120),(175,150),(200,150),(225, 200), (250,120)

Note: Alice and Bob agreed previously about the number of photons between each two control points and the number of the control pointes.



Figure(5): B-Spline curve generate in Alice and Bob using (10) secret control points coordinate.

The Secret Key will be as follows according base protocol (see 5.1): 0011110001001…….

- **Bob Public key** figure**(**6**):**
  Bob send his public key to Alice which represent a B-spline curve description with public control points , Bob use (5-control points) to generate his curve as follow :
  (100,250),(150,180),175,110),(200,280), (250,200)

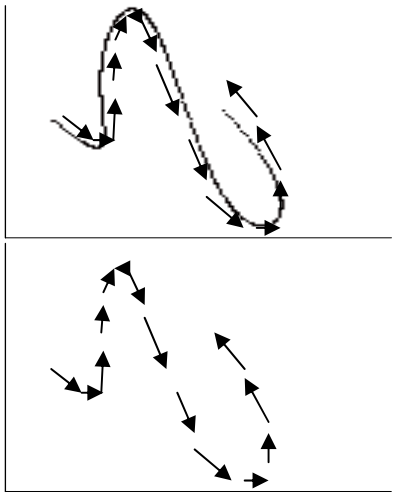


Figure (6): Bob-public key (B-Spline curve using 5- control points) and its quantum description.

Note:

Reflected (0º) > "0"
Reflected (90º) > "1"
Reflected (135º) > "2"
Reflected (45º) > "3"

According to the reflected that illustrated in (section -6) The description for Bob public key using 4-states

is: **2011322220111** *Bob public key*

Stage 2: (sending process)

- Alice want sent a message " **GO**" to Bob , she encoded this massage using (ITA2) International Telegraph Alphabet No.2[10]:

  Massage **G O null(padding)**
  Encoded 01011 00011 0000

Cipher process:

- Alice cipher her massage using public key description from Bob with secret key description that agreed previous both Alice and Bob about it and perform XOR function that illustrated in section -7 . the process as follow:

Public key (Bob):	**20113222201112**	
Secret key :	00111100010010	**XOR**
Encoded massage:	0101100011**0000**	
Cipher text	02101322330002	

Stege-3: received process

- Bob Received the cipher text from Alice by optical public channel.
- Bob used his secret key and public key with cipher text to extract the massage:

Public key (Bob):	**20113222201112**	
Secret key :	00111100010010	**XOR**
Cipher text	02101322330002	
Encoded	01011000110000	

- Bob use (ITA2) to convert the code:

  01011 00011 0000
  G O null

The massage is : GO

Stage -4 : End.

8 Conclusions

The idea of quantum cryptography is invented to prevent eves dropping through a principle in quantum theory that the photon could be polarized once. Then the recipients will ignore the wrong polarized photon and the even drops photon will not be received by the recipient and will not be considered as a part of the key. On the other hand, the use of curve to invent the key will add more security to the system due to the higher randomness that the photon sequence is invented with. In this work a key generation system is invented depending on using a curve generated depending on a(secret and public) control points then this curve described as a sequence of photons spin on one eight directions. This sequence is sent to the other communication party and the correctly polarized photons will be considered the required key. An example of the proposed protocol was presented and the randomness tests of the resulted key are proved to have a high degree of randomness.

9 References

[1] Schaefer E. D., "***An introduction to Glyptography***", Santa Clara University, 1999.

[2] Mermin N. D., "**Lecture Notes on Quantum Computation and Information Theory** ", Cornell University, Physics 481-681, CS 483, Fall, 2000.

[3] Alfred J.M., Paul V. C. and Scott A. V., "***Handbook of Applied Cryptography***", Fifth Addition,2001.

[4] Moses T., " **Quantum Computing and Quantum Cryptography**", Entrust. Security Digital Inteties and Information, 2003.

[5] Understanding Quantum Cryptography – id Quantique, Switzerland, "***id Quantique" White Paper,vesion1.***

[6] Firas Husham Al-Mukhtar, "***Parallel Generation of Non Linear Curves with Computer Aided Application***", PhD. Thesis, Computer & Informatics Information Institute for Postgraduate Studies, 2003 .

[7] Hala B. Abdul Wahab, Rana F. Ghani, , ."***Quantum Description of Curve Cryptography Technique to Implement Key Distribution System",*** Journal of information technology, Vol.2 No.1 , 2008.

[8] Aill Hassan Tarish , "***Designing and Implementing a Stream Cipher Image Cryptography System***" M.Sc. Thesis, University of Technology,2000.

[9] Alaa Edwad William," **Eavesdropping Strategies of Optical Fiber Communication Link",** M.Sc. Thesis, University of Technology, 2005.

[10] Beker H., piper F., (1982). " ***Cipher System, the Protection of Communication",*** Northwood Books Publications, London.