https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#toc

https://www.gla.ac.uk/schools/physics/staff/sarahcroke/#researchinterests,publications,articles

Classical cryptography can be divided into two major branches; secret or symmetric key cryptography and public key cryptography, which is also known as asymmetric cryptography. Secret key cryptography represents the most traditional form of cryptography in which two parties both encrypt and decrypt their messages using the same shared secret key. While some secret key schemes, such as one-time pads, are perfectly secure against an attacker with arbitrary computational power [Gisin02], they have the major practical disadvantage that before two parties can communicate securely they must somehow establish a secret key. In order to establish a secret key over an insecure channel, key distribution schemes basd on public key cryptography, such as Diffie-Hellman, are typically employed.

Paper Summary

(Imp Notes)

Cryptography

Public key cryptography

Assymetric.

traditional methodology

Same key is used. Typically to share the key b/w parties is done via DHKE

Secret key cryptoge

Symmetric

No prior distri

one can use some one's publi key and then encrypt using public key of the reciever. Once reciever receives th encrypted message, then it can decrypt using its private key.

while there is no requirement to exchange keys in such cases, however, all these crypto-systems are built upon the difficulty power or difficult computation power of attacker all based on unproven assumptions of difficulty of certain problems such as integer factorizati or discrete logarithm.

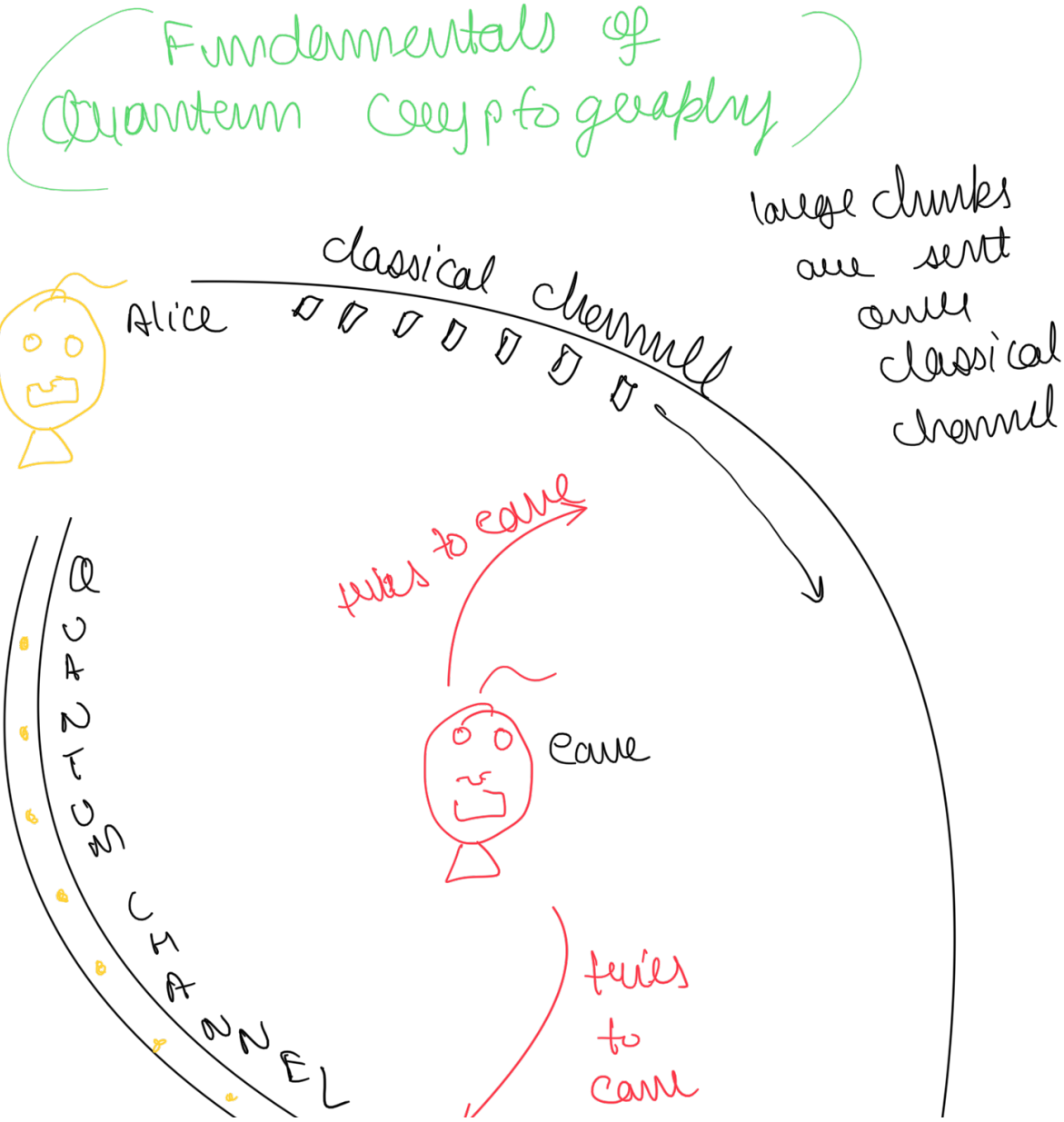
In contrast to secret key cryptography, a shared secret key does not need

to be established prior to communication in public key cryptography. Instead each party has a private key, which remains secret, and a public key, which they may distribute freely. If one party, say Alice, wants to send a message to another party, Bob, she would encrypt her message with Bob's public key after which only Bob could decrypt the message using his private key. While there is no need for key exchange, the security of public key cryptography algorithms are currently all based on the unproven assumption of the difficulty of certain problems such as integer factorization or the discrete logarithm problem. This means that public key cryptography algorithms are potentially vulnerable to improvements in computational power or the discovery of efficient algorithms to solve their underlying problems. Indeed algorithms have already been proposed to perform both integer factorization and solve the discrete logarithm problem in polynomial time on a quantum computer [Shor97] [Bruss07].

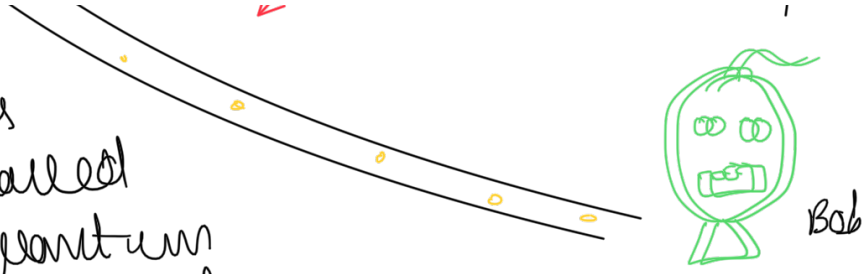
While the advent of a feasible quantum computer would make current public key cryptosystems obsolete and threaten key distribution protocols such as Diffie-Hellman, some of the same principles that empower quantum computers also offer an unconditionally secure solution to the key distribution problem. Moreover, quantum mechanics also provides the ability to detect the presence of an eavesdropper who is attempting to learn the key, which is a new feature in the field of cryptography. Because the research community has been focused primarily on using quantum mechanics to enable secure key distribution, quantum cryptography and quantum key distribution (QKD) are generally synonymous in the

literature.

From these principles the protocols are divided into two categories; those based primarily on the Heisenberg Uncertainty Principle, and those utilizing quantum entanglement. *While much of the recent research focus is on developing practical quantum cryptosystems [Bruss07]*

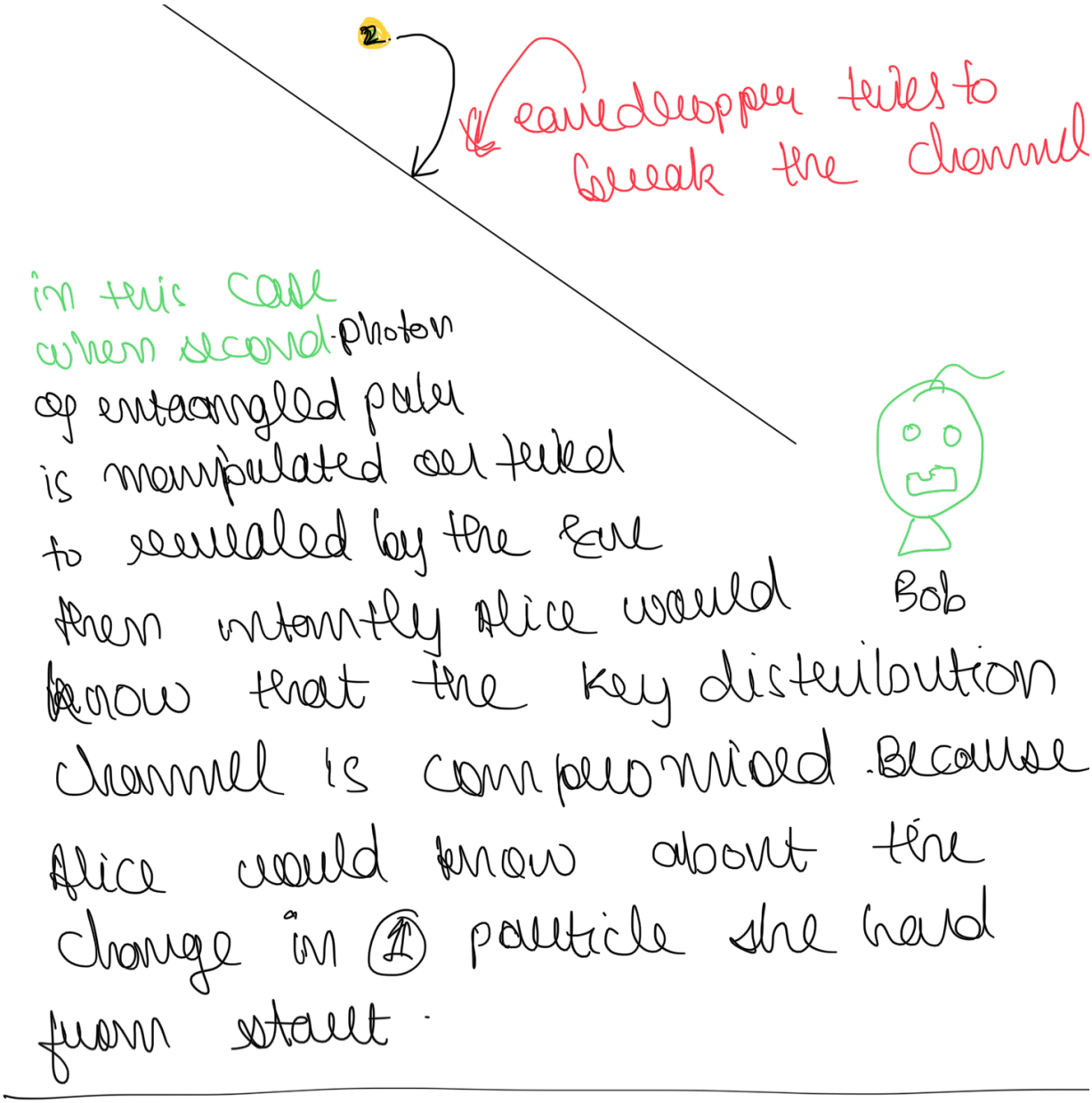


only keys are shared over quantum channel



In perspective of eavesdropper, even, eavesdropper (Eve) is able to break the classical channel, the data packets will be of no use since the key remains unknown. Whereas, the keys are shared over the quantum channel, which on interception will result in the detection of breach. As when Alice sends the quantum entangled pairs of photons to Bob, if Eve intercepts in between them, the entanglement will be collapse This can be shown as :-

one photon from pair is put on channel to send to Bob



The basic model for QKD protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. This is shown in figure 1. An eavesdropper, called Eve, is assumed to have access to both channels and no assumptions are made about the resources at her disposal. With this basic model established, we describe in layman's terms the necessary quantum principles needed to understand the QKD protocols.

Heisenberg Uncertainly Principle :- HUP

(a) You can always have only one state of a quantum setting with certainty. One property of a pair of conjugate properties can be known with certainty.

Heisenberg Uncertainty Principle (HUP) which states that in a quantum system only one property of a pair of conjugate properties can be known with certainty. Heisenberg, who was initially referring to the position and momentum of a particle, described how any conceivable measurement of a particle's position would disturbs its conjugate property, the momentum. It is therefore impossible to simultaneously know both properties with certainty.Quantum cryptography can leverage this principle but generally uses the polarization of photons on different bases as the conjugate properties in question. This is because photons can be exchanged over fiber optic links and are perhaps the most practical quantum systems for transmission between two parties wishing to perform key exchange.

No Cloning Theorem : It is impossible to create multiple copies of quantum state

the no cloning theorem 1982. states that its impossible to create multip identical copies of an arbitrarily unknown quantum state. The importan of no cloning theorem is that, without NCT, one may think to create multiple copies of same quantum particle. That is, one can overcome heisenberg uncertainty principle, by creating multiple copies of quantum state & then measuring its polariza of each copy to create many copies. However this will violate HUP Because otherwise its collapsed already if you would be knowing quantum state of each photon already. This is against the fundamental Properties of quantum mechanic

One principle of quantum mechanics, the no cloning theorem, intuitively

follows from Heisenberg's Uncertainty Principle. The no cloning theorem, published by Wooters, Zurek, and Dieks in 1982 stated that it is impossible to create identical copies of an arbitrary unknown quantum state [Bruss07] [Wooters82]. One could see that without the no cloning theorem, it would be possible to circumvent Heisenberg's uncertainty principle by creating multiple copies of a quantum state and measuring a different conjugate property on each copy. This would allow one to simultaneously know with certainty both conjugate properties of the original quantum particle which would violate HUP.

2.2 Quantum Entanglement :-

Eckert 91 :

The other important principle on which QKD can be based is the principle of quantum entanglement. It is possible for two particles to become entangled such that when a particular property is measured in one particle, the opposite state will be observed on the entangled particle instantaneously. This is true regardless of the distance between the entangled particles. It is impossible, however, to predict prior to measurement what state will be observed thus it is not possible to communicate via entangled particles without discussing the observations over a classical channel. The process of communicating using entangled states, aided by a classical information channel, is known as quantum teleportation and is the basis of Eckert's protocol as will be described in Section 4 [Eckert91] .

BB84 : BB84 IMPORTANT :-

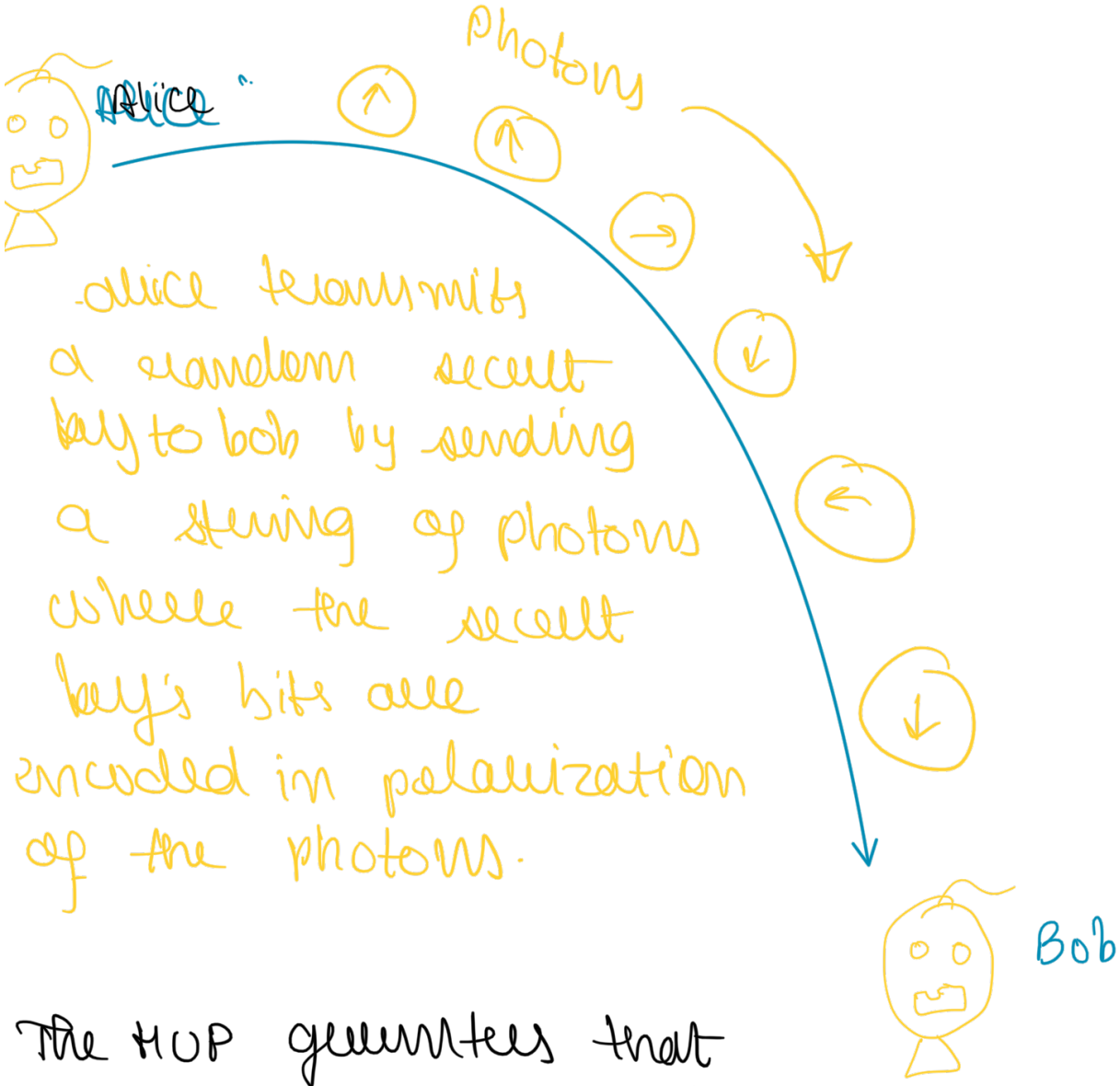
1984 = C. Bennett and G. Brassard

(a) most prominent quantum cryptographic protocol.

(b) All other HUP based protocols are

more or less variants of this protocol.

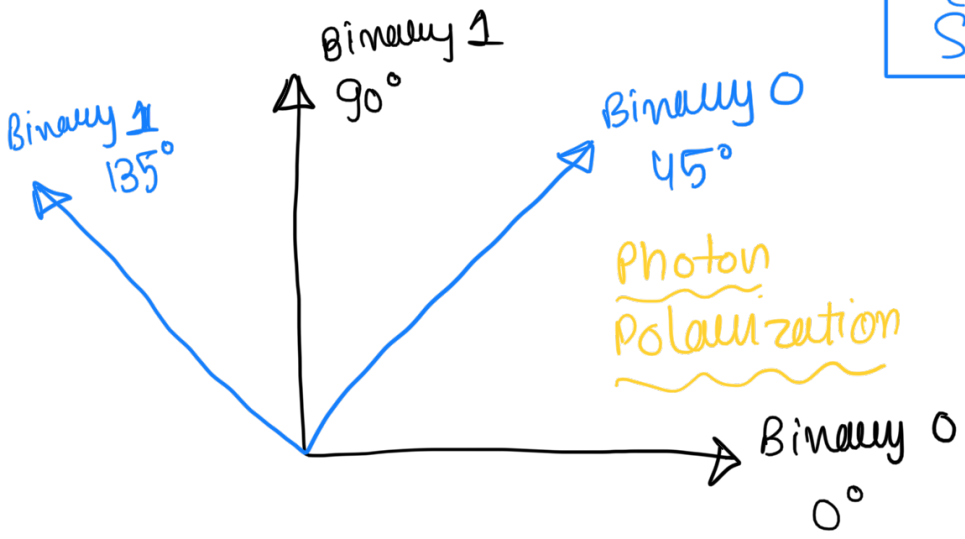
(c) Basic idea:

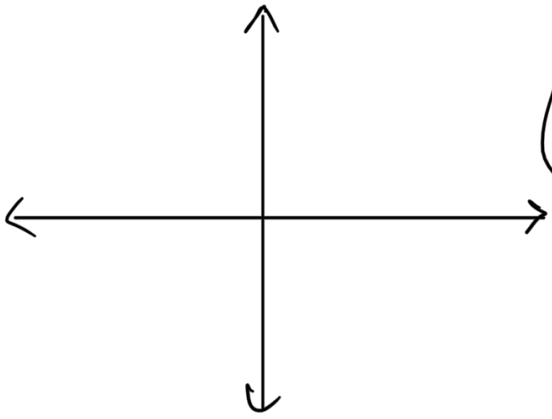


The HUP guarantees that we cannot measure these photons and transmit them on to Bob without disturbing the photons state in detectable way. Thus revealing her presence.

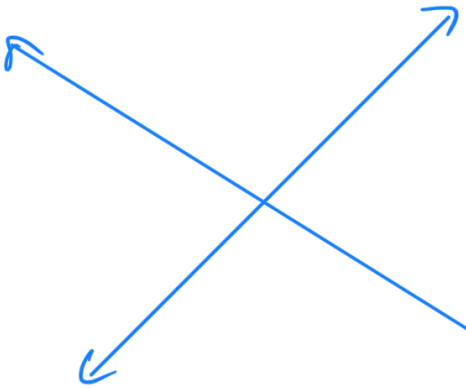
3.1 BB84 Protocol :-

Bit Encoding Schemes





(Rectilinear basis)



(Diagonal Basis)

Phase 1 of communication :

Bit String = 00101001

(a) Alice ——— quantum channel ———→ Bob

(b) bits $\xleftarrow{\$}$ $\{0,1\}^n$

(c) basis $\xleftarrow{\$}$ $\{X, +\}^n$

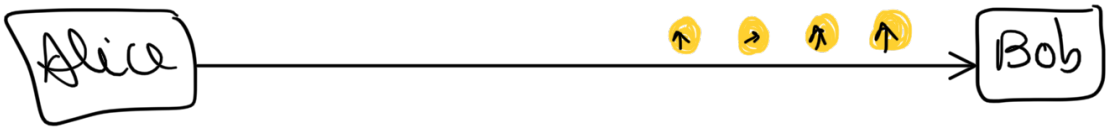
(d) Encode (bits) using basis

encoded bit(s) $\leftarrow$ encode (bits, basis)

(e)

transmit photon corresponding to each bit - with corresponding polarization.

(f) For every photon bob receives, Bob measures the photon's polarization by a randomly chosen basis



(g) encoded bit (from Alice) should match decoded bits (Bob)

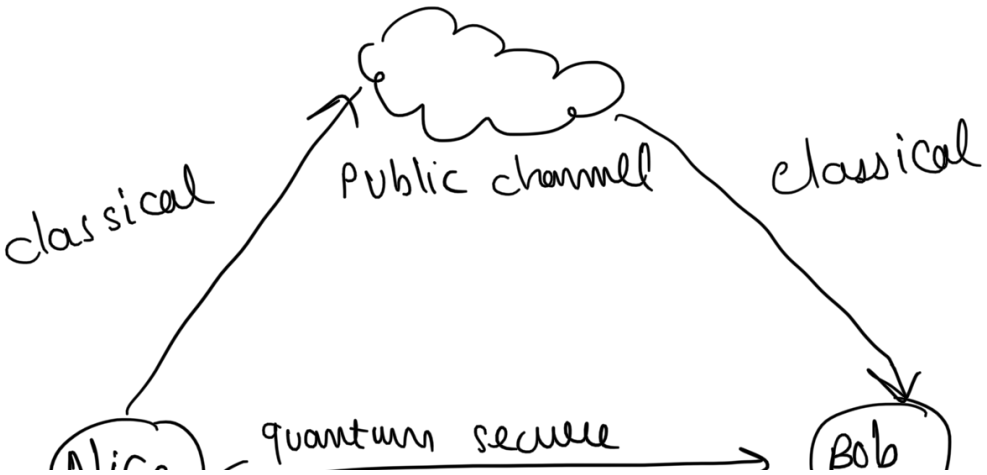
That is :-

In the first phase, Alice will communicate to Bob over a quantum channel. Alice begins by choosing a random string of bits and for each bit, Alice will randomly choose a basis, rectilinear or diagonal, by which to encode the bit. She will transmit a photon for each bit with the corresponding polarization, as just described, to Bob. For every photon Bob receives, he will measure the photon's polarization by a randomly chosen basis. If, for a particular photon, Bob chose the same basis as Alice, then in principle, Bob should measure the same polarization and thus he can correctly infer the bit that Alice intended to send. If he chose the wrong basis, his result, and thus the bit he reads, will be random.
In the second phase, Bob will notify Alice over any insecure channel what basis he used to measure each photon. Alice will report back to Bob whether he chose the correct basis for each photon. At this point Alice and Bob will discard the bits corresponding to the photons which Bob measured with a different basis. Provided no errors occurred or no one manipulated the photons, Bob and Alice should now both have an identical string of bits which is called a sifted key. The example below shows the bits Alice chose, the bases she encoded them in, the bases Bob used for measurement, and the resulting sifted key after Bob and Alice discarded their bits as just mentioned [Wiki-SIFT].

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Before they are finished however, Alice and Bob agree upon a random subset of the bits to compare to ensure consistency. If the bits agree, they are discarded and the remaining bits form the shared secret key. In the absence of noise or any other measurement error, a disagreement in any of the bits compared would indicate the presence of an eavesdropper on the quantum channel. This is because the eavesdropper, Eve, were attempting to determine the key, she would have no choice but to measure the photons sent by Alice before sending them on to Bob. This is true because the no cloning theorem assures that she cannot replicate a particle of unknown state [Wooters82]. Since Eve will not know what bases Alice used to encoded the bit until after Alice and Bob discuss their measurements, Eve will be forced to guess. If she measures on the incorrect bases, the Heisenberg Uncertainty Principle ensures that the information encoded on the other bases is now lost. Thus when the photon reaches Bob, his measurement will now be random and he will read a bit incorrectly 50% of the time. Given that Eve will choose the measurement basis incorrectly on average 50% of the time, 25% of Bob's measured bits will differ from Alice [Rieffel00]. If Eve has eavesdropped on all the bits then after n bit comparisons by Alice and Bob, they will reduce the probability that Eve will go undetected to $¾^n$ [Lomonaco98]. The chance that an eavesdropper learned the secret is thus negligible if a sufficiently long sequence of the bits are compared.

BB84 protocol in simple words :—

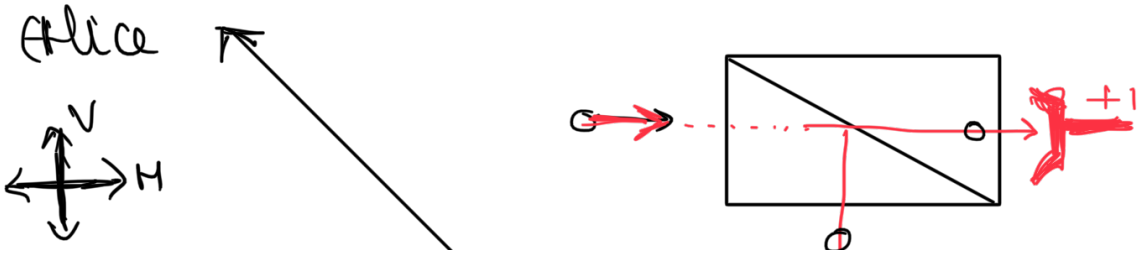


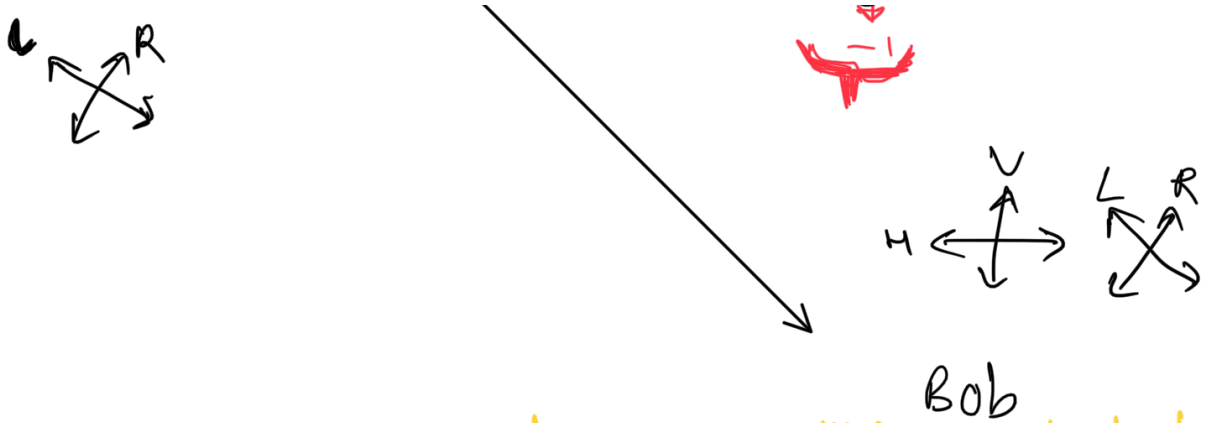
Alice ← $|\psi\rangle_1$ $|\psi\rangle_2$ $|\psi\rangle_3$ ....

(#) any measurement on an individual quantum object leaves a trace. In other words its impossible for Eve to read the Quantum information on the photon without perturbing it. This perturbation can be detected by Alice / Bob. who can communicate over classical public channel. which does not need to be secure.

The polarization of the photons turned out to be the privileged support for quantum key distr

The BB84 scheme with polarized one-photon wave packets :-





In order to generate a key, that will be sent to bo
Alice has a source of polarized photon and
she can choose a polarization of each photon
among 4 possibilities associated with 2 diff.
linear polarization basis. Two are along the
axis X and Y and are often noted V and
vertical
The two other polarization are at 45° and a
usually noted R & L for Right & Left.
Both are orthogonal polarizations. That is to
say, the 2 output channels of polarizing beam
splitter conviniently oriented the R &L
corresponds to 2 polarizing 2 beam splitter
at 45° from each other. They are assoc
two non commuting observables. When bob
receives a photon, you analyzes its polarization
with a polarization beam splitter of which it
chooses randomly the orientation b/w 2
possibilities either vertical @ 45°, if its
choice corresponds to polarization sent by
Alice, he obtains a result corresponding
to the value chosen by Alice. This is case
for instance, if Alice sends a photon wi

(V) or (H) and if it puts it [illegible] at (0°/90°) from x axis. But if we make the wrong choice that is to say if Bob puts polariser/detector in 45°/135° from x when Alice has sent H or V photon then he obtains a random result un-correlated with the initial choice of Alice. so he gets the right information in after cases only. It may seem a poor result, but infact, there is a simple way for Bob and Alice to know what were the right choices and keep these only this is called

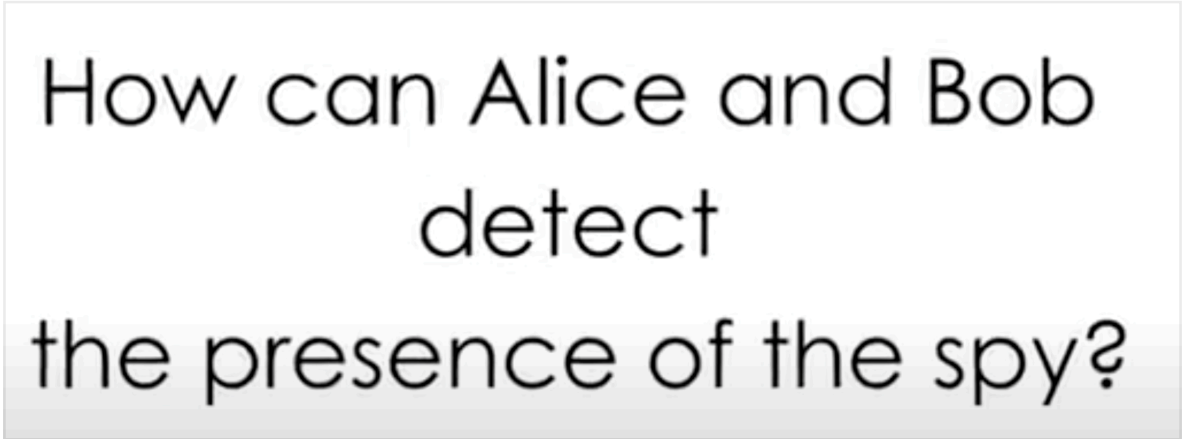
RECONCILIATION.

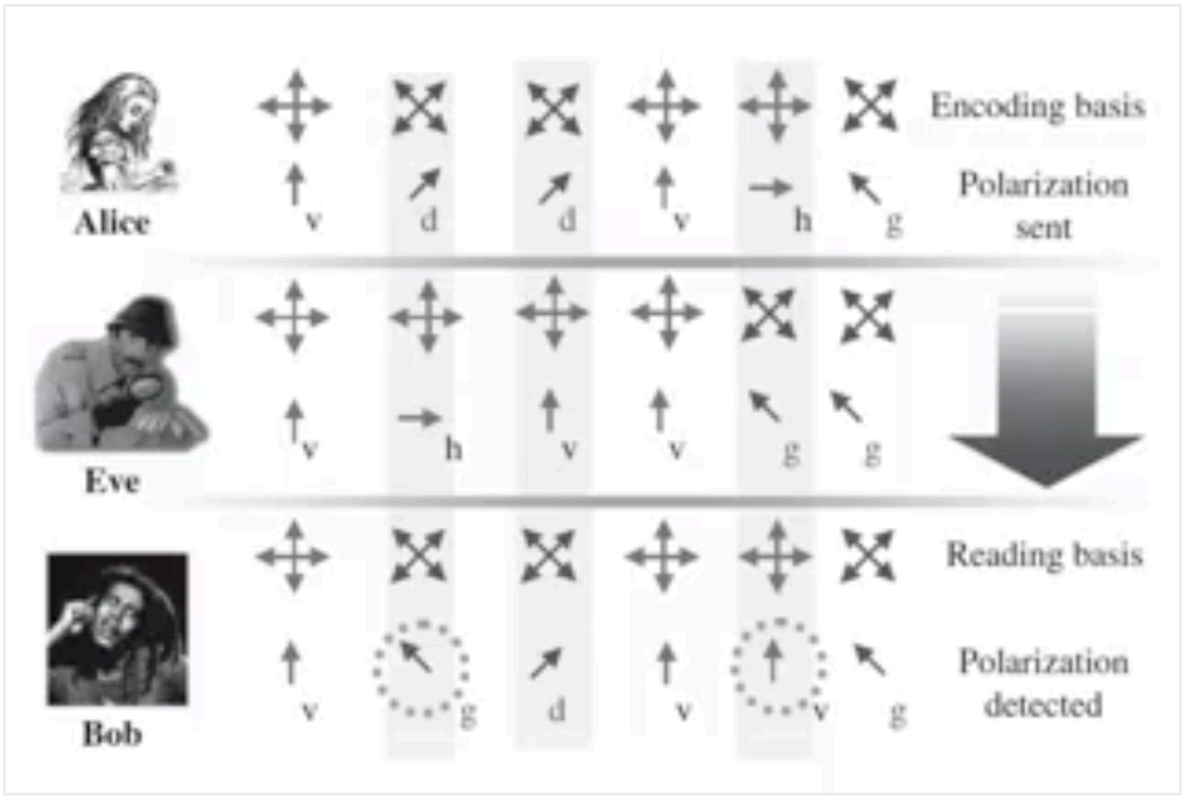
In order for Alice and Bob to know what were the right choices, its a faces that bob announces on the public channel what were the choices of basis, and then Alice replies which ones are the correct via the public channel. Alice and bob now knows what were the situation where both had right polarizatio & wrong ones. They keep only right cases.

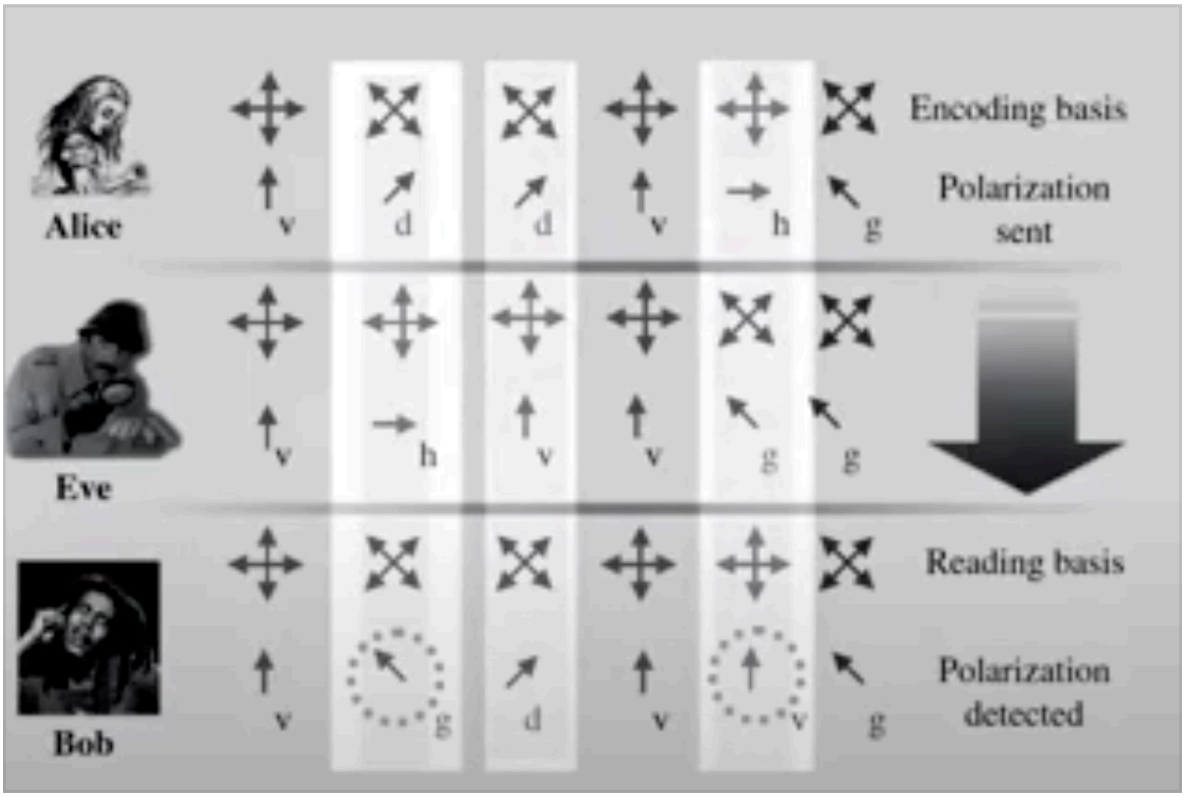
After elimination, they keep only identical cases and removes the error from final strings. The communication for chosen orientations b/w Alice and bob can happen over public channel. It can be listened to &

Trying to get copy of key :o

let us pretend we are Eve and try to obtain the same information as Bob without being detected to get information we must intercept the polarized photon and make a polarization measurement on it but that Bob will receive nothing and does this fit on this photon will not be used for the reconciliation procedure so we must be a smarter evil after doing the measurement we will use a 1 Photon Source to resend a photon towards Bob with the polarization we have just found ball will then receive a photo with a polarization that we know so if this photon is used for the key and information we will get on the public channel we will know that value of a bit indicate let us now take the point of view of Alice and Bob were as smart and know as much quantum optics as if they understand that if you do what we have just been describing measuring a photon polarization and resending a photon with the results I have just found can they detect such maneuver the answer is yes can you find how you do not find yet I'll give you a hint what Alice and Bob can do is sacrifice a subset of the key they are established after reconciliation more precisely Bob will choose randomly some of the cases where they agreed and tell on the public channel what he found in disguises with this information Alice can tell that there is an eavesdropper is there is one can you tell why I am sure most of you I found the answer let us describe it in detail since it will allow us to fully appreciate where the quantum nature of the signal plays a role the series of cases shown here allow us to understand there are cases when it does not choose a simpler ization orientation at the one decided by ELISA here it is cases number 2 3 and 5 in these cases the result found by Eve is random but this is not the point the fact is that in these cases ball will find a random result which means that in half these cases he finds the wrong direction as shown here in cases 2 & 5 so when receiving the results found by Bob in cases 2 & 5 Alice will observe that they are wrong although Bob had chosen the right basis she will thus conclude that there is a spy on the channel and 1 Bob that this game must not be used can you tell what is a fraction of the cases where Bob gets a wrong result although we have chosen the right basis




Alice
Eve
Bob
Encoding basis
Polarization sent
Reading basis
Polarization detected
v
d
d
v
h
g
v
h
v
v
g
g
v
g
d
v
v
g


Alice
Eve
Bob
Encoding basis
Polarization sent
Reading basis
Polarization detected
v
d
d
v
h
g
v
h
v
v
g
g
v
g
d
v
v
g