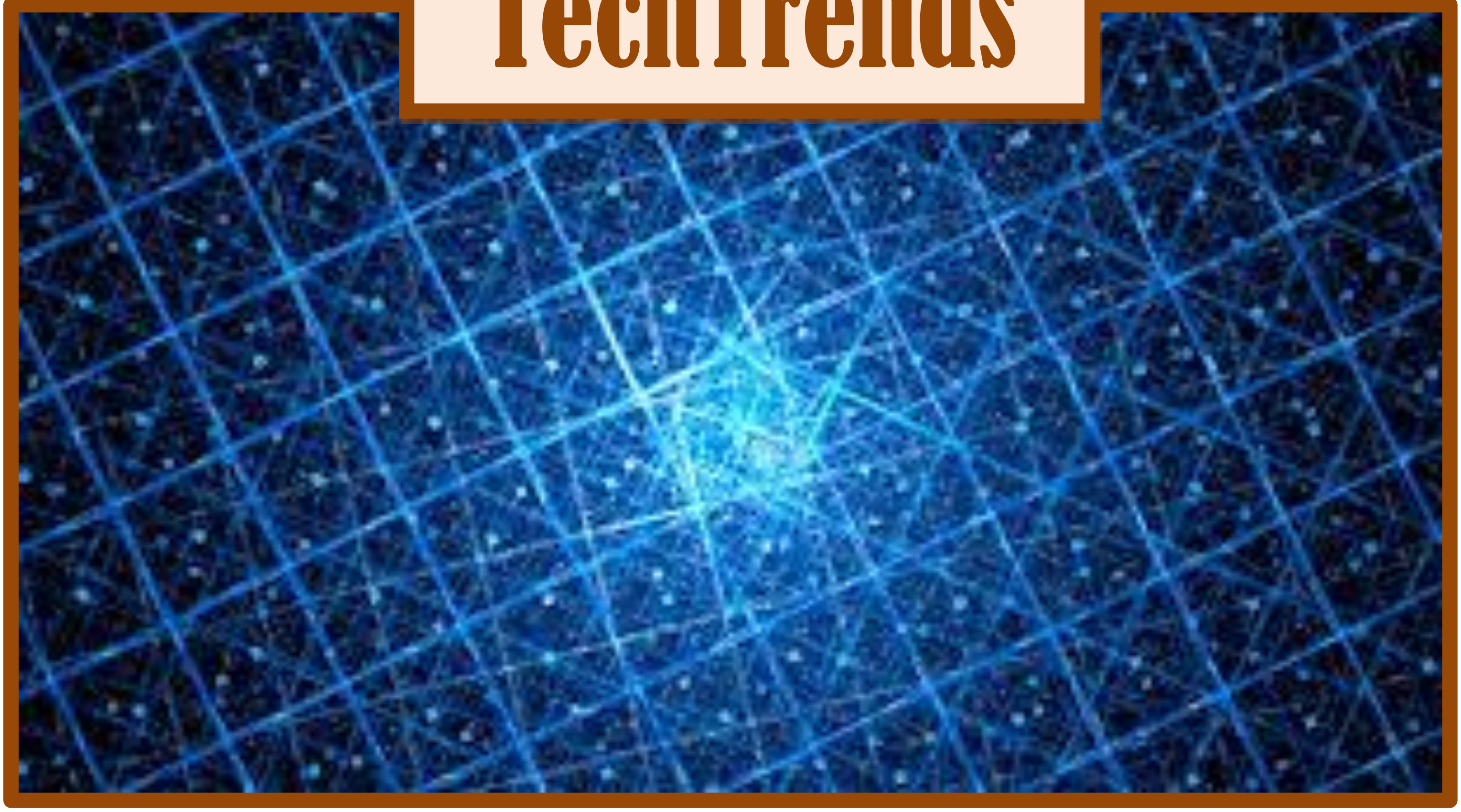
Department of Computer Engineering

Government Polytechnic for Girls,Surat

January-2020 : Vol.- 4

TechTrends

E-Newsletter



Vision:

To empower girls of diploma computer engineering to excel in IT Industries and serve the society.

Mission:

- To strive for academic excellence and professional competence among students and staff.
- To encourage innovative ideas among students to enhance their entrepreneurship skills.
- To provide high tech educational resources and supportive infrastructure.

Follow us on

gpgdceenewsletter@gmail.com

gpgdceenewsletter@gmail.com

Quantum Cryptography

Shri N. S. Khandelwal,
Lecturer,
Department of Computer Engineering

1. Introduction

Today we have very sophisticated and strong algorithms that are more than strong enough for most uses. Some communication data are so critical and so desired by other powerful entities that even our current algorithms may be broken. This type of data might be spy interactions, information warfare, government espionage and so on. Cryptography is the art of devising codes and ciphers, and cryptanalysis is the art of breaking them. Cryptology is the combination of the two.

1.1 Classical Cryptography

Classical Cryptography is based on encrypting the plain text to be send by the source using some mathematical formula. These classical cryptosystems come in two flavors: symmetric systems and asymmetric systems.

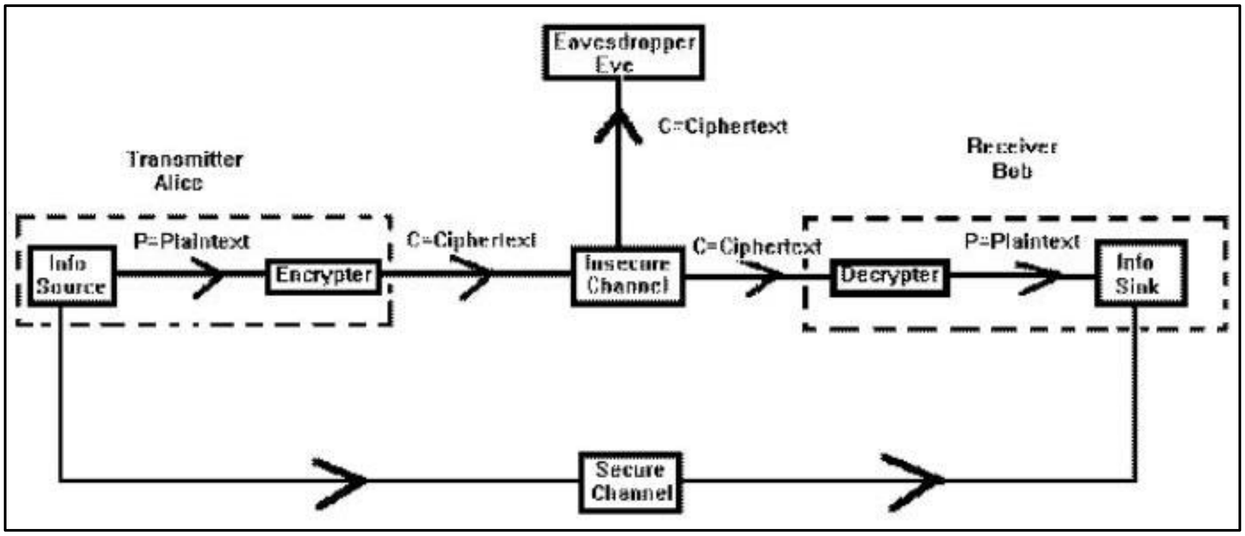


Fig 1.1: Demonstration of Classical Cryptography

Classical cryptography (RSA, AES etc.) does not detect eavesdropping but protects data based on the computational difficulty. If fast technique for factoring large integers is discovered, RSA will not survive anymore. High amount of computation is required , so channel capacity (bits/sec) of Message Information is Reduced. Many efforts are made to overcome these shortcomings; one of it has led to “Quantum Cryptography”.

1.2 Key Distribution Problem

Classical Cryptography suffers from Key Distribution problem that is to communicate the key securely between two pair of users. Conventional (classical) key distribution schemes are fundamentally insecure. There is nothing to prevent an eavesdropper from making a copy of the key during the key distribution process.

Quantum physics has provided a way around this problem. By harnessing the unpredictable nature of matter at the quantum level, physicists have figured out a way to exchange information on secret keys.In the recent past, there has been a good deal of a new cryptographic method whose security is based on the fundamental laws of quantum physics, quantum cryptography. The main achievement is that Quantum Cryptography can solve the problem of key distribution.

1.3 Quantum Cryptography

Quantum cryptography aims at providing information security that relies on the main properties of quantum mechanics. Quantum mechanics guarantees that the act of an eavesdropper intercepting a photon, even if it is just to observe or to read it, irretrievably changes the information encoded on that photon

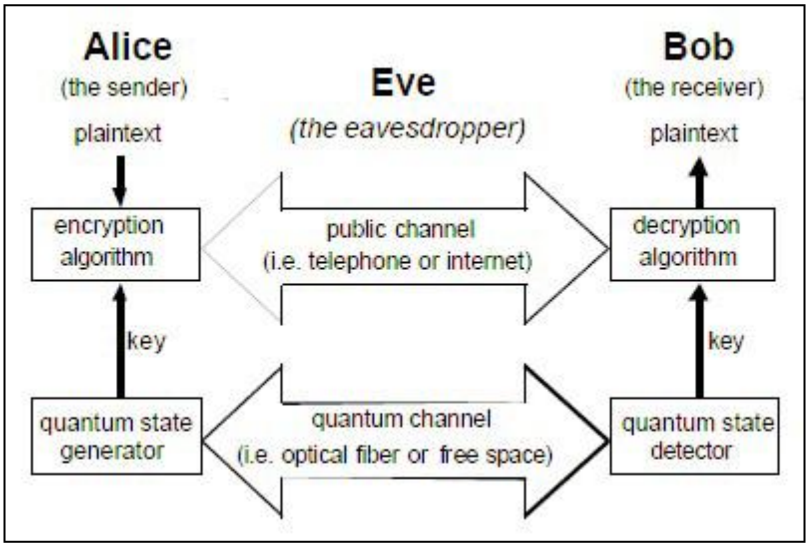


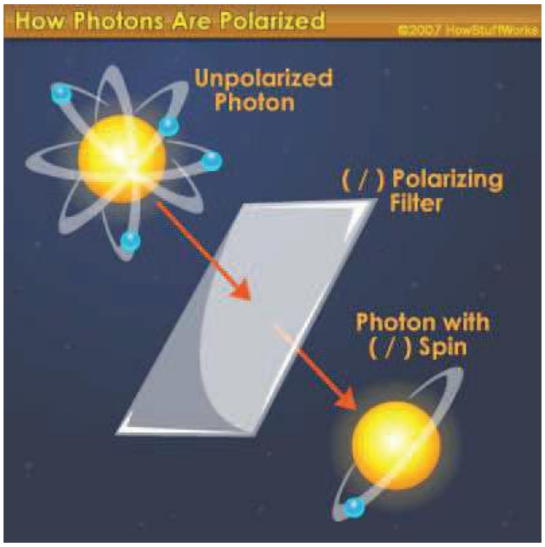
Fig 1.2: Quantum Cryptographic Communication System

2. Quantum Theory Fundamentals

Electromagnetic waves such as light waves can exhibit the phenomenon of polarization, in which the direction of the electric field vibrations is constant or varies in some definite way. A polarization filter isa material that allows only light of a specified polarization direction to pass. If the light is randomly polarized, only half of it will pass a perfect filter.

2.1 Photons

According to quantum theory, light waves are propagated as discrete particles known as photons. A photon is a mass less particle, the quantum of the electromagnetic field, carrying energy, momentum, and angular momentum called as spin. They can exist in all of their possible states at once, called the wave function. This means that whatever direction a photon can spin diagonally, vertically and horizontally, it does all at once. Light in this state is called un polarized.

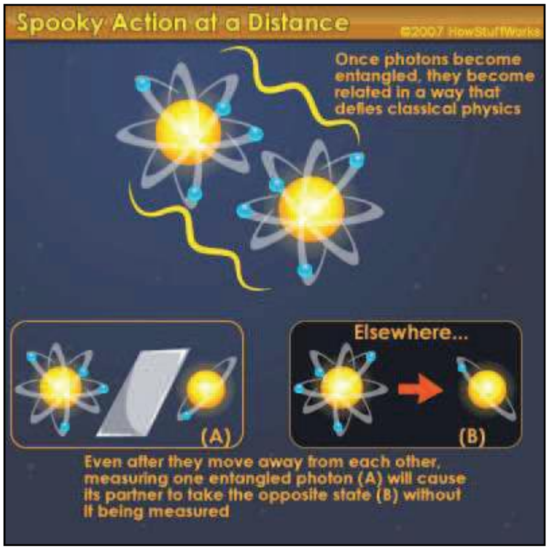

How Photons Are Polarized

©2007 HowStuffWorks

Fig 2.1: Photon Polarization

2.2 Entanglement

Entangled pairs are pairs of photons generated by certain particle reactions. Each pair contains two photons of different but related polarization. Entanglement affects the randomness of measurements. Entangled based protocols that means two entities can be defined such that their properties are entangled altering one effects the value of other. If an entangled object like a key is shared between two parties it maintains integrity of the key.


Spooky Action at a Distance

©2007 HowStuffWorks

Once photons become entangled, they become related in a way that defies classical physics

Even after they move away from each other, measuring one entangled photon (A) will cause its partner to take the opposite state (B) without it being measured

Fig 2.2: Entangled Photons

2.3 Heisenberg's Uncertainty Principle and Photon Polarization Principle

The quantum cryptography relies on two important pillars of 20th century quantum mechanics the Heisenberg uncertainty principle and the principle of photon polarization. According to the Heisenberg uncertainty principle two interrelated properties cannot be measured individually without affecting the other. That it's impossible to know both an object's position and velocity at the same time. The principle is that since you cannot partition the photon into two halves measuring the state of photon will affect it value. So if someone tries to detect the state of photons being send over to the receiver the error can be detected. The Heisenberg Uncertainty Principle ensures that any active attack will not permit an attacker to faithfully read the key transmission.

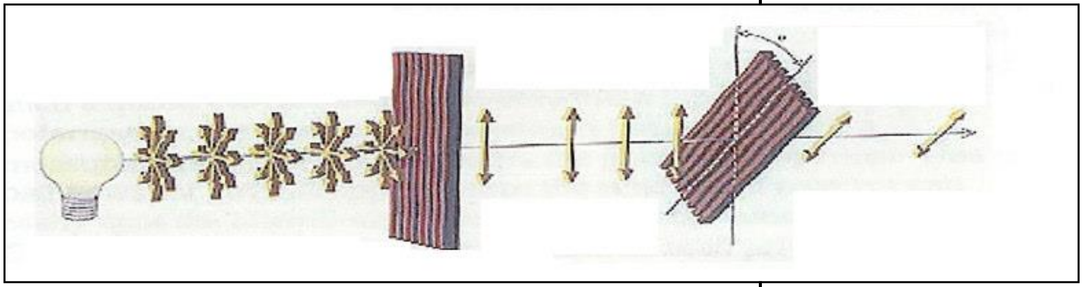


Fig 2.3: Polarization of Light By a Filter

In Fig 2.3, we can see that light from a bulb passes through a polarization filter with is inclined to 90 degree so we get vertical ray of light out of it, if we place another filer that is inclined differently rays are again rotated. If the rays are at orthogonal angle to the filter we will get no output.

The photon polarization principle explains how light photons can be polarized in a specific direction. Photons can be polarized from 0 to 360 degree and intermediate spin positions like 45 or 90 degree can be detected using filters inclined to certain directions. In addition, an eavesdropper cannot copy unknown quits i.e. unknown quantum states, due to no-cloning theorem. This is because at the quantum level, even looking at the atom or subatomic particle changes its attributes. This means that if there is an Eavesdropper carrying out a passive attack such as sniffing, the receiver would know because just this simple act changes the characteristics or polarization of the photons. This means that the photons that were travelling in a horizontal manner could be tilted left and ones that were travelling in a vertical manner could now be travelling horizontally.

3. Quantum Key Exchange

Quantum communication involves encoding information in quantum states, or quits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret key method can take place. The genius of quantum cryptography is that it solves the problem of key distribution. A user can suggest a key by sending a series of photons with random polarizations. This sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail.

In quantum cryptography, photon polarization is commonly used to represent bits (1 or 0). Polarization is the orientation of electromagnetic waves, which is what photons are. Photons are the particles that make up light. The electromagnetic waves have an orientation of horizontal or vertical, or left hand or right hand. Let’s say Alice and Bob are spies and need to send their data back and forth with the assurance it won’t be captured. To do so, they need to establish a symmetric encryption key on both ends, one for Alice and one for Bob. Now both Alice and Bob each have their own photon gun, which they will use to send photons back and forth to each other. They also have mapping between the polarization of a photon and a binary value. The polarizations can represented as vertical (|), horizontal (-), left (\), or right (/), and since we only have two values in binary, there must be some overlap. In this example, a photon with a vertical (|) polarization maps to the binary value of 0. A left polarization (\) maps to 1, a right polarization (/) maps to 0, and a horizontal polarization (-) maps to 1. This mapping (or encoding) is the binary value that make up an encryption key. Bob must have the same mapping to interpret what Alice sends to him. Bob will use this as his map so when he receives a photon with a polarization of (\), he will write down a 1. When he receives a photon with the polarization of (|), he will write down a 0. He will do this for a whole key and use these values as the key to decrypt a message Kathy sends him.

So they have to agree upon a key, which is mapping between the polarization states of photons and how those states are represented in a binary value. This happens at the beginning of the communication session over a dedicated fiber line. Once the symmetric is established, it can be used by sender and receiver to encrypt and decrypt messages that travel over a more public communication path, like the internet. The randomness of the polarization and the complexity of creating a symmetric key in this manner help ensure that an eavesdropper will not uncover the encryption key.

3.1 BB84 Protocol

Bennett and Brassard described an unconditionally secure quantum key distribution system. The system is called the BB84 system.

Table 3.1: Typical Polarization State Pairs

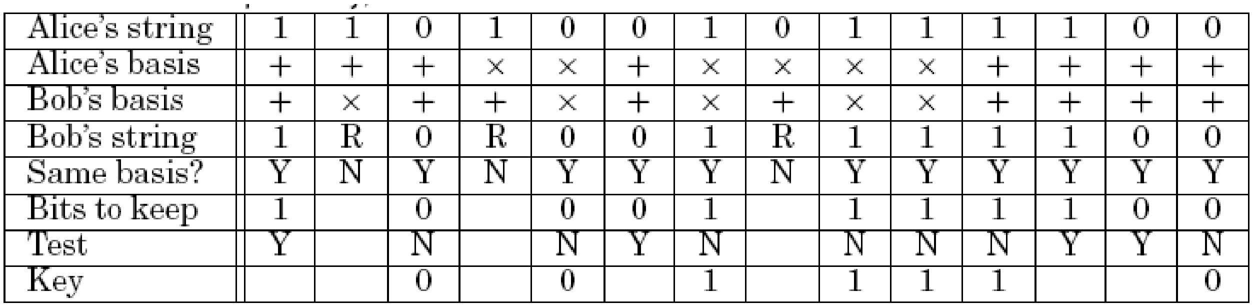
Basis	Representation	Random Bit 0	Random Bit 1
Rectilinear	+	↑	→
Diagonal	X	↗	↖

The protocol works as follows [15]:

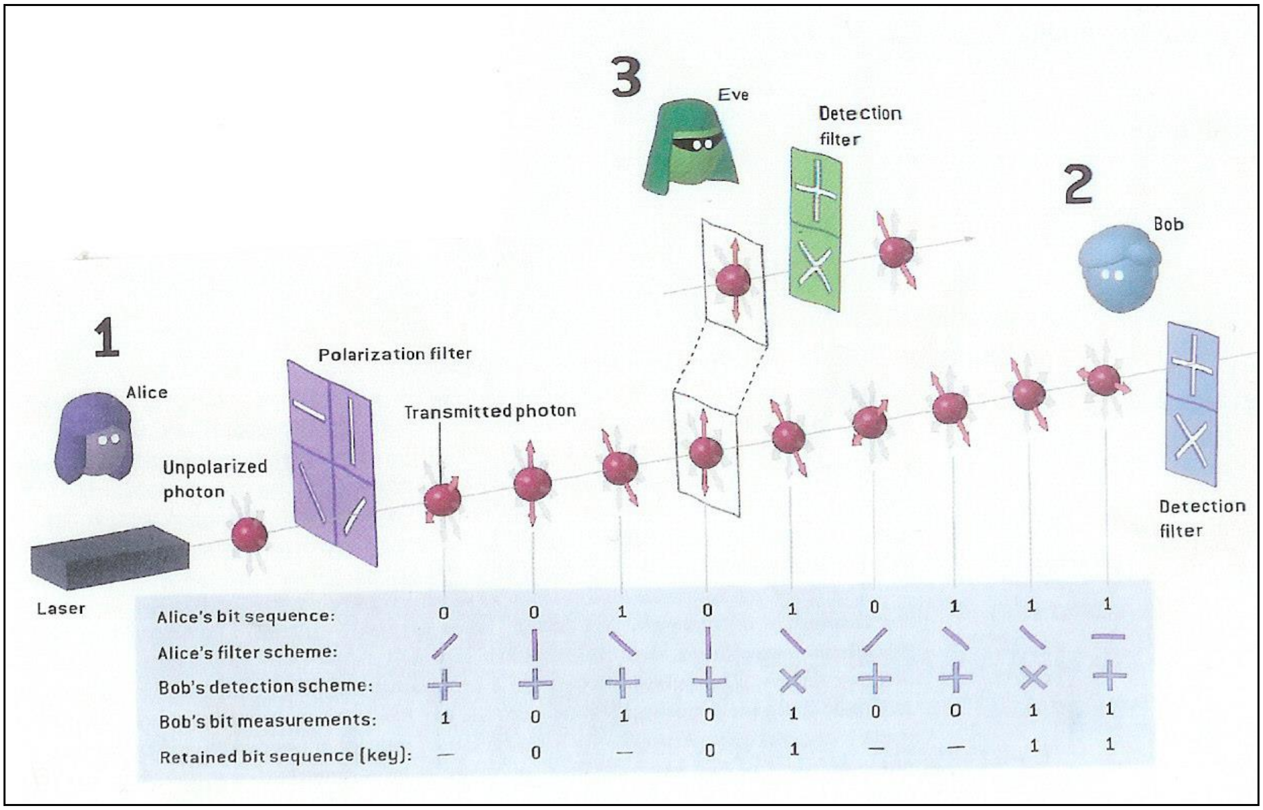
- Alice randomly prepares a string of random qubits, each in one of the four states |, --, /, \ and sends them to Bob.

- For each qubit that Bob receives, he chooses at random one of the two bases (+ or ×) and measures the qubit. For instance, if Alice sends a photon | and Bob measures with his + polarizer oriented either - or |, he will correctly deduce Alice sent a | photon, but if he measures with his X polarizer, he will deduce (with equal probability) either \ or /, neither of which is what Alice actually sent. Furthermore, his measurement will have destroyed the original polarization.
- Bob tells Alice which basis he used to measure each photon, and Alice tells him whether or not it was the correct one. Neither Alice nor Bob announces the actual measurements, only the bases in which they were made. They discard all data for which their polarizer's didn't match, leaving two perfectly matching strings. These are forming the so-called shifted key.
- Alice and Bob choose a subset of the shifted key to estimate the error-rate. They dose by announcing publicly the bit values of the subset. If they differ in too many cases, they abort the protocol, since its security cannot be guaranteed.
- Finally, Alice and Bob obtain a joint secret key from the remaining bits by performing error correction and privacy amplification.

Table 3.2: The BB84 Key Distribution Protocol



Alice's string	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's string	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	0	0
Test	Y		N		N	Y	N		N	N	N	Y	Y	N
Key			0		0		1		1	1	1			0



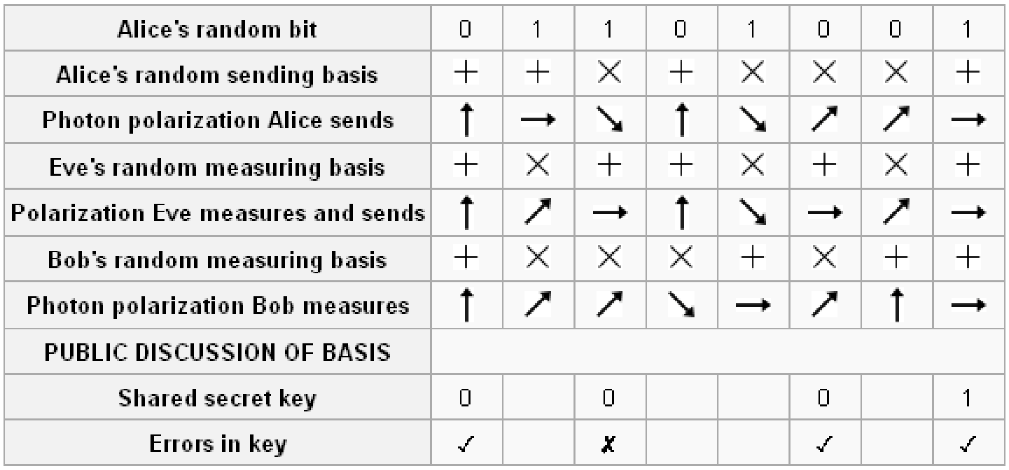
Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	—	0	—	0	1	—	—	1	1

Fig 3.1: Demonstration of BB84 Protocol

3.2 Detecting Eavesdropper

To check the presence of an eavesdropper, we look at a simple eavesdropping strategy, which is called “intercept-and-resend”.

Table 3.3 Detection of Eve’s Presence in BB84 Protocol



Alice’s random bit	0	1	1	0	1	0	0	1
Alice’s random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve’s random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob’s random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

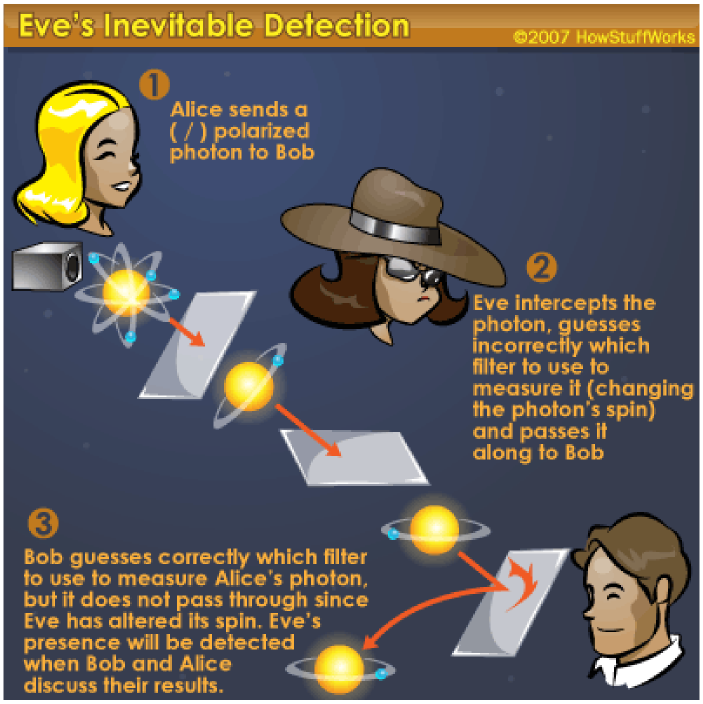

Eve’s Inevitable Detection
©2007 HowStuffWorks
1
Alice sends a (/) polarized photon to Bob
2
Eve intercepts the photon, guesses incorrectly which filter to use to measure it (changing the photon’s spin) and passes it along to Bob
3
Bob guesses correctly which filter to use to measure Alice’s photon, but it does not pass through since Eve has altered its spin. Eve’s presence will be detected when Bob and Alice discuss their results.

Fig 3.2: Detecting an Eavesdropper

4. Applications

- E-voting
- Satellite television broadcasts
- Video Conferencing
- Financial Institutions
- Online banking
- WLAN security
- Cloud security
- Cyber security
- ATM transactions

5. Benefits

- It provides complete secret communication and will play a great role in military, national defense, national economic construction and others.
- Because the delay of quantum communication is zero, it can be realize faster-than light communication, it can meet requirements of remote, high capacity, networking easily and other aspects.
- It is virtually un-hackable and provides highly secure Quantum key distribution.
- This technique is very simple to use.
- Fewer resources are required to implement this technique.
- Quantum cryptology is the first cryptology that safeguards against passive interception of an eavesdropper.
- It has a faster key refresh rate than traditional cryptosystem.
- It employs truly random key generation.
- It guarantees proactive intrusion detection.
- It provides lower total cost of ownership.
- It involves speedy set up with virtually zero maintenance.

6. Conclusion

- An important and unique characteristic of Quantum cryptography is the ability to detect the presence ofany third party between two communicating users. The security of quantum cryptography depends on the foundation of quantum mechanics, and that can revolutionize the network security. The primary use of Quantum cryptography systems is for the distribution of secret keys for encrypting and decrypting a conversation between two parties. The Quantum cryptography system is very promising and advancements are being made to improve upon the technology, but it is still susceptible to various attacks and limitations which need to be overcome in near future.

7. References

1. Bennett, Charles H., and Gilles Brassard, “Quantum cryptography: Public Key Distribution and Coin Tossing,” Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.

2. Salvatore Vittorio. “Quantum Cryptography: Privacy Through Uncertainty” [Online]. Available: http://www.csa.com/discoveryguides/crypt/overview.php

3. Josh Clark. “How Quantum Cryptography Works” [Online]. Available: http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm

4. Nguyen, Thi Mai Trang, Mohamed Ali Sfaxi, and Solange Ghernaouti-Helie, “Integration Of Quantum Cryptography In 802.11 Networks,” The First International Conference onAvailability, Reliability and Security(ARES), IEEE 2006.

5. Dagmar Bruss, G, Abor Erd´ Elyi, Tim Meyer, Tobias Riege, and J Org Rothe, “Quantum Cryptography: A Survey,” ACM computing Surveys 2007.

QUIZ (4)

Reasoning Questions

1. ELFA, GLHA, ILJA, _____, MLNA

   A. OLPA

   B. KLMA

   C. LLMA

   D. KLLA

2. (i) All the trees in the park are flowering trees.
   (ii) Some of the trees in the park are dogwoods.
   (iii) All dogwoods in the park are flowering trees.

   If the first two statements are true, the third statement is What is the average of first five multiples of 12?

   A. true

   B. false

   C. uncertain

Answer of Last Quiz (3)

1. **Option C** Explanation :

   Since each day of the week is repeated after 7 days.
   After 133 days, it will be Thursday.
   ∴ So one day before that would be Wednesday.

2. **Option A** Explanation:

   Average = 12*(1+2+3+4+5) *

   = 12 * 15*

   = 12 * 3= 36

INNOVATIVE SOLUTIONS THROUGH MOBILE APP

(Date: 10/12/2019 To 13/12/2019)

Computer department of Government polytechnic for girls, Surat has organized an android workshop for 4 days from 10/12/2019 to 13/12/2019 on **“Innovative Solutions through Mobile Application”** under **SSIP**, in which the expert teachers Mr Vaibhav Surana and Mr Amrish Kakadiya from **CORONA INSTITUTE** have shared their expertise with the students.

All the students of semester 6th have participated in this workshop. They taught them to develop innovative android application using android studio.

OR GIRLS- SURAT
EM WORKSHOP
ON
SOLUTIONS
GH ANDROID
MOBILE APP
2019 To 13/12/2019
PUTER DEPARTMENT
Android application development

Student Corner:

Law of attraction

How many of you experienced that ‘if I got this then it would be so amazing’ or ‘if I do this then life would be much better’ and same happened to you….many of you right? Or how many of you had planned something and everything goes right but you had a doubt and it went all wrong in the end. It was like you knew all along that something like this would happen…of course everyone of you. Everyone has experienced either of the above situations at least once in their life. Some could say it’s just a coincidence but it cannot be a coincidence if it is experienced by everyone. And yes it is true. There is a perfect science behind it. We can say it is the programming of our mind or heart according to which we attract things, situations and people.

In simple words we call it the ‘law of attraction’.

How does the law of attraction works?

We can think of the law of attraction as a magnet. Just like a magnet attracts metals towards itself your thoughts attracts situation, things and people towards yourself. For example you thinking of the car of your dreams or money you need for opening your own company or marrying the man or woman of your life. For instance when you think ‘I must not be late for college’ but such suddenly your tire got flat or you forgot your id card or my favorite one is you could not open your eyes in the morning and you got late. And you will think that ‘this is not what I wanted or wished for’ but actually what you need to think was that ‘I am on time for my college’ because the universe is not interested in knowing what you don’t want rather it is only interested in knowing what you actually want.

So the according to the law of attraction we need to focus on what we actually want and have an absolutely clear image about it.

What is the science behind the law of attraction?

We all know that there are two states mind: conscious and subconscious. Both have their particular importance in our body. The conscious mind understands logic and works accordingly and the subconscious mind is illogical.

The conscious mind makes a big fat wall around the subconscious mind to protect it because subconscious mind is illogical and whatever belief or thought or wish comes to it delivers to universe to realize. For example if someone says that you are a monkey then the conscious mind wall will laugh and give a kick to that thought saying ‘idiot I am a human being and not a monkey’. But the illogical mind does not understand this kind of logic so thoughts which enter in this state of mind become reality. So when you say that ‘I want to become an entrepreneur’ then your conscious mind is going to answer that ‘Engineering and entrepreneur?! Chal ja ghode bech ke soja’.

So how to make this both to work in favor of us that we will see in the next issue of our newspaper…

To be continued…

Tanushree Manish Doctor
Enrollment No. : 186150307021-3rd A
Department of Computer Engineering