Quantum Cryptography: A Survey

A Study based on Quantum Key Distribution Protocols In Quantum Cryptography

Neelkamal (174101022)
Computer Science and Engineering Department
Indian Institute of Technology, Guwahati
Guwahati,India.
neeljhajharia1@gmail.com

***Abstract*— The purpose of this research paper is to provide a literature review on quantum cryptography which leads to understand the basics of quantum concept and the quantum key distribution protocols which provides the base to quantum communication and quantum cryptography. Through this paper i provide a brief introduction to quantum mechanics and quantum computation to describe the idea how quantum physics plays an important role in computation also it provides quantum-mechanical background needed to present some fundamental protocols from quantum cryptography.**

Then we discuss quantum key distribution using the BB84 protocol, quantum cryptography beyond key distribution and the challenges present in practical implementation of quantum key distribution protocols. The paper conclude with the progress and future scope of the quantum cryptography.

Keywords—Cryptography, Quantum, Protocol, Key Distribution, Perfect Security.

I. Introduction

Most digital networks generally rely on modern cryptosystems to secure the confidentiality and integrity of traffic carried across the network. Modern cryptography algorithms are based over the fundamental process of factoring large integers into their primes, which is said to be intractable. But modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics.

Also in conventional symmetric cryptographic algorithms, communication security relies solely on the secrecy of an encryption key. If two users, Alice and Bob, share a long random string of secret bits the key then they can achieve unconditional security by encrypting their message using the standard one-time-pad encryption scheme. The central question then is: how do Alice and Bob share a secure key in the first place? This is called the key distribution problem. Unfortunately, all classical methods to distribute a secure key are fundamentally insecure because in classical physics there is nothing preventing an eavesdropper, Eve, from copying the key during its transit from Alice to Bob. On the other hand, public-key cryptography solves the key distribution problem by relying on computational assumptions such as the hardness of factoring. Therefore, such schemes do not provide information theoretic security because they are vulnerable to future advances in hardware and algorithms, including the construction of a large-scale quantum computer. Quantum cryptography, or more specifically, quantum key distribution (QKD)[1][5], promises in principle unconditional security.

Quantum cryptography is an emerging technology in which two parties can secure network communications by applying the phenomena of quantum physics. As the security of these transmissions is based on the inviolability of the laws of quantum mechanics, it remains secure against an adversary with unlimited computing power.

The scope of this research paper is to understand the fundamental concept of quantum cryptography, quantum key distribution techniques, quantum networks and protocols. In particular, we will review quantum key distribution via the BB84 protocol. After that we discuss other aspects of quantum cryptography under the following headings quantum cryptography beyond key distribution, providing challenges which are present in establishing quantum cryptography based network. threats to security and challenges present in quantum cryptosystem, identify the problem with present quantum cryptosystem and the real world implementation of this technology.

II. The Concept Of Quantum

A. What is Quantum ?

In physics, a quantum is the minimum amount of any physical entity involved in an interaction. the magnitude of the physical property can take on only discrete values consisting of integer multiples of one quantum.

For example, a photon is a single quantum of light. Similarly, the energy of an electron bound within an atom is also quantized, and thus can only exist in certain discrete values. Atoms and matter in general are stable because electrons can only exist at discrete energy levels in an atom. Quantization is one of the foundations of the much broader physics of quantum mechanics.

B. The Development of Quantum Theory.

- In 1900, Planck made the assumption that energy was made of individual units, or quanta.
- In 1905, Albert Einstein theorized that not just the energy, but the radiation itself was *quantized* in the same manner.
- In 1924, Louis de Broglie proposed that there is no fundamental difference in the makeup and behavior of energy and matter; on the atomic and subatomic level either may behave as if made of either particles or waves. This theory became known as the *principle of wave-particle duality*: elementary particles of both energy and matter behave, depending on the conditions, like either particles or waves.
- In 1927, Werner Heisenberg proposed that precise, simultaneous measurement of two complementary values - such as the position and momentum of a subatomic particle - is impossible. Contrary to the principles of classical physics, their simultaneous measurement is inescapably flawed; the more precisely one value is measured, the more flawed will be the measurement of the other value. This theory became known as the uncertainty principle, which prompted Albert Einstein's famous comment, "God does not play dice."
- The Copenhagen Interpretation- The two major interpretations of quantum theory's implications for the nature of reality are the Copenhagen interpretation and the many-worlds theory. Niels Bohr proposed the Copenhagen interpretation of quantum theory, which asserts that a particle is whatever it is measured to be, but that it cannot be assumed to have specific properties, or even to exist, until it is measured. This translates to a principle called superposition that claims that while we do not know what the state of any object is, it is actually in all possible states simultaneously, as long as we don't look to check.To illustrate this theory, we can use the famous and somewhat cruel analogy of Schrodinger's Cat.

III. The Concept of Qubit

A. Quantum Bit

In quantum computing, a qubit or quantum bit is a unit of quantum information. The quantum analogue of the classical binary bit. A qubit is a two-state quantum-mechanical system, such as the polarization of a single photon.Classical computers encode information in bits. Each bit can take the value of 1 or 0. These 1s and 0s act as on/off switches that ultimately drive computer functions. Quantum computers, on the other hand, are based on qubits, which operate according to two key principles of quantum physics: superposition and entanglement[15].

Using these two principles, qubits can act as more sophisticated switches, enabling quantum computers to function in ways that allow them to solve difficult problems that are intractable using today's computers.

B. Quantum Superposition

It is a fundamental principle of quantum mechanics. It states that any two (or more) quantum states can be added together and the result will be another valid quantum state and conversely, that every quantum state can be represented as a sum of two or more other distinct states as shown in Fig. 1.

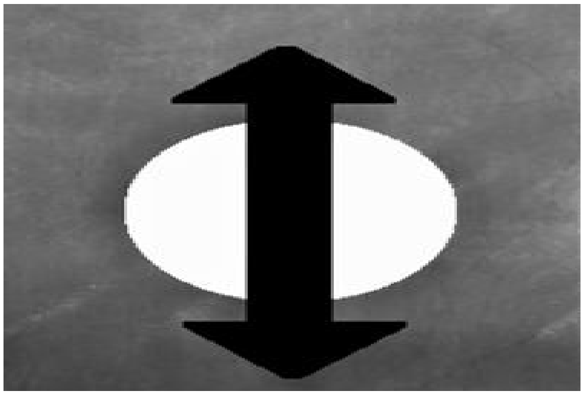


Fig. 1 Quantum Superposition

Or we can say that superposition means that each qubit can represent both a 1 and a 0 at the same time i.e. linear superposition of the "basis states" $|1\rangle$ and $|0\rangle$ here $|0\rangle$ and $|1\rangle$ are the Dirac notation for the quantum state that will always give the result 0 and 1 respectively when converted to classical logic by a measurement.

C. Quantum Entanglement

It is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated.This leads to correlations between observable physical properties of the systems. For example, it is possible to prepare two particles in a single quantum state such that when one is observed to be spin-up, the other one will always be observed to be spin-down and vice versa, this despite the fact that it is impossible to predict, according to quantum mechanics, which set of measurements will be observed.

As a result, measurements performed on one system seem to be instantaneously influencing other systems entangled with it. But quantum entanglement does not enable the transmission of classical information faster than the speed of light. Entanglement means that qubits in a superposition can be correlated with each other; that is, the state of one (whether it is a 1 or a 0) can depend on the state of another as shown in Fig. 2.

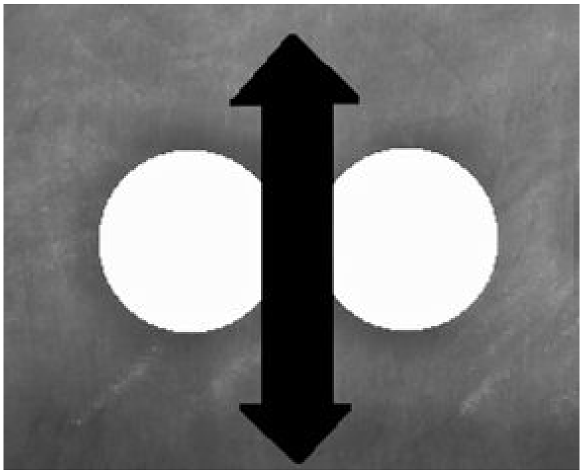


Fig. 1 Quantum Entanglement

D. Operations On Pure Qubit States

There are various kinds of physical operations that can be performed on pure qubit states.

- A quantum logic gate can operate on a qubit: mathematically speaking, the qubit undergoes a unitary transformation. Unitary transformations correspond to rotations of the qubit vector in the Bloch sphere.
- Standard basis measurement is an operation in which information is gained about the state of the qubit. The result of the measurement will be either $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$ .Measurement of the state of the qubit alters the values of α and β. For instance, if the result of the measurement is $|0\rangle$, α is changed to 1 (up to phase) and β is changed to 0. Note that a measurement of a qubit state entangled with another quantum system transforms a pure state into a mixed state.

E. Representation Qubit States

In general, a quantum state |ψ> is an element of a finite-dimensional complex vector space (or Hilbert space)H,, in which we can introduce an orthonormal basis, consisting of the two states |0> and |1>.. Unlike its classical counterpart, the quantum state can be in any coherent[10] superposition of the basis states:

|ψ>=α|0>+β|1>.

Where α and β are, in general, complex coefficients.It is convenient to deal with normalized states, so we require <ψ|ψ>=1 for all states|ψ> that have a physical meaning.This is due to the fact that the quantum mechanical equation of motion, the Schr¨ odinger equation, is linear: Any linear superposition of its solutions (the quantum states) is also a solution. Since we require quantum states to be normalized, we find that the coefficients in (1) have to fulfill $|\alpha|^2 + |\beta|^2 = 1$ where|·|denotes the absolute value.

The physical meaning of |ψ>=α|0>+β|1> can most easily be understood when we measure the quantum state|ψ>. In quantum mechanics, this is achieved by a positive operator valued measurement(POVM).

Bloch sphere

It might, at first sight, seem that there should be four degrees of freedom, as α and β are complex numbers with two degrees of freedom each. However, one degree of freedom is removed by the normalization constraint $|\alpha|^2 + |\beta|^2 = 1$, which can be treated as the equation for a 3-sphere embedded in 4-dimensional space with a radius of 1 (unit sphere). This means, with a suitable change of coordinates, one can eliminate one of the degrees of freedom. One possible choice is that of Hopf coordinates:

$$\alpha = e^{i\psi} \cos\frac{\theta}{2},$$
$$\beta = e^{i(\psi+\phi)} \sin\frac{\theta}{2}.$$

Additionally, for a single qubit the overall phase of the state $e^{i\,\psi}$ has no physically observable consequences, so we can arbitrarily choose α to be real (or β in the case that α is zero), leaving just two degrees of freedom:

$$\alpha = \cos\frac{\theta}{2},$$
$$\beta = e^{i\phi} \sin\frac{\theta}{2}.$$

The possible states for a single qubit can be visualised using a Bloch sphere. As shown in Fig. 3.

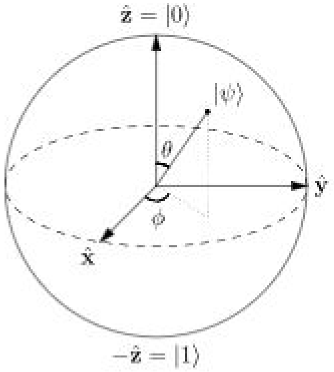


Fig. 3 Bloch Sphere Representation

Represented on such a sphere, a classical bit could only be at the "North Pole" or the "South Pole", in the locations where | 0 〉 and | 1 〉 are respectively. The rest of the surface of the sphere is inaccessible to a classical bit, but a pure qubit state can be represented by any point on the surface. For example, the pure qubit state $|0 >+ i|1 > /\sqrt{2}$ would lie on the equator of the sphere, on the positive y axis.

The surface of the sphere is a two-dimensional space, which represents the state space of the pure qubit states. This state space has two local degrees of freedom.

It is possible to put the qubit in a mixed state, a statistical combination of different pure states. Mixed states can be represented by points inside the Bloch sphere. A mixed qubit state has three degrees of freedom: the angles φ and θ, as well as the length r of the vector that represents the mixed state.

IV. BB84 Quantum Key Distribution Protocol

A. Why we need QKD?

Classical cryptography is based on the computational difficulty to compute the secret key using the current computing systems. Depending only on the difficulty of computational complexity does not provide enough security because finding a fast method to calculate the secret key will compromise the security of the systems. Quantum computing uses the law of physics for communication allowing new concepts to be applied in computing especially in cryptography and key distribution by applying quantum theorems and principles whose security can't be compromised which we will observe and prove in this section.

B. Necessary Conditions for QKD

There are two parties want to communicate i.e. Alice and Bob which generates keys K_A and K_B respectively. Also we have an eavesdropper Eve which we assume have access to all computation power. In this scenario a QKD protocol should satisfy two conditions -

(i) ε-Correctness: $Pr(K_A \neq K_B) \leq \varepsilon$ where K_A and K_B are Shared Quantum key produced by "Alice" and "Bob" and ε is small error probability.

(ii) ε-Secrecy: $\rho_{K_A} \approx_{\varepsilon} I/\left|K_A\right| \otimes \rho_E$ which provides the trace distance between ρ and σ is small.

The definition of the trace distance is precisely related to how well the two states can be distinguished. So if two states are epsilon close in trace distance, where epsilon is extremely small,this means that no process in the universe can distinguish the states very well.In particular it also means that if we were to use a key inside a larger protocol,for example in a one time pad encryption scheme that uses the key produced by quantum key distribution,then the resulting protocol will hardly see any difference whether we used the real state or the ideal state where Eve is completely ignorant.This is because if it could see a difference this would constitute a measurement that would allow us to distinguish the real from the ideal case but we precisely know that this is impossible by the properties of the trace distance.

C. Distribution of BB84 States

- **BB84 States**

  This protocol uses a special class of states, namely the BB84[8] states. There are four of them-

  |0>,|1> are standard basis,

  |+>,|-> are hadamard basis where $|+>= (1/\sqrt{2})\,(|0>+|1>)$ and $|->= (1/\sqrt{2})\,(|0>-|1>)$

  The elements of the standard basis are the eigenstates of Pauli Z.And the elements of the Hadamard basis are the eigenstates of Pauli X.

- **BB84 Measurements**

  We can measure these states in these four basis-

  |0>,|1> i.e in standard basis and |+>,|-> which are hadamard basis.

- **Steps To Distribute States Between Two Parties**

  To execute this protocol, Alice and Bob need a quantum channel to deliver qubits to each other. In addition assume that they have a classical authenticated channel.

(i) Alice chooses a random $N = (4+n)n$ bit string $x_A = x_1, x_2, ..., x_N$.

(ii)Alice chooses a random N bit base string $\theta_A = \theta_1, \theta_2, ..., \theta_N$.

Bob chooses a random N bit base string $\widehat{\theta}_A = \widehat{\theta}_1, \widehat{\theta}_2, ..., \widehat{\theta}_N$ for $1 \leq j \leq N$.

(iii)Alice sends to Bob bit x_j encoded in base $\theta_j : |x_j >_{\theta_j}$.

(iv) Bob measure the qubit in the basis $\widehat{\theta}_j$ to obtain outcome $\widehat{x}_j$.

Let's say Alice chooses a basis 0 or 1, where 0 is for the standard and 1 for the Hadamard basis. She also chooses a random bit x_A. She sends that bit encoded in the basis θ to Bob.

Bob also chooses a random basis standard or Hadamard, and will measure the incoming qubit in that basis.This gives him some classical measurement outcome which is $\widehat{x}$.

Here we can observe. If Alice and Bob have the same basis then in fact their bits will agree. Because in our actual protocol there might be an eavesdropper Eve trying to intercept the qubit and we know Eve cannot clone the qubit.

Hence If Eve could clone the standard basis, then she cannot clone the Hadamard basis.

We will do this procedure many times.

At the end Alice has a string x, and a basis string θ which says which bit was measured in which basis.Bob also has a string $\hat{x}$, namely the string corresponding to his measurement outcomes.He also remembers which bases he measured in, so he has the string $\hat{\theta}$.

Now by our little observation as before we know that if they measured in the same basis,then the bits agree.

D. BB84 Protocol

- Alice and Bob distribute BB84 states.
- Bob announces receipt of the states.
- Alice and Bob exchange bases strings θ_A, $\widehat{\theta}_B$

  They discards all rounds where $\hat{\theta}_j \neq \theta_j$.
- Alice randomly chooses n of the remaining rounds to test. She tells Bob which rounds are tested. Alice and Bob exchange bits x_j, $\hat{x}_j$ for those rounds.

  Alice and Bob compute error rate δ. If it exceeds a threshold they abort the protocol.
- Information reconciliation: Alice sends error-correcting information C to Bob.
- Privacy Amplification: Alice chooses an extractor seed y and sends it to Bob.

  Alice computes $K_A = Ext(X_{A,remain}, Y)$.

  Bob computes $K_B = Ext(X_{B,remain}, Y)$.

The first thing we will do is to distribute BB84 states and these strings agree whenever they measured in the same basis.

Bob will announce receipt of these states. Now Alice and Bob will actually tell each other which bases they have measured in and they will discard all the rounds where they used a different basis.We are now in a situation where they share a shorter string, namely, a string corresponding to all the positions where they measured in the same basis.

So if there is no noise by the property all of the bits should now agree They test whether there are any errors. Alice chooses half of the remaining rounds to test. She tells Bob which rounds are tested and Bob exchanges the bits corresponding to those rounds.

Is Bob's measurement outcome exactly equal to the bit x that Alice prepared? From this Alice and Bob can compute an error rate, that we will call δ which is equal to the number of incorrect bits, the number of positions of the tested bits. If there is no noise. So we don't expect any error, the error rate should be zero. Eve may have maybe some knowledge about the string. Alice is going to choose an extractor seed y and send it to Bob. Alice computes K_A, namely the extractor function applied to the remaining bit string and the seed y. Similarly Bob computes K_B, the extractor function applied to his remaining string and extracts the seed y. This is our protocol.

E. Checking Correctness And Secrecy

Correctness: First we have to check that the protocol is correct. This means that K_A should be equal to K_B.Why would this be the case? If there is no noise, the string that Alice has, the remaining string is in fact exactly the same as Bob's remaining string. So if they apply the extractor function to the same inputs, the same string x and the seed y, they get the same outputs K_A equals K_B. Hence the protocol is correct. If there is error on the channel the two remaining strings will very likely not be the same.

In fact the probability that they are the same, if there is even a very tiny bit of noise and the string is very long, is very small. So we now need to add an extra step, error-correction so that we not need to abort the process on seeing just a single error. We are only going to abort the process only if the error exceeds a certain threshold. Now Alice is going to send some error correcting information C to Bob. If the remaining strings may not have been the same a prior ,but the error correcting information, as before, allows Bob to correct these errors. So we are again back to a situation where x_A remain is actually equal to x_B , the remaining string of Bob with a very high probability. So the protocol is again correct.

Secrecy: We will check now Is the protocol secure? The intuition is that if Eve tries to tamper at all with the qubits, then with very high probability the test that Alice and Bob will perform catches her out.So the probability that Eve tried to tamper and they still don't see any errors is very small. In a real implementation, it is completely impossible that there is no noise, even if they measure in the same basis. Also that Eve can always eliminate all errors,so all errors could potentially be due to the eavesdropper Eve. Alice and Bob can actually still make key even if Eve introduces some, but not too many errors. If Eve tries to tamper with the channel, then she will introduce errors and we can use the magnitude of these errors to make an estimate of how much Eve will have tampered. The more errors there are, the more Eve may have learned. In particular, there will be a theorem, that says that the minimum entropy that Eve has about the remaining string is never smaller than n times one minus the binary entropy of this error rate which we call privacy amplification in the context of we know that Eve will be ignorant or almost ignorant about the resulting key. We need to show that Eve has high min entropy about the string x_A remain.

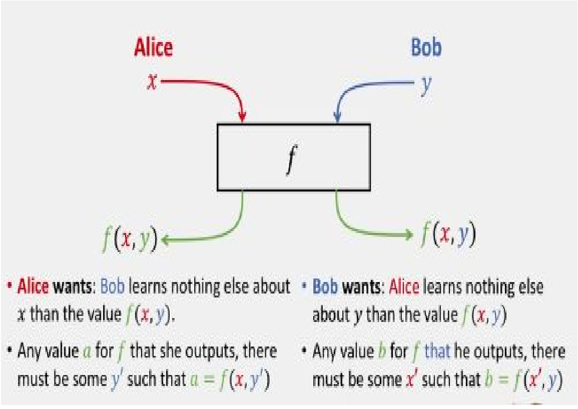
V. Quantum Cryptography Beyond Key Distribution

In this section we discuss multiparty cryptography where the users, Alice and Bob and sometimes their comrades engage in a simple task, such as flipping a coin or computing a function. But now they no longer trust each other. We then try to find protocols that are secure from the point of view of the honest party, irrespective of possible malicious behavior from the other parties. The two most important examples of tasks in two-party cryptography are oblivious[4] transfer and bit commitment.

A. Multiparty Communication

Multiparty computation, also sometimes called secure function evaluation. The general setup for the task of secure function evaluation is assume there's Alice, and there's Bob and both of them are trying to compute the same function, f. Everyone knows what the function is. But Alice has an input, x, that's secret to her. And Bob has an input, y, that is secret to him. Now, Alice should be able to put her input x into this protocol, and Bob puts his input y into this protocol and at the end of the protocol, each of them should learn the outcome. Also Alice wants to be sure that whatever Bob is going to do in the protocol, he cannot learn more about her input x than he can infer by looking at the output f(x,y) and same fo Bob.What if Alice has some value for f in mind, and she wants to force Bob to think that the outcome of the function f is a particular value? So we want one extra condition here namely,that whatever value the output of the computation takes,it is actually consistent with the protocol.So let's take that the output of the computation is a.Then Alice want to be sure that there exists some input y for Bob such that a is equal to f(x,y). So that's the task of secure function evaluation which we want to solve by just communicating over some communication as mentioned in Fig. 4.

.



- Alice wants: Bob learns nothing else about x than the value $f(x,y)$.
- Any value a for f that she outputs, there must be some y' such that $a = f(x,y')$
- Bob wants: Alice learns nothing else about y than the value $f(x,y)$
- Any value b for f that he outputs, there must be some x' such that $b = f(x',y)$

Fig. 4 Secure Function Evaluation Task

B. Quantum Protocol For Oblivious Transfer

Oblivious Transfer

In OT protocol a sender transfers one of potentially many pieces of information to a receiver, but remains oblivious as to what piece (if any) has been transferred. A more useful form of oblivious transfer called 1–2 oblivious transfer or "1 out of 2 oblivious transfer".It is generalized to "1 out of *n* oblivious transfer" where the user gets exactly one database element without the server getting to know which element was queried, and without the user knowing anything about the other elements that were not retrieved.

Ideal Functionality

An ideal functionality is a protocol in which a trusted party that can communicate over perfectly secure channels with all protocol participants computes the desired protocol outcome.

Universal Composability

The framework of universal composability is a general-purpose model for the analysis of cryptographic protocols. It guarantees very strong security properties. Protocols remain secure even if arbitrarily composed with other instances of the same or other protocols.

Impossibility Results

There exists no bit commitment protocol that is universally composable in the Standard Model. The intuition is that in the ideal model, the simulator has to extract the value to commit to from the input of the environment. This would allow the receiver in the real protocol to extract the committed value and break the security of the protocol. This impossibility result can be applied to other functionalities.

Oblivious Transfer Protocol

In oblivious transfer, Alice can transfer over one of her two strings to Bob. She doesn't know which string Bob got to learn and Bob only gets to learn one of the two strings, but not both of them.

For any dishonest Bob in our protocol, there exists a simulator that interacts with the ideal functionality and in doing so produces the exact same result as the dishonest Bob, then we'll say that the protocol is secure against the dishonest Bob. The only thing Bob can do is lie about his input, which is something that we'll never be able to prevent anyways.So that's the notion of security. It's a very strong notion of security. It's necessary if we want protocols to be composable. this definition achieves universal composability unfortunately it's so strong that it makes a lot of things impossible to achieve, at least with perfect security.But we can implement it under computational assumptions.So for instance, the existence of one-way functions and in that case, we can derive the whole of multiparty computation just from our implementation of oblivious transfer.

The protocol follow these steps:

(i) Alice prepares a bunch of BB84 states, 2n of them.

(ii) Alice is going to choose randomly some angles, θ_i ,random bases, and some bits,x_i for $1 \leq i \leq 2n$ and she send to Bob the corresponding BB84 states. So x_i encoded in basis θ_i .

(iii) Bob receives the states and he measures them in random bases. Bob will choose some $\widehat{\theta}_i$ and he measures and obtains some outcomes $\widehat{x}_i$.

(iv) Once he's done, he tells Alice, “done”.

(v) Then Alice sends over to Bob her basis choices i.e θ_1 up to θ_{2n} .

(vi) Bob define two sets, I is the set of indices i in which he made the correct guess i.e. $\theta_i = \widehat{\theta}_i$ and $\bar{I}$ is the set of i such that $\theta_i \neq \widehat{\theta}_i$. For simplicity, let me assume that each of these sets has the same size n. Bob set an interval I_Y , depending on his input Y . $I_Y = I, I_{1-Y} = \bar{I}$ and send I_0 and I_1 over to Alice.Depending on his input Y . Bob puts the set of bases that he correctly guessed either in I_0 , if Y is equal to 0, or I_1 , if y is equal to 1. Alice doesn't know this.

(vii) Alice gets these sets, and replies with her bits xor-ed with her secret string depending on the interval I . She sends $t_0 = x_{I_0} \oplus S_0$ and $t_1 = x_{I_1} \oplus S_1$ to Bob.

(viii) Bob simply outputs S_Y , which will be equal to what he received from Alice for the y. Bob will compute t_Y parity with his own output, $\widehat{x}$ and I_Y .

This protocol is correct but the protocol is not secure against cheating Bob as Bob say done without having measured, then he'll wait for Alice's bases theta, and then only measure using the basis information he got from Alice. So Alice is giving away too much information here. She's trusting that he's measured when he says he's measured.

Security Against The Attack

Now there's two ways around this-

(i) To enforce a little bit stronger assumptions, put a technological requirement on Bob.This is called the bounded storage model.

(ii) Another way to use the idea of a commitment Alice will instead of asking Bob to just say done and trusting him on faith is to ask him to commit. So we'll replace this by a commitment.

C. Bit Commitment Scheme

A commitment scheme will have two phases

(i) **Commit Phase**: In the commit phase, Alice thinks of a single bit ‘r’. Alice puts her bit inside the envelope.

(ii) Open Phase: Bob is given access to the envelope. Bob can open the envelope and recover the secret bit,’r’, that Alice put inside the envelope.

This scheme should satisfy these conditions-

(i) **Correctness Condition:** If both Alice and Bob execute the bit commitment protocol correctly, then it should be the case that the bit Bob recovers when he opens the envelope, ‘r’, is exactly the bit ‘r’ that Alice placed inside the envelope. That's if the users follow the honest behavior.

(ii) **Binding Condition:** The probability that Alice can convince Bob that she committed to a 0 and the probability that Alice can convince Bob that she committed to a 1 should be, at most, 1.

(iii) **Epsilon Binding Condition**: In the setting of epsilon security if the probability that Alice is able to convince Bob that she committed to a 0 is 1, then the probability that she committed to a 1 should be 0,or should be at most epsilon, which is going to be a negligible function.

(iv) **Hiding Condition:** At the end of the commit phase, Bob has no information about ‘r’.

Alice wants the commitment to be hiding. More formally, we thus have a joint state of the bit r and Bob's system b is close to being uniform on r and uncorrelated from Bob.This is the commitment scheme which satisfies these two conditions.It is binding.Alice can not change her mind.And it is hiding.Bob cannot learn the bit ahead of time.

Oblivious transfer can be used to implement any multiparty function, so oblivious transfer implies bit commitment. Bit commitment can be used to implement OT in the quantum case. So if we can implement the bit commitment,then we can implement everything.By analysing the protocol we can observe that hiding implies not binding.These two weak security requirements contradict each other. And as a consequence, bit commitment is not possible, even in the quantum case. Also there is no perfectly secure non-trivial computation of multiparty functions in the very strong notion of security. The idea is same for the impossibility of commitment schemes.Now that impossibility result applies to protocols that have perfect security or near perfect security. But we can still ask the question if there wouldn't exist some functionalities, oblivious transfer, bit commitment, maybe others, that can be obtained, constructed with somehow stronger guarantees using quantum protocols than classical protocols and this turns out to be the case called coin tossing, where even though we can't do it perfectly, there is an advantage to quantum communication.

VI. Challenges In Key Distribution

Quantum key distribution (QKD) promises unconditional security in data communication and is currently being deployed in commercial applications. But in today's scenario various challenges exist in practical implementation of QKD which we will discuss in this section.

Security loopholes in QKD are closely related to loopholes in Bell[7] inequality tests is a key subject in the foundations of quantum mechanics. The so-called collective attacks is an important challenge for an implementation however, information-theoretic security is achieved only when security against the most general attacks is proven. several QKD protocols have been demonstrated to provide composable security against collective attacks using reasonable data block sizes and practical setups, including decoy-state[11] BB84, coherent-one-way, and CV-QKD.

A. Possible Attacks On Existing QKD Protocols

The photon-number-splitting attack

In the BB84 protocol Alice sends quantum states to Bob using single photons. The most pulses actually contain no photons (no pulse is sent), some pulses contain 1 photon (which is desired) and a few pulses contain 2 or more photons. If the pulse contains more than one photon, then Eve can split off the extra photons and transmit the remaining single photon to Bob. This is the basis of the photon number splitting[12] attack, where Eve stores these extra photons in a quantum memory until Bob detects the remaining single photon and Alice reveals the encoding basis. Eve can then measure her photons in the correct basis and obtain information on the key without introducing detectable errors.

There are several solutions to this problem. The most obvious is to use a true single photon source instead of an attenuated laser.

The most promising solution is the decoy state protocol, in which Alice randomly sends some of her laser pulses with a lower average photon number. These decoy states can be used to detect a PNS attack, as Eve has no way to tell which pulses are signal and which decoy.

The counter detector side-channel attacks

A side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself the need to counter these attacks has led to the discovery of measurement device independent[13] (MDI) QKD.

Denial of service

Because currently a dedicated fibre optic line is required between the two points linked by quantum key distribution, a denial of service attack can be mounted by simply cutting or blocking the line. This is one of the motivations for the development of quantum key distribution networks, which would route communication via alternate links in case of disruption.

Man-in-the-middle attack

Quantum key distribution is vulnerable to a man-in-the-middle[14] attack when used without authentication to the same extent as any classical protocol, since no known principle of quantum mechanics can distinguish friend from foe.

Intercept and resend

The simplest type of possible attack is the intercept-resend attack, where Eve measures the quantum states (photons) sent by Alice and then sends replacement states to Bob, prepared in the state she measures. To detect an eavesdropper with probability P= 0.999999999 Alice and Bob need to compare n = 72 key bits.

Trojan-horse attacks

A quantum key distribution system may be probed by Eve by sending in bright light from the quantum channel and analyzing the back-reflections in a Trojan-horse[17] attack. In a recent research study it has been shown that Eve discerns Bob's secret basis choice with higher than 90% probability, breaching the security of the system.

B. Secure Key Rate

The secure key rate achieved by the underlying QKD layer in a typical application scenario is crucial. Higher secure rates allow for a more frequent update of encryption keys in symmetric ciphers, and for a proportional increase in the one-time-pad communication bandwidth as this scheme requires the key to be as long as the message. Presently, strong disparity exists between the classical and QKD communication rates. Classical optical communications delivering speeds of 100 Gbit/s per wavelength channel are currently being deployed, On the other hand, the Mbit/s rates achieved by QKD systems today are sufficient but if we want in the longer term to encrypt high volumes of classical network traffic using the one-time-pad, major developments on the secure key rate generated by QKD will be required.

C. Communication Over Large Distance

Extending the communication range of QKD systems is a major driving factor for technological developments in view of future network applications. Also the point-to-point distance is increasingly unappealing because the channel loss will inevitably reduce the key rate to a level of little practical relevance. This is also true for CV-QKD systems, which are in general more sensitive to losses. Here it is crucial to keep the excess noise. Hence distance is a major factor in QKD.

To extend the distance of secure QKD we can use these approaches:

- The first approach says that by setting up trusted nodes, for instance, every 50 km, to relay secrets, it is possible to achieve secure communication over arbitrarily long distances.
- The second approach is quantum repeaters, which remove the need for the users to trust the relay nodes. But quantum repeaters are beyond current technology,
- The third approach is ground-to-satellite QKD. By using one or a few trusted satellites as relay stations, it is possible to extend the distance of secure QKD to the

global scale. China has successfully launched the world's first Quantum Satellite which is able to successfully sent the data over a distance of 1,200 kilometers from space to Earth, which is up to 20 orders of magnitudes more efficient than that expected using an optical fiber of the same length, the researchers claimed. It's also further than the current limits of a few hundred kilometers

D. Mobile Quantum Key Distribution Network

The studies in free-space QKD may also open the door to mobile QKD networks. In such a network, the mobility of QKD platforms requires the network to be highly reconfigurable where QKD users should be able to automatically determine the optimal QKD route in real time based on their locations. Furthermore, due to the strong ambient light, an effective filtering scheme is required to selectively detect quantum signals. Recent studies analyze the effect of fading and of atmospheric turbulence to CV-QKD[16] and show that CV-QKD with coherent detection could be robust against ambient noise photons due to the intrinsic filtering function of the local oscillator. QKD at microwave wavelengths, which are widely used in wireless communications, might be feasible over short distances. Driven by various potential applications, we can expect that mobile QKD will become an active research topic in the coming years.

Cost and robustness

Chip-scale integration will bring high level of miniaturisation, leading to compact and light-weight QKD modules that can be mass-manufactured at low cost. Development of chip-scale QKD is still at its early stages. Further research in this direction will help bring the QKD technology closer to its wide adoption.

VII. Conclusion

In this paper, we have discussed quantum key distribution, quantum cryptography beyond key distribution and important challenges in practical QKD. As the lead application of the field of quantum information processing, advances in QKD will have important implications in many other applications too.

A great range of quantum communication protocols beyond QKD include, for instance, quantum bit commitment, quantum secret sharing, quantum coin flipping, quantum fingerprinting, quantum digital signatures, blind quantum computing and position-based quantum cryptography. For quantum bit commitment and position-based quantum cryptography are can not be perfectly achieved with unconditional security. However, the protocols which are based on relativistic constraints or on noisy storage assumptions, where by assuming that it is impossible for an eavesdropper to store quantum information for a long time, one can retrieve security for such protocols. Factors preventing wide adoption of quantum key distribution outside high security areas include the cost of equipment, and the lack of a demonstrated threat to existing key exchange protocols. However, with optic fibre networks already present in many countries the infrastructure is in place for a more widespread use.

The formidable developments that can be expected in the next few years will mark important milestones towards the quantum internet[9] of the future.

References

[1] Bennett, C. H. & Brassard, G. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*..

[2] W. Wootters and W. Zurek, "The no-cloning theorem".

[3] Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing.

[4] Kilian, Joe *Founding cryptography on oblivious transfer*.

[5] Eleni Diamanti, Hoi-Kwong Lo,Bing Qi & Zhiliang Yuan "Practical Challenges in Quantum Key Distribution Review Article".

[6] Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.*

[7] Ekert, A. K. Quantum cryptography based on Bell's theorem.

[8] Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol.

[9] Kimble., H. J. The quantum internet.

[10] Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states.

[11] Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution.

[12] Wang, X.-B. Beating photon-number-splitting attack in practical quantum cryptography.

[13] Lo, H.-K., Curty, M. & Qi, B. Measurement device independent quantum key distribution.

[14] A. Henochowicz, Minitrue: Man-in-the-middle Attacks Enabled by CNNIC, China Digital Times

[15] Ma, X., Fung, C.-H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources.

[16] Pirandola, S. *et al.* Reply to 'Discrete and continuous variables for measurement-device-independent quantum cryptography'.

[17] Jain, N. *et al.* Risk analysis of trojan-horse attacks on practical quantum key distribution systems. *IEEE J. Sel. Topics Quantum Electron*.