Quantum Description of Curve Cryptography Technique to Implement Key Distribution System

Dr. Hala Bahjat Abdul wahab Dr. Rana Fareed Ghani
Department of Computer Science
University of Technology

Abstract

The main goal of this paper is combining the curve security methods with quantum cryptography concepts in order to increase the capability of cryptography systems that are used for the key distribution. Depending on the generation of curve description with quantum cryptography concepts, the curve description will be sent to the other party to agree about the key depending on the suggested protocol in this paper. The combination of the two cryptography direction guaranteed that the resulted key have the required randomness.
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.

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

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 newest hot spots in security research is curve security. 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 [Mer00].
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. Cryptography

Cryptography technology allows people using networks to ensure that message they send remain private (secure) from hackers, industrial espionage, and government wiretap abuses. Cryptography is the ancient art and science of transforming information, it is a technology so widespread that it is impossible to stop, and it will prove vital to the future of electronic commerce [Sch99]. The great developments in cryptography tend to use key (encryption and decryption operations) to increase the complexity of attack operations. For security purpose, the key length should be as big as the size of the plaintext message. Get such a key and merging it is a real problem in cryptography. This problem may be solved by using pseudo random number generator but cryptographic system need a cryptographically strong

(Pseudo) random numbers that cannot be break (guessed) by the attacker. Random numbers are typically used to generate a session keys, and their quality is critical for quality of the resulting cryptosystem [Alf01].

There are two types of encryption system in use today [Sch97].

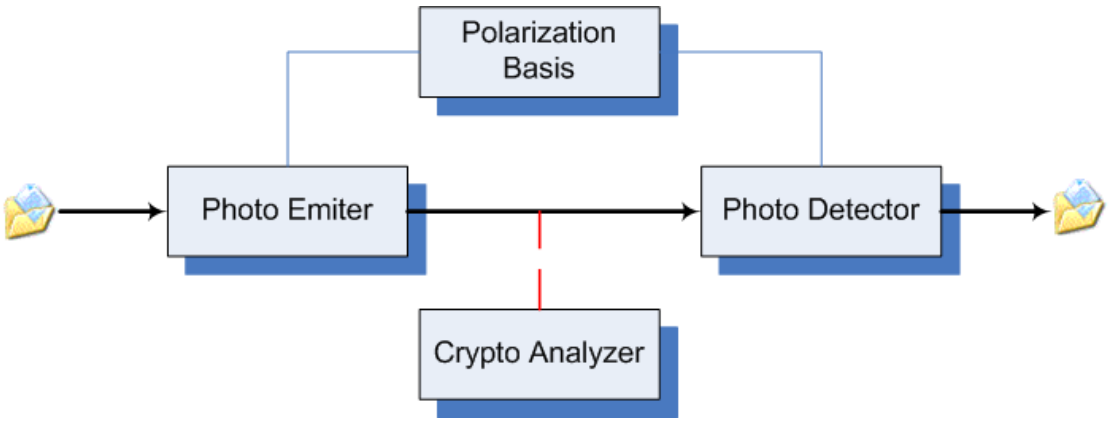
- A secret-key cryptography (symmetric key cryptography):
  Secret-key cryptography applies a secret key for encryption and decryption. Due to its high performance, symmetric-key is normally used to encrypt data for privacy.
- Public-key cryptography (Asymmetric-key cryptography):
  Public-key cryptography applies a public key for encryption and a private key for decryption. Public-key cryptography is often used for key distribution and digital signatures.

2.1 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 [Mos03].

Quantum Cryptograph features

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



2.2 The key distribution problem

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, RSA key transport, etc.

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. When you read this article for example, the sheet of paper must be lighted. The impact of the light particles will slightly heat it up and hence change it. This effect is very small on a piece of paper, which is a macroscopic object. However, the situation is radically different with a microscopic object. 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 a key and not valuable information. Once the key is validated, it can be used to encrypt data. Quantum physics allows to prove that interception of the key without perturbation is impossible [Mos03].

3. 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.

Bezier Polynomials[Fau79]

Bezier curves were developed by Paul de Casteljau in 1059 and independently by Pierre Bezier around 1962. They were formulated as ingredients in Computer Algorithm Graphic Design (CAGD) systems at two automobile companies, Citroen and Renault, to help in designing shapes for automobile bodies. The Bezier curve P(t) based on control points $P_0, P_1, \cdots, P_L$ does not generally pass through, or interpolate all the control points but have seen that it always interpolates P_0 and P_L. This is very useful prosperity, because a designer who is inputting a sequence of points thereby knows precisely where the Bezier curve will begin and end [Ala00] . Bezier's form is

$$R = r(u) = (1-u)^3 r_0 + 3u(1-u)^2 r_1 + 3u^2(1-u)r_2 + u^3 r_{3,}$$

where $0 \le u \le 1$ for any given segment,

r_0= first control point, r_1=second control point,

r_2= third control, r_3=last control point.

Thus the curve described by Bezier's form passes through the points r_0 and r_3, has a tangent at r_0 in the direction from r_0 to r_1 and at r_3 has a tangent in the direction from r_2 to r_3. Figure (1) shows the Bezier curve.

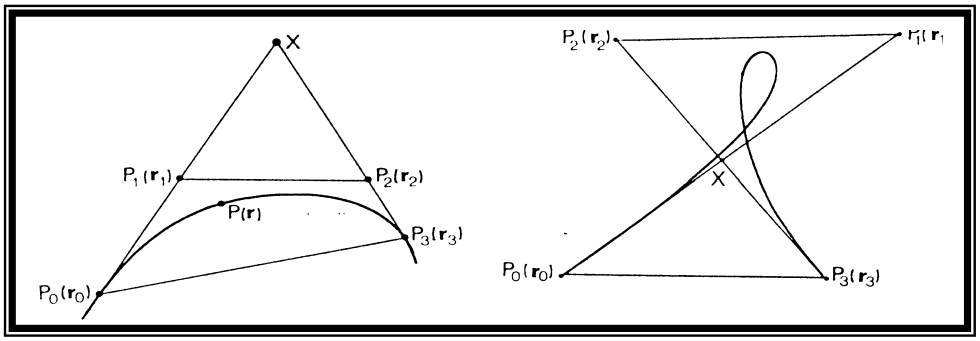


Figure (1): Bezier curve

The straight lines P_0P_1, P_1P_2 and P_2P_3 of a figure (1) are called the characteristic polygon of the curve, although it is not usually a closed figure. In order to design a curve, we choose the points P_0 and P_3 through which we want the curve to pass, and then place P_1 and P_2 on the desired tangents at P_0 and P_3. The lengths of P_0P_1 and P_2P_3 are then adjusted simultaneously to give greater fullness to the curve, or differentially in order to draw the curve nearer to one or other tangent.

3.2 Parametric Forms of Curves

A parametric form for a curve produces different point on the curve, based on the value of a parameter. A parametric form suggests the movement of a point through time, which we can translate into the motion of a pen as it sweeps out the curve. The path of a particle traveling along the curve is fixed by two functions, x( ) and y( ),and we speak of (x(t),y(t)) as the position of the particle at time t. The curve itself is the totality of points "visited" by the particle as t varies over some interval. Figure (2) shows a plane curve to be traced by a moving point. If we use the parameter t to denote time, then the parametric equations x=x(t), y=y(t) specify how x- and y-coordinates of the moving point vary with time [Fir03].

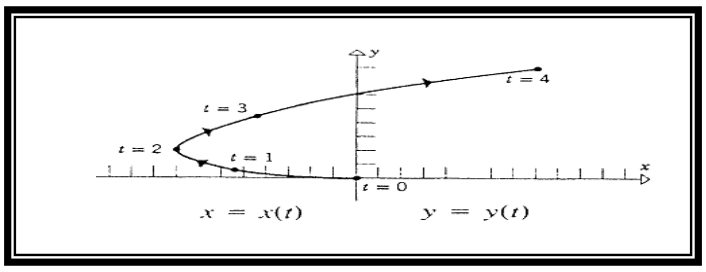


Figure (2): Plane curve.

Algorithm: drawing a piece of a Bezier curve.

Input: Given four points; $(x_i, y_i), i = 0,\ldots,3$.

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

Process:

Step1: for u= 0 to 1 step 0.01

Step2: let $X = (1-u)^3 x_0 + 3(1-u)^2 u x_1 + 3(1-u)u^2 x_2 + u^3 x_3$

Step3: let $Y = (1-u)^3 y_0 + 3(1-u)^2 u y_1 + 3(1-u)u^2 y_2 + u^3 y_3$

Step4: Plot (x, y)

Step5: Next u

Step6: End.

To continue the curve , repeat this process for the next set of four points, beginning with the third point.

Example:

To explain the work of the algorithm, figure (3) shows an example that is used to set control points (x ,y) and use a parameter *t* with increment (10) each time. The output of the implementation of the algorithm to generate the curve is shown in figure(3).

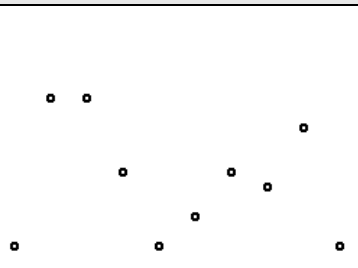
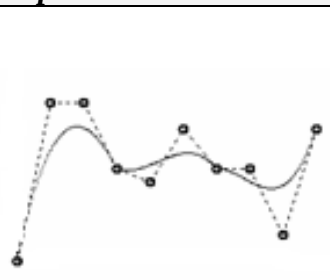
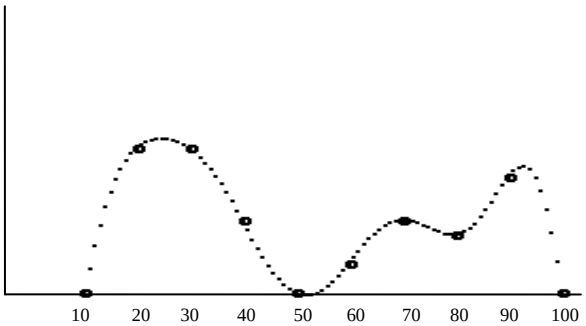
t(i)	*X(i)*	*Y(i)*	*Control Points*	*Interpolated Curve*
10	100	300		
20	125	200		
30	150	200		
40	175	250		
50	200	300		
60	225	280		
70	250	250		
80	275	260		
90	300	220		
100	325	300		

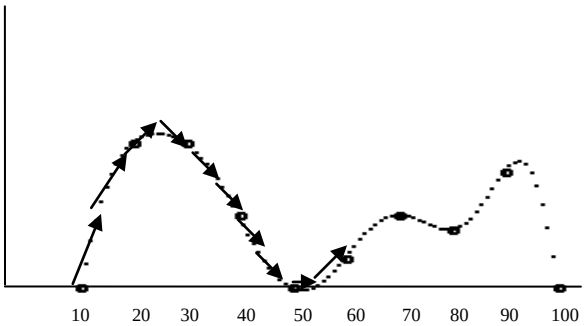
Figure (3): Example of algorithm of drawing a piece of a Bezier curve.

4. Using Curve Generation Technique in Quantum Cryptography

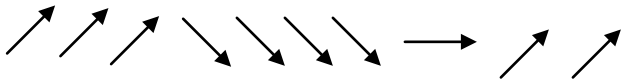
In this section, a description of the proposed quantum protocol for key generation and distribution is presented.

The key is generated as steps on the curve. These steps are coupled with equalized period of time. These steps will be represented as the quantum photons polarized with different directions. As an example, consider the following curve





Alice and Bob agreed previously about the value of time steps t and the number of the time steps N as parameters before any sending or receiving operations. 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 follows:



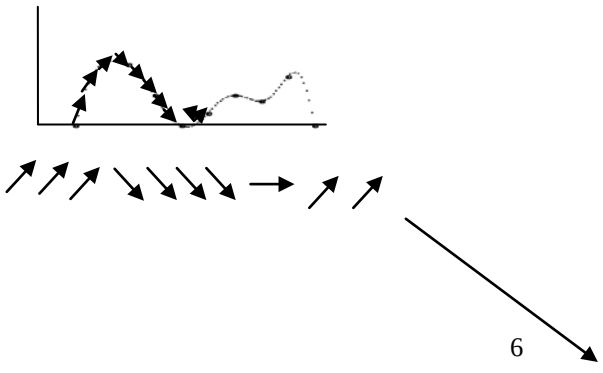
4.1 The Proposed Protocol of Key Distribution problem.

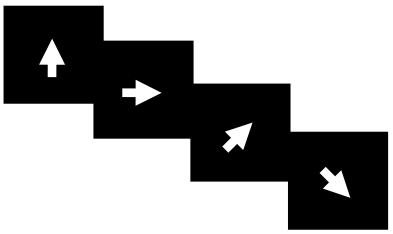
The protocol of key sending will be as follows:

1. 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).
2. Alice and Bob agreed previously about the number of photons between each two control points and the number of the control pointes.
3. Alice invents a curve.
4. Alice generates the key sequence as described in the previous section.
5. Alice sends each photon with its specific direction.
6. Bob will receive photons and measure them with different polarization.
7. If Bob receive the photon properly, he will add this photon to the key.
8. Bob will send the position of the properly received photons to Alice.
9. 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 untel the key is completed.

Example

As an example of how the suggested protocol works, the following figure presents the steps of protocol:

<table>
<tr><td colspan="2">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).</td></tr>
<tr><td colspan="2">Alice and Bob agreed previously about the number of photons between each two control points and the number of the control pointes.</td></tr>
<tr><td>Alice</td><td>Bob</td></tr>
<tr><td colspan="2">Alice invents a curve.
  </td></tr>
</table>



Bob polarize each photon with one of polarization angles.
For example he received the sequence of photons as follows:

↗ - ↗ ↘ - ↘ ↘ → - -

Bob will send the positions of the properly polarized photons
1 3 4 6 7 8

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 001110…….

5. Conclusion

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 eve drops photon will not be received by the recipient and will not be considered as apart 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.

References

[Mer00] Mermin N. D.,(2000). "**Lecture Notes on Quantum Computation and Information Theory** ", Cornell University, Physics 481-681, CS 483, Fall, 2000.

[Sch99] Schaefer E. D., (1999) . ”***An introduction to Glyptography***”, Santa Clara University.

[Alf01] Alfred J.M., Paul V. C. and Scott A. V., (2001), ”***Handbook of Applied Cryptography***”, Fifth Addition.

[Sch97] Schneir B., (1997). ”***Applied Cryptography***”, Second Edition.

[Mos03] Moses T., (2003)." **Quantum Computing and Quantum Cryptography**", Entrust. Security Digital Inteties and Information.

[Mer00] Mermin N. D.,(2000). "**Lecture Notes on Quantum Computation and Information Theory** ", Cornell University, Physics 481-681, CS 483, Fall, 2000.

[Fau79] Faux I. D., Pratt M. J. (1979).”***Computational Geometry for Design and Manufacture***”, Ellis Horwood Limited, USA.

[Ail00] Aill Hassan Tarish (2000). ”***Designing and Implementing a Stream Cipher Image Cryptography System***” M.Sc. Thesis, University of Technology.

[Fir03] Firas Husham Al-Mukhtar(2003). ”***Parallel Generation of Non Linear Curves with Computer Aided Application***”, PhD. Thesis, Computer & Informatics Information Institute for Postgraduate Studies .