Some Aspects of Quantum Cryptography and Network Security

Jaydip Sen¹, Piyali Roy Chowdhury², Indranil Sengupta¹
¹Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur-721302, INDIA
²Department of Computer Science and Engineering
Future Institute of Engineering and Management, Kolkata-700150, INDIA
emails: sen_jaydip@yahoo.com, roychowdhury.piyali@gmail.com, isg@iitkgp.ac.in

Abstract- Quantum mechanics is the current best description of the world as we know it. Experiments have shown that quantum predictions are accurate up ten places of decimal. In quantum cryptography much work has been devoted to the study of Quantum Key Distribution (QKD). The purpose of QKD is to securely distribute secret keys between the users in a network. As a result, several quantum cryptographic protocols have been implemented and tested after the advent of quantum computing. In this paper, we have given a brief overview of QKD, and some practical networks that integrate QKD in the current Internet security architecture. We have also discussed some aspects of quantum network security with particular attention to Byzantine Agreement Protocol.

I. INTRODUCTION

The purpose of cryptography is to transmit information in such a way that access to it is restricted entirely to the intended recipient. Originally, the secrecy of a cipher text depended on the secrecy of the entire encryption and decryption procedures. However, today we use ciphers for which the algorithms for encryption and decryption could be revealed to anybody without compromising the security of a particular cryptogram. In such ciphers, a set of specific parameters, called a ‘key’ is supplied together with the plaintext as an input to the encryption algorithm. The key and the cryptogram together form the input to the decryption algorithm. The encryption and decryption algorithms are publicly announced. The security of the cryptogram depends entirely on the secrecy of the key, and this key must consist of any randomly chosen, sufficiently long string of bits.

While classical cryptography employs various mathematical techniques to prevent eavesdroppers from learning the contents of encrypted messages, in quantum mechanics the information is protected by the laws of physics. In classical cryptography, an absolute security of information cannot be guaranteed. The Heisenberg’s Uncertainty Principle and quantum entanglement (Section III) can be exploited in a system of secure communication, often referred to as “Quantum Cryptography” [12]. Quantum Cryptography provides means for two parties to exchange a secret shared key over a private channel with complete security of communication.

There are at least three major types of quantum cryptosystem for key distribution. They are as follows: (i) Cryptosystems with encoding based on two non-commuting observables proposed by S. Weisner (1970) and by C.H. Bennett and G. Brassard (1984)[13]. (ii) Cryptosystems with encoding built upon quantum entanglement and Bell theorem proposed by A.K. Ekert (1990) [14][15]. (iii) Cryptosystems with encoding based on two non-orthogonal state vectors proposed by C.H. Bennett (1992) [16].

A quantum cryptosystem of type (i) includes a transmitter and a receiver. The sender may use the transmitter to send photons in one of the four polarizations 0, 45, 90 or 135 degrees. A recipient at the other end uses the receiver to measure the polarization. According to the laws of quantum mechanics, the receiver can distinguish between rectilinear polarizations (0 or 90) or it can quickly be reconfigured to discriminate between diagonal polarizations (45 and 135). It can never, however, distinguish both types. The key distribution requires several steps. The sender sends photons with one of the four polarizations, which are chosen at random. For each incoming photon, the receiver chooses at random the type of measurement: either the rectilinear type or diagonal type. The receiver records the results of measurements but keeps them secret. Subsequently, the receiver publicly announces the type of measurement (but not the results), and the sender tells the receiver which measurements were of the correct type. These cases are translated into bits (1’s and 0’s) to generate the key. An eavesdropper is bound to introduce errors to this transmission because he/she does not know in advance the type of polarization of each photon, and quantum mechanics does not allow him/her to acquire crisp values of two non-commuting observables (here rectilinear and diagonal polarizations). The two legitimate users of the quantum channel test for eavesdropping by revealing a random subset of the key bits and checking (in public) the error rate. Although they cannot prevent eavesdropping, they can never be fooled by an eavesdropper, because any effort, however subtle and sophisticated it may be, to tap the channel will be detected. Whenever they are not happy with the security they can try to set up key distribution again.

In cryptosystems of type (ii), a sequence of correlated particle pairs is generated, with one member of each pair being detected by each party (for example, a pair of so-called Einstein-Podolsky-Rosen photons, whose
polarizations are measured by the parties). An eavesdropper on this communication would have to detect a particle to read the signal, and retransmit so that his presence remains unknown to the communicating parties. However, the act of detection of one particle of a pair destroys its quantum correlation with the other, and the two parties can easily verify whether this has been done, without revealing the results of their own measurements, by communication over an open channel.

Stephen Weisner first introduced the idea of quantum cryptography in the early 1970’s. He proposed the theory of Conjugate Coding, which was eventually published in Sigact News in the year 1983. In 1984, Bennet and Brassard published their idea on quantum cryptography inspired from Weisner’s work. They produced the BB84, [1] which is considered the first quantum cryptographic communication protocol. This protocol has been experimentally implemented for over 50 kilometers using fiber optic cables and 1 kilometer in the free space. After nearly two decades as a laboratory curiosity, quantum key distribution (QKD) techniques are now emerging as useful building blocks in highly secure networks.

The rest of the paper is organized as follows: Section II provides some important research works on quantum networking, Section III briefly introduces some important fundamental concepts of quantum computing, Section IV describes BB84 QKD protocol in details, Section V illustrates some cases of current network infrastructure where QKD can be integrated to provide higher level security, Section VI highlights two important quantum network security issue-Byzantine Agreement Problem and Fingerprinting, and Section VII concludes the paper.

II. CURRENT RESEARCH IN QUANTUM NETWORKING

On the 3rd November 2003, MagiQ Technologies Inc., a quantum information processing company based in New York, launched the world’s first commercially available quantum key distribution system, called Navajo Secure Gateway. It supports secure key exchanges at distances up to 120 km- a major technical accomplishment that makes very long secure spans possible via cascading devices [2]. This elaborated scheme does not use quantum effects to transmit secret data. Instead, it distributes secret keys based on quantum theory up to a rate of 1,000 keys per second. It has been proved that the chances of decrypting the data by an eavesdropper without the key is reduced to zero in such a situation [4]. A team from Boston, Harvard and BBN Technology sponsored by DARPA has undertaken a five year research program that consists of building and testing a highly secure quantum network [3]. This ambitious project is supposed to perform extensive testing against sophisticated eavesdropping attacks. In MIT, Boston, an initiative has been taken to develop the design for a quantum network under the sponsorship of Army Research Office (MURI). This design will allow robust transmission of quantum information even in presence of high levels of errors and loss of information. Three leading e-security organizations in Geneva have joined forces to deploy what will be the first ever Integrated Quantum Key Infrastructure (IQKI). This initiative has come after they joined hands with a trade organization in order to create the infrastructure necessary for worldwide distribution of unbreakable quantum keys at the ITU Telecom World Conference (ITWC) in Geneva in October 2003 [5].

III. SOME FUNDAMENTAL CONCEPTS

A. Heisenberg’s Uncertainty Principle

The security in QKD is based on the laws of physics and not on any assumption about the intractability of certain mathematical problems, even when the eavesdroppers have access to unlimited computing power. Heisenberg’s uncertainty principle states that we cannot measure a system without perturbing it. For cryptographic purposes, Heisenberg’s principle could lead us to the following logic:

No perturbation → No measurement → No eavesdropping → No leak of information

Stated in other words, quantum cryptography ensures that communications cannot be eavesdropped without introducing errors that can be readily detected by the receiver.

B. Entanglement

Another feature in quantum mechanics that is utilized in quantum cryptography is the entanglement between two quantum systems. The concept of entanglement states that if two or more quantum systems have interacted in the past then they may share information in a form that influences all of them regardless of their spatial separation. A special case of entanglement principle is the EPR (Einstein, Poldolsky and Rosen) paradox. It says that as long as two photons remain unobserved, their properties remain indefinite and are superposition of all of their possible states. But because of their common origin, the properties of the photons are entangled.

C. Photons Polarization:

From the point of view of implementation, the quantum bits (qubits) exchanged between the two parties (say Alice and Bob) are encoded in the form of photons through a beam of light. At the best, each photon represents a single qubit. Suppose the photon’s polarization chosen for encoding the bits of information is as follows: vertical polarization for ‘1’ and horizontal polarization ↔ for ‘0’. Thus, the sequence of pulses ↓↑↓↑ corresponds to ’10110’. In measuring
polarization of photons, we refer to a pair of orthogonal polarization as a basis. In addition, one could choose the diagonal polarization as a second basis, such that 10110 represents the string “10110”. A pair of basis is said to be conjugate if the measurement of the polarization in the first basis randomizes the measurement in the second basis. For example, if we measure a horizontally or vertically polarized photon in the diagonal basis, we cannot determine any information about the initial polarization of the photon. Alternatively, the circular polarization could be used as a second basis. The quantum communication channel for photons can be either free space or optical fiber—the standard media used in telecommunications. Thus the communication channel is not really quantum whereas the information carriers are quantum.

IV. BB84 QKD PROTOCOL

A. Two Different Protocols

Currently two different types of quantum key distribution are proposed based on two counter-intuitive features of quantum mechanics: uncertainty and entanglement. The first type uses the polarization of photons to encode the bits of information and relies on the quantum randomness to prevent an intruder (say Oscar) from obtaining the secret key. The second type uses entangled photon states to encode the bits and relies on the fact that the information defining the key only “comes into being” after measurements are performed by Alice and Bob—the two communicating parties.

BB84 QKD protocol is actually the one that is quite extensively studied both theoretically and experimentally. We will now investigate the BB84 protocol in detail.

B. Quantum Transmission

In the first step of BB84 protocol, Alice sends individual qubits to Bob in states chosen at random from the four states: ↔, ↑, ↓, /, \ which are identified as the polarization states ‘horizontal’, ‘vertical’, ‘45°’, and ‘135°’ respectively. The individual qubits could be sent all at once or one after the other, the only restriction being that Alice and Bob should be able to establish a one-to-one correspondence between the transmitted and the received spins.

Next, Bob measures the incoming qubits in one of the two bases, chosen at random (using a random-number generator independent from that of Alice). Consequently, from the probability theory, Bob will use a correct polarizer half of the time and an incorrect polarizer the other half of the time. However, he will still get the correct result even in 50% of the second half. Thus Bob will come up with correct result in 0.5 * 1 + 0.5 * 0.5 = 75% of the total time. Under perfect situation, uncertainty principle tells us neither Bob nor Oscar, on average, can obtain a measurement better than 75%. At this point, Bob and Alice will have perfectly correlated results whenever they use the same basis but uncorrelated results otherwise.

<table>
<thead>
<tr>
<th>Table 1: Results showing Bob’s prediction about Alice’s string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice’s random string: 1 0 1 0 0 1 1 0 1 0 0 1 0 1 0</td>
</tr>
<tr>
<td>Alice’s random basis: + X + X + X + X + X</td>
</tr>
<tr>
<td>Alice sends to Bob: ↑ / \ / / / / / / / / / /</td>
</tr>
<tr>
<td>Bob measures with: + X + X + + X + X + + X</td>
</tr>
<tr>
<td>Bob’s results: ↑ / \ / / / / / / / / / /</td>
</tr>
</tbody>
</table>

C. Basis Reconciliation:

We can think of a straightforward error correction scheme: Alice announces the bases to Bob and Bob announces the positions he measured in the right bases. If the state is compatible, they keep the bit; if not, they discard it. The key shared at this point is called the sifted key or raw key (it is not really shared since Alice’s and Bob’s versions are different due to noise and eavesdropping on the channel). In this way about 50% of the bit string is discarded.

| Valid data: | | | | | | | |
| Translated to key: | 1 0 | 0 | 1 | 1 | 1 | 0 |

At this stage of the protocol, Alice and Bob use a public channel for basis reconciliation. This is very common in crypto-protocols. This channel does not have to be confidential, but authentication must be guaranteed. Our analysis suggests that neither Alice nor Bob can decide which key results from the protocol. Although neither party sent a secret key to the other, a secret key was established between them. Indeed, it is the conjunction of both of their random number generators that produced the key.
D Possible Attack Model:

Tentative Attack: Essentially, to overcome the problem of eavesdropping, one might try to build protocols that, given Alice and Bob can only measure the Quantum Bit Error Rate (QBER), either provides them with a verifiably secure key or stops the protocol execution and informs the users that the key distribution has failed. Consider a scenario where the intruder Oscar intercepts a qubit passing through the communication channel from Alice to Bob. Bob will be able to detect this interception since he will not receive the expected qubits. Bob can then inform Alice about this on a public channel so that she can discard the communication already intercepted by Oscar. Thus, Oscar’s effect will only be to reduce the bit rate, possibly to zero, but this does not give him any useful information. Therefore, for real eavesdropping Oscar must send a qubit to Bob. Ideally he would like to send this qubit in its original state, keeping a copy for himself.

Failed Attack: It can be proved that a general copy machine that copies any unknown state cannot be realized in practice. Therefore, Oscar cannot keep a perfect quantum copy. In classical information, copying is a fundamental process that is frequently used to an extent that the fan-out gate is usually omitted from, and is assumed to be a natural part of a classical circuit. This is in sharp contrast with quantum information, where the fact that quantum states cannot be copied is a fundamental attribute. This major difference is one of the reasons that make quantum information attractive, since it prevents Oscar from perfect eavesdropping and hence makes quantum cryptography potentially secure.

A More Realistic Approach: So far, all we have shown is that Alice and Bob can arrive at a shared key without publicly announcing any of the bits. But in real life, there are always some errors due to noise in the channel and the equipment, and from Oscar who is trying to gain information by eavesdropping. We will briefly discuss some encountered technical problems. First, Alice and Bob’s bits will differ due to real photon detectors. Second, actual photon emitters generate an average number, $n$, of photons per pulse of light. They cannot reliably generate single photon. In addition, they cannot maintain the same average number, $n$, each time, which makes it difficult for Alice and Bob to agree on a one-to-one correspondence between the exchanged qubits. Oscar will increase the quantum bit error rate (QBER) by intercepting the photons as they are transmitted from Alice to Bob. Since communication errors and eavesdropping cannot be distinguished, Alice and Bob will have to assume that all discrepancies are due to Oscar in order to be on the safe side. Therefore, Alice and Bob must apply some classical information processing protocols, like error correction and privacy amplification to their data. The first protocol is necessary to obtain identical keys and the second to obtain a secret key.

Intercept-resend strategy: This simple but practical attack consists of Oscar intercepting, measuring, and sending qubits to Bob. Since Oscar, like Bob, has no idea about the basis Alice uses to transmit each photon, he must choose bases at random for his measurements. He then resends to Bob another qubit in the state corresponding to his measurement. If he happens to be lucky and chooses the correct basis, Alice and Bob will not notice his intervention. But he may choose wrong basis as well. Oscar will send back to Bob each polarization for the photon in his measurement with equal probability, because he has no information about Alice’s random-number generator. The correct rate in each case when Oscar is present is tabulated in Table 2.

The correct rate, on average, is $0.5 + 0.25 = 0.75$, such that the error rate on average is $1 - 0.75 = 0.25$. In this case, Oscar gets 50% information whereas he leaves a 25% error rate in the sifted key. Alice and Bob can thus easily detect the presence of Oscar. We assume that Oscar performs two actions: opaque eavesdropping with probability of $\lambda$, and no eavesdropping with probability $1 - \lambda$. Thus Bob’s row key will not agree with Alice’s row key with probability of $0.25 * \lambda = 0.25 \lambda$. If however, Oscar applies this strategy to only a fraction of the communication say $\lambda = 10\%$, then the error rate will be only $2.5\%$, while Oscar’s information will be $5\%$.

<table>
<thead>
<tr>
<th>Oscar Right Polarizer</th>
<th>0.5 * 1 = 0.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oscar Wrong Polarizer</td>
<td>0.5 * 0.5 = .25</td>
</tr>
</tbody>
</table>

Reconciliation (extension of BB84): At this stage, the possible errors in the key are caused by technical imperfection and the possible interception by Oscar. Reconciliation is the first classical information processing protocol performed on the sifted key to obtain identical keys between Alice and Bob. Since Oscar presumably listens to all public transmissions, Alice and Bob must reveal as little information as possible while ensuring that they end up with identical keys. Error reconciliation, like the base reconciliation, is performed over a public channel. The following reconciliation algorithm may be followed may be followed [6].

1. The sender, Alice and the receiver Bob, agree on a random permutation of bit positions in their strings (to randomize the location of errors).
2. The strings are partitioned into blocks of size $k$ ($k$ is so chosen that the probability of multiple errors per block is very small).
3. For each block, Alice and Bob compute and publicly announce parities. The last bit of each block is then discarded.
4. For each block for which their calculated parities are different, Alice and Bob use a binary search with $\log(k)$ iterations to locate and correct the error in the block.
5. To account for multiple errors that might remain undetected, steps 1-4 are repeated with increasing block sizes in an attempt to eliminate these errors.
6. To determine whether additional errors still remain, Alice and Bob repeat a randomized check in the following manner. Alice and Bob agree publicly on a randomized assortment of half the bit positions in their bit strings. Then they publicly compare parities (and discard a bit). If the strings differ, the parities will disagree with probability $\frac{1}{2}$. If there is a disagreement, Alice and Bob use a binary search to find and eliminate it, as above.
7. If there is no disagreement after $l$ iterations, Alice and Bob conclude their strings agree with a very low probability of error ($2^{-l}$).

**Privacy Amplification (extension of BB84):** At this point, Alice and Bob possess identical strings, but those strings are not completely private. Oscar may have gained some information about them through intercept/resend. During the reconciliation phase, Oscar did not gain any information, since the last bit of each parity-check block was discarded. However, some of his original information about specific bits might have been converted to information about parity bits.

Privacy amplification, which was developed by Ueli Maurer and other classical cryptographers, while quantum cryptography was being developed, turned quantum cryptography into a practical technology for secure communications. It is a sort of cryptographic version of error correction, which allows Alice and Bob to start with similar shared random keys about which Oscar has some information and make shorter shared random keys which are identical and about which Oscar has (essentially) no information.

Alice announces to Bob the description of a randomly selected hashing function $f$ from $N-K$ bits to $N-K-L-R-S$ secret bits. Both of them apply $f$ on the reconciled key in order to get the final secret-key $X_f$ in $\{0, 1\}^{N-K-L-R-S}$.

**B92 protocol:** Since the security of quantum cryptography relies on the inability of Oscar to distinguish unambiguously and without perturbation between the different states that Alice sends to Bob, Bennett noticed that only two non-orthogonal states are needed. The four different states used in the BB84 are more than really necessary for quantum cryptography. Although two non-orthogonal states are enough, it is not very secure in practice, since one can unambiguously distinguish between them at the cost of some losses[17]. In 1992, Bennett came up with B92 quantum key distribution protocol that is a modified version of BB84 protocol.

Thus we observe that the quantum key distribution protocols allow two communicating parties Alice and Bob to generate and share random secret keys that exhibit very small error rate. They also enable two communicating parties, Alice and Bob to estimate the level of eavesdropping, so that they can try to reduce the error introduced by an intruder Oscar, and increase (amplify) the privacy of their shared random keys.

V. INTEGRATING QKD IN CURRENT INFRASTRUCTURE

Currently, quantum network security does not appear as an independent application that provides a complete set of protocols for secure communication. However, quantum key distribution techniques go along with the well-established Internet technology. These techniques are employed in the public Internet, or more likely, with private networks that employ the Internet protocol suite, in order to build secure communication systems. Such private networks are currently in widespread use around the world with customers who desire secure and private communications, e.g. financial institutions, governmental organizations, militaries and so forth, and that an integration of QKD technologies to these types of private networks may prove both feasible and immediately appealing in certain context. We consider one such system architecture as proposed by a team from BBN Technologies and MIT under the sponsorship of DARPA [7].

A. Security Architecture

The secure communication between gateways and even workstations on any network is achieved by the well-defined architecture of IPSec. It specifies the protocols, algorithms, databases and policies required for secure communication. Therefore, it would be optimal if we can integrate QKD technology with the current Internet security architecture. This will guarantee secure Internet traffic using quantum cryptographic techniques.
Figure 1: System architecture for a point-to-point QKD link

Figure 1 illustrates the basic setup with some details. The salient features of the systems are as follows:

1. Two QKD endpoints establish communications via a dedicated fiber or wavelength for the quantum path, and via the Internet for messaging.
2. The sender prepares and transmits raw keys, from which both sides come to agreement on a shared, secret key.
3. The secret key is then employed in the cryptographic gateway for protecting message traffic that will travel through the Internet within secure IPsec tunnels.

Figure 2 provides a multi-layer approach for the QKD protocol. These layers outline the modular approach for design of QKD protocols.

B System Architecture

We now briefly describe the system architecture of a quantum network as it evolves through three major stages, from a single, stand-alone QKD link supporting highly secure Internet communication, through both trusted and untrusted QKD networks.

B.I System Architecture of a Point-to-Point QKD Link

Figure 3 presents a simplified block diagram of a point-to-point QKD link, as it would most likely be deployed for secure networking, e.g., one that securely links a branch office to a corporate headquarters. Each enclave is typically a collection of one or more local ethernets that connect to the public Internet via specified devices such as VPN gateway. Thus, one needs to administer only a single device in order to establish or monitor external security for a given private enclave. These gateways are responsible for setting up security associations (and thus encrypted tunnels) with authorized distant gateway(s), for encrypting all local traffic before it is injected into the public network and for decrypting and authenticating traffic received from the public network before sending it onwards, in the clear, within the destination enclave. Given the nature of QKD, one would need two distinct communication paths: one for the transmission of the cryptographic keys, and the other for the encrypted message traffic.
This architecture suffers from serious drawbacks mainly due to the current technology. Fiber attenuation and error infiltrations limit the size of terrestrial links to 50 km or less. The point-to-point architecture is constrained by the distance over which a single link may be operated. Moreover, isolated point-to-point links are subject to simple denial-of-service attacks such as active eavesdropping or even physically cutting the fiber. Finally, in practice it may be prohibitively expensive to establish pair-wise, dedicated, point-to-point links between all private enclaves for communication purpose.

### B.II System Architecture of a Trusted Network

The drawback of the architecture in Section V.B.I can be overcome by linking the QKD endpoints via a mesh of QKD relays or routers forming a QKD network. Such QKD networks can be built in several ways. In one approach, the QKD relays may transmit only the keying material but not the message traffic. Thus, after the various relays have established pair-wise agreed-upon keys along an end-to-end point, e.g. between the two QKD endpoints, they may employ these key pairs to securely transmit a key 'hop-by-hop' from one endpoint to the other, being one-time pad encrypted and decrypted with each pair-wise key as it proceeds from one relay to the next. In this approach, the end-to-end key will appear in the clear within the relays’ memory, but will always be encrypted when passing through a link. Such a design may be termed a ‘key transport network’.

In another approach, the QKD relays may transport both keying material and message traffic. Figure 4 illustrates this approach, in which the relays are acting as Internet routers with pair-wise QKD mechanisms providing link encryption between the routers. In essence, each IP datagram of message traffic is encrypted once as it travels from the QKD endpoint to its first relay. Then it is decrypted, held in the clear in the relay’s memory, and then encrypted again with a second set of keys and sent onwards to the next relay. This operation continues hop by hop, until the datagram is finally received at the destination endpoint and sent onwards to the attached private enclave. This network differs from the standard structure of the Internet by interposing a set of encrypted tunnels (‘virtual links’) between cooperating routers.

The major weakness of trusted network architecture is that the relays must be trusted. As the keying material and message traffic are available in the clear in the relays’ memories the relays become points of vulnerabilities.

### B.III System Architecture of an Untrusted Network

As in classical cryptography, an end-to-end approach is likely to provide the most satisfactory architecture for disentangling the user’s keying material for secure traffic flows from the network that transports such flows. We present an approach that introduces unamplified photonic switches into the QKD network architecture in order to provide end-to-end key distribution via a novel mesh of untrusted switches.
The main strength of untrusted QKD networks is that they provide truly end-to-end key distribution; QKD endpoints need not share any secrets with the key distribution network or its operators. This feature may be extremely important for highly secure networks. Their weaknesses are, however, very significant. Unlike trusted relays, the untrusted switches cannot extend the geographic reach of a QKD network. In fact, they may significantly reduce the network’s reach since each switch adds at least several dB losses to the photonic path. In addition, it will be difficult in practice to employ a variety of transmission media within an untrusted network, since a single frequency may not work well along a composite path that includes both fiber and free space links. Untrusted networks may also introduce new vulnerabilities to traffic analysis.

The principal weakness in untrusted QKD networks (i.e. limited geographic reach) may potentially be countered by quantum repeaters. There is currently a great deal of active research on construction of such repeaters, and if positive results are achieved, these repeaters should slide neatly into the architecture of untrusted QKD networks to enable seamless QKD operations over much greater distances than what are currently feasible.

QKD techniques can be integrated to standard Internet technology in order to provide highly secure communications for practical use. The architectures that we have discussed in this section show how to integrate QKD links with current Internet technology. Such QKD networks should be able to defend against eavesdropping, noise and denial-of-service attacks on the links.

VI. QUANTUM NETWORK SECURITY

In classical information, we usually restrict ourselves to binary representation of data, since use of larger bases does not fundamentally offer any additional tasks. Can we assume the same for quantum information? That is, can we make full use of the physical resources offered by quantum by limiting our information carriers to qubits? It seems the answer is negative. It will be clear in this section.

A Byzantine Agreement Problem

Matthias Fitzi, Nicolas Gisin, and Ueli Maurer from Switzerland proposed a quantum solution for a slightly modified version of the Byzantine Agreement Problem using qutrits (i.e. superposition of |0>, |1>, and |2>). However, no classical qubit-based solution of this problem has been found till date. We briefly state the problem of Byzantine Agreement before discussing the solution proposed by Fitzi, Gisin and Maurer [8].

The Byzantine army is divided into n divisions, each division commanded by a general. Among the generals maximum of m might be traitors, where m < n/2. The divisions are camped around a city and the generals can only communicate in a one-to-one fashion using messengers. One of the generals, the commanding general, makes a detailed plan of an attack and wants to inform the others of it. Naturally, the traitor generals will try to prevent the loyal generals from reaching an agreement on the plan of action. It may be noted that the commanding general himself might be one of the traitors.

We will now consider a modified version of the classical problem, where the task is to find a protocol that achieves detectable broadcast so that at the end of protocol execution, the generals agree on a commander’s plan if everybody is loyal, otherwise either all loyal players agree on one plan of action or they abort the protocol.

The problem relates to coordinating several computers in a network where some computers might fail. However, detectable broadcast cannot be attained using classical channels. It is not yet proved whether it is possible to construct a protocol to solve this problem using qubits. For simplicity, let us assume n = 3, and denote by S, R_0, and R_1, the commanding general and the other two generals respectively. We assume that the three players (generals) share many qutrits triplet’s j each in the Aharonov state that are entangled in such a way that whenever the three qutrits are all measured in the same basis, all three results will differ. The following protocol was presented by Fitzi, Gisin, and Maurer:

1. First, the sender S sends (broadcasts) the bit x to the two receivers R_0 and R_1 using the classical channels. Let the bits received by R_0 and R_1 are x_0 and x_1 respectively. Next, the sender S measures all his qutrits in the z-basis. Whenever he gets
the result \(x\), \(S\) sends the index \(j\) to both the receivers. Accordingly, the player \(R_0\) and \(R_1\) each receives a set of indices \(J_0\) and \(J_1\) respectively.

2. Both the receivers test the consistency of their data. For this purpose, they measure their qutrits in the \(z\)-basis. If all results with indices in \(J_0\) differ from \(x_0\), then the player \(R_0\) has consistent data and he sets a flag \(y_0 = x_0\). If a set of data is inconsistent, then the player sets his flag to \(y_0 = ?\) (interpreted as inconsistent).

3. The two receivers send their flags to each other. If both flags agree, then the protocol terminates with all honest players (loyal generals) agreeing on \(x\).

4. If \(y_0 = ?\), player \(R_0\) knows that the sender is dishonest. He concludes that the other receiver is honest and he simply accepts the bit he receives from him (if \(y_0 = y_1 = ?\), then they both end with the “value” ?).

5. Now the only interesting case that remains to be analyzed is where both the receivers claim that they received consistent, but different data. The strategy we propose in this case is that the player \(R_1\) will not change his bit \(y_1\), unless the player \(R_0\) convinces him that he did indeed receive the bit \(y_0\) from the sender in a consistent way. To convince \(R_1\) of his honesty, \(R_0\) sends him all the indices \(k\) belonging to \(J_0\) for which he has the results \(I - y_0\).

6. The receiver \(R_1\) now checks whether he gets “enough” indices \(k\) from \(R_0\) such that:
   
   (a) “Almost all” indices \(k\) from \(R_0\) are not in \(R_1\)’s index set \(J_1\), and also
   
   (b) These \(k\) indices correspond to qutrits for which \(R_1\)’s results are “almost all” equal 2. If \(R_0\) indeed got an index set that is consistent with bit \(y_0\) then \(S\) holds \(y_0\), \(R_0\) holds \(I - y_0\), and hence, \(R_0\)’s result must be a 2. If the test succeeds, player \(R_1\) changes his bit to \(y_1\), otherwise he keeps \(y_1\).

To see how the protocol works, consider the 6 possible cases \(\{0 1 2, 0 2 1, 1 2 0, 1 0 2, 2 0 1, 2 1 0\}\) that can occur when the three players measure their qutrits. If \(R_0\) receives the bit 0, then the qutrits are either 0 1 2 or 0 2 1. \(R_0\) can prove that by announcing all the cases he obtained a value 1, for such cases \(R_1\) will have a value 2. If \(R_0\) pretends to have a value \(1\) then he will be required to prove it by giving the indices that correspond to \(2\). However, \(R_0\) cannot differentiate between cases 1 0 2 and 2 0 1. Thus approximately only half of the indices that \(R_0\) sends to \(R_1\) will give a value of \(1\), and \(R_1\) will be able to realize that \(R_0\) is trying to cheat him.

B. Fingerprinting

Let us now move to a different problem in the area network security: fingerprinting, a mechanism that arises in the study of communication complexity, is the problem of determining if two strings are equal as little communication and storage of information as possible.

The model of communication complexity considered is called the simultaneous message passing model, which was introduced by Yao [9]. In this model, Alice and Bob, the two communicating parties, are not allowed to directly communicate with one another. Instead, they each send a message to a third party, called the referee, who determines the output of the protocol based on the messages sent by Alice and Bob. The collective goal of the three parties is to cause the protocol to check if \(x = y\), while minimizing the amount of communication required from Alice and Bob to the referee.

Newman and Szegedy [10] proved that fingerprints of size \(O(n^{1/2})\) bits are required to ensure a small probability of error, if Alice and Bob do not have a prior shared secret key. Following quantum theory, Buhrman, Cleve, Watrous, and Wolf [11] have shown how to solve this problem using \(O(\log n)\)-qubits and proved that their method is nearly optimal. The reason behind the exponential saving provided by quantum systems is that quantum systems contain large sets of nearly orthogonal states. It is known that there are sets of \(2^r\) states that are nearly orthogonal pair wise in \(O(\log n)\) qubit systems.

It is easy to see that \(O(\log n)\) is nearly optimal for quantum, given that any \(k\)-qubit quantum state can be specified with exponential precision using \(O(k2^k)\) bits and since \(O(n^{1/2})\) is the lower bound on size of the fingerprint for classical bits.

VII. CONCLUSION

Quantum cryptography is an effort to allow two users of a communication channel to create a body of shared and secret information. This information, which generally takes the form of a random string of bits, can be used as a conventional secret key for secure communication. The advantage of quantum cryptography over traditional key exchange methods is that the exchange of information can be shown to be secure in a very strong sense, without making any assumptions about the intractability of certain mathematical problems. Even when assuming hypothetical eavesdropper with unlimited computing power, the laws of quantum mechanics guarantee (probabilistically) that the secret key exchange will be secure, given a few other assumptions. In this paper, we have briefly introduced some fundamental concepts of quantum computing and their applications in the field of cryptography and network security. We have discussed the concept of quantum key distribution in some detail and also illustrated some current network infrastructures where it can be gainfully employed for security purpose. We have also described the application of quantum computing in network security with Byzantine Agreement Problem’s solution and fingerprinting using quantum computing protocol.
REFERENCES


