CHAPTER 1

INTRODUCTION

Nothing exists except atoms and empty space; everything else is opinion.
—Democritus of Abdera (ca. 400 BC)

Quantum computing has demonstrated its usefulness in the last decade with many new scientific discoveries. The quantum algorithms were under intensive research during the last quarter of the twentieth century. However, after Shor published the prime factorization method in 1994, and Grover introduced the quantum search method in 1996, results in the field of quantum algorithms tapered off somewhat. In the middle of the ’90s, there was silence in the field of quantum algorithms and this did not change until the beginning of the present century. This silence has been broken by the solution of some old number theoretic problems, which makes it possible to break certain—and not just those that are based on RSA—very strong cryptosystems. Notably, these hard mathematical problems can now be solved by polynomial-time quantum algorithms. Later, these results were extended to other number theoretic problems, and the revival of quantum computing has been more intensive than ever.

These very straightforward quantum algorithms can be used only if there is a stable framework of physical implementations standing behind them. Many new techniques have been developed in the last decade to implement a quantum computer in practice, using linear optics, adiabatic systems, and entangled physical particles. By the end of the twentieth century, many new practical developments had been realized, and many novel results introduced in the field of quantum computation and *quantum information processing*.

Another important research field related to the properties of the physical implementations of quantum information focused on the decoherence and the precision of the measurement outcomes. Many researchers started to analyze the question of whether entanglement could help to increase the precision of quantum computation and the probabilities of the right measurement outcomes.

The main task of quantum complexity theory is to clarify the limitations of quantum computation and to analyze the relationship between classical and quantum problem classes. As the quantum computer becomes a reality, the classical problem

Advanced Quantum Communications: An Engineering Approach, First Edition.
Sandor Imre and Laszlo Gyongyosi.

classes have to be regrouped and new subclasses have to be defined. The most important question is the description of the effects of quantum computational power on NP-Complete problems. According to our current knowledge, quantum computers cannot solve NP-Complete problems; hence if a problem is NP-Complete in terms of classical complexity theory, then it will remain NP-Complete in quantum complexity theory, too. On the other hand, there are still many open questions, such as the complexity of quantum computations or the error-bounds of the various quantum algorithms, and it is expected that new results will be born in the near future.

1.1 EMERGING QUANTUM INFLUENCES

Efficient quantum algorithms that have been developed for breaking classical cryptographic systems could become a reality in the next decade. According to Moore's law, the physical limitations of classical semiconductor-based technologies could be reached by 2020, and we and you, dear reader, will step into the Quantum Age.

Public key classical cryptography relies heavily on the complexity of factoring integers (or similar problems such as discrete logarithms). Quantum computers can use the Shor algorithm to efficiently break today's public key cryptosystems. We will need a new kind of cryptography in the future. Because classical cryptographic methods in wired and wireless systems are vulnerable, new methods based on quantum mechanical principles have been developed.

To break classical cryptosystems, several new different quantum algorithms (besides Shor's algorithm) can be developed and used. After quantum computers are built, today's encrypted information will no longer stay secure, because although the computational complexity of these classical schemes makes it hard for classical computers to solve them, they are not hard for quantum computers! Using classical computers, the efficiency of code breaking is restricted to polynomial time; however, with a quantum computer these tasks can be completed exponentially faster.

1.2 QUANTUM INFORMATION THEORY

The theoretical background of communication over quantum channels is based on the fundamental results of *quantum information theory*. The actual state of quantum information theory reflects our current knowledge of the quantum world, and it also determines the success of quantum communication protocols and techniques.

The phenomena of the quantum world cannot be described by the fundamental results of classical information theory. Quantum information theory is the natural extension of the results of classical information theory. But it brings something new into the global picture and helps to complete the missing, classically indescribable, and even unimaginable parts. Quantum information theory lays down the theoretical background of quantum information processing and synthesizes it with other aspects of quantum mechanics, such as experimental quantum communications, secure and private quantum channels, or quantum error correction

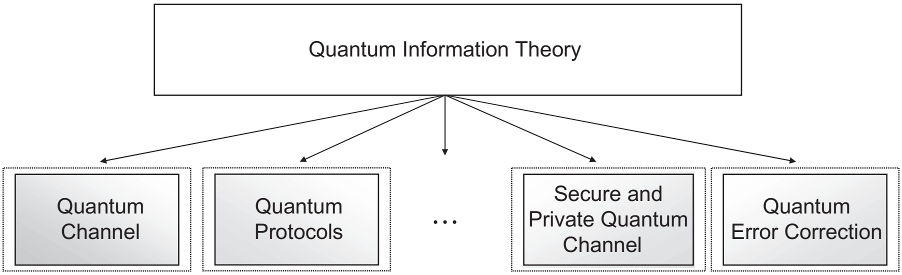
Quantum Information Theory
Quantum Channel
Quantum Protocols
...
Secure and Private Quantum Channel
Quantum Error Correction

Figure 1.1. Quantum information theory provides the theoretical background for various subjects in quantum information processing.

techniques. This field is the cornerstone of quantum communications and quantum information processing.

The primary employment of quantum information theory is to describe quantum channel capacities, to measure entanglement, and to analyze the information-theoretic security of quantum cryptographic primitives. In Figure 1.1, we highlighted some important parts of quantum information theory.

With the help of quantum information theory, information transmission through the quantum channel can be discussed for both classical and quantum information. The former can be defined by a formula very similar to the classical Shannon channel coding theorem. On the other hand, the latter challenge has opened new dimensions in information transmission. As we will see, there are still many open questions in quantum information theory. The various channel capacities of quantum channels have been proven to be nonadditive in general; however, there are many special cases for which strict additivity holds. These fundamental questions will be discussed in detail in this book.

As follows from the connection defined between classical and quantum information theory, every classical and quantum protocol can be described by using the elements of quantum information theory. The definitions and main results of quantum information theory, such as the density matrix, entanglement, measurement operators, quantum Shannon theory, von Neumann entropy, quantum relative entropy, Holevo bound, fidelity, and quantum informational distance, are discussed in Chapter 2.

1.3 DIFFERENT CAPACITIES OF QUANTUM CHANNELS

The concept of a quantum channel models communication at an abstract level, thus it does not require the deep analysis of the various physical systems. Instead it will be sufficient to distill their essence from the information transmission point of view.

The *capacity* of a quantum channel gives us the rate at which classical or quantum information increases with each use of the quantum channel. We can define the *single-use* and the *asymptotic capacity* of the quantum channel: the first quantifies the information that can be sent through a single use of the channel, the latter quantifies the information that can be transmitted if arbitrarily many uses of the quantum channel are allowed.

Many capacities can be defined for a quantum channel: it has a *classical capacity*, a *quantum capacity*, a *private capacity*, an *entanglement assisted capacity*, and a *zero-error capacity* (classical and quantum). Some of these have also been defined in classical information theory, but many of these are completely new.

The classical capacity of a quantum channel was first investigated by Holevo, who showed that from a two-level quantum state, or qubit, at most one bit of classical information can be extracted. This theory is not contradictory to the fact that the description of a quantum state requires an infinite number of classical bits. As we will see, this "one classical bit bound" holds just for two-level quantum states (the qubits) since, in the case of a *d*-level quantum state (called qudits) this bound can be exceeded.

The classical capacity of a quantum channel can be measured in different settings, depending on whether the input contains tensor product or entangled quantum states, and the output is measured by *single* or by *joint measurement settings*. These input and output combinations allow us to construct different channel settings, and the capacities in each case will be different. This is a completely new phenomenon in comparison to classical communication systems, where this kind of differentiation is not possible. The *additivity* of a quantum channel depends on the encoding scheme and on the measurement apparatus that is used for measuring the quantum states. If we use product input states, there is no entanglement among them, and if we do not apply joint measurement on the output, then the classical capacity of a quantum channel will be additive, which means that the capacity can be achieved by a single use. If we use joint measurement on the outputs, then such additivity is not guaranteed, which also suggests that in general the classical capacity is not additive. We note that many questions are still not solved in this field, as we will see later in Chapter 3 where the properties of classical capacity of quantum channels are discussed in detail.

The *classical capacity* of a quantum channel was formulated by Holevo, Schumacher, and Westmoreland [Holevo98], [Schumacher97], and it is known in quantum information theory as the *HSW* channel capacity. While the classical capacity measures classical information transmission over a noisy quantum channel, the *quantum capacity* of a quantum channel describes the amount of quantum information that can be transmitted through a noisy quantum channel. The formula of quantum capacity was introduced by Lloyd, Shor, and Devetak in [Lloyd97], [Shor02], [Devetak03], and after the inventors it is called the *LSD* channel capacity. Both the HSW and the LSD channel capacities provide lower bounds on the ultimate limit for a noisy quantum channel to transmit classical or quantum information. One of the most important applications of quantum capacity is the transmission of entanglement. The quantum error-correction techniques are developed for the optimization of quantum capacity in a noisy environment.

As in the case of classical channel capacity where we will use the *Holevo information* as measure, for quantum capacity we will introduce a completely different correlation measure, the concept of *quantum coherent information*. We note that the generalized quantum channel capacity cannot be measured by the *single-use* version of quantum coherent information (or at least, it works just for some special channels), hence we have to compute the *asymptotic* form. This fact also implies that the additivity of the quantum capacities will be violated, too. These questions and the still unsolved questions are described in Chapter 4, and we give a very nice implementation for their use in quantum communications.

Chapters 3 and 4 can be regarded as a "practical" application of the results described in the Chapter 2. While Chapter 2 provides a strong information theoretic background, Chapters 3 and 4 bring these results to reality, and converts them to a tangible format.

Exploiting the combination of the elements of quantum information theory and computational geometry, many still open questions regarding quantum channel capacities can be answered in a rather different way by comparison of the well-known methods. A plausible geometrical picture can be assigned to each channel model, and instead of numerical calculations on their capacities, one can utilize the much more straightforward geometric representation. This interesting and rather surprising field is introduced in Chapter 5.

1.4 CHALLENGES RELATED TO QUANTUM CHANNEL CAPACITIES

One very interesting and important problem regarding the capacity of quantum channels is whether entanglement between states can improve sending classical information through quantum channels. This problem is known as the *additivity problem.*

The question of additivity has emerged from an attempt to find an unambiguous formula for the capacity of a noisy quantum channel. The accessible classical information from continuous quantum degrees of freedom is limited. This limitation stands behind the additivity of quantum channel capacity. Up to this day, strict additivity for quantum channel capacity has been conjectured but not proven, and the additivity property of quantum channels is still an exciting subject of current research.

We are going to discover this field using an elegant geometrical interpretation in Chapter 6 where we also investigate whether entanglement across input states could help to enhance the transmission of information on quantum channels—as entanglement can help in other problems in quantum computation. To walk around this question different channel models will be studied.

The other, rather challenging current problem of quantum information theory is called *superactivation*. It makes it possible to use zero-capacity quantum channels to transmit information! The effect of superactivation was discovered in 2008, and later, in 2009, it was shown that both the classical and quantum zero-error capacities of a quantum channel can be superactivated in certain cases. The complete theoretical background of the superactivation is currently unsolved; however, we know that it is based on the nonadditivity (i.e., on the extreme violation of additivity) of the various quantum channel capacities and the entangled input states. Chapter 7 explains the theoretical background of superactivation of quantum capacity, quantum zero-error capacity, and the zero-error capacity of quantum channels, and we show how the various channel capacities of quantum channels can be superactivated.

1.5 SECRET AND PRIVATE QUANTUM COMMUNICATION

Using current classical computer architectures, the brute-force breaking of today's public key cryptosystems could take an extremely long time, since the problem of factoring large integers in polynomial time is still not solved. On the other hand, if we use *quantum computers* instead of classical computer architectures, the factorization problem can be solved with polynomial complexity. This famous discovery of Shor's was successfully demonstrated experimentally in 2001, and it revealed the fact that classical cryptographic methods will not be able to provide security in the future. However, the one-time pad (OTP) method could achieve perfect theoretical security in classical systems, but according to the challenges of key-distribution, these methods cannot be efficiently applied in practice. The perfect security of the OTP method was proved by Claude Shannon, but the problem of key-distribution in classical systems is not solvable according to the problem of copying information.

The status of the security of classical cryptosystems will change dramatically after the advent of quantum computers. Currently used and well-known cryptosystems, such as the RSA algorithm, Diffie-Hellman method, elliptic curve cryptography, Buchmann-Williams key exchange scheme, or the algebraically homomorphic cryptosystems, will be broken immediately when quantum computers become reality. On the other hand, not every problem can be solved by the exponential increase in speed. Currently, we conjecture that NP-Complete problems do not have efficient quantum algorithmic solution—at least, currently we have not found them—hence finding quantum mechanics-based solutions for exponential speedups of these problems is an important question and task in the future. However, currently all the classical cryptosystems are based on non NP-Complete problems, and the exponential speedup of quantum algorithms, and the theoretical weakness of these schemes, can be exploited quantum mechanically. We note that there have been some attempts to develop classical cryptosystems, which seem immune against quantum attacks, such as hash-, code- or lattice-based cryptography, the multivariate quadratic equation cryptosystems or secret-key cryptography, but these methods are neither efficiently implementable in practice, nor protected by NP-Complete problems. The proofs of the resistance of these classical schemes against quantum computers are based on the loose assumption that there will be no quantum algorithm in the future for an attack on these classical schemes better than Shor's or Grover's algorithm. As we have seen in history, cryptoanalysts could be easily disposed to believe that the best possible attack against the analyzed protocol has been found (see Enigma in WWII) or that it will not be possible in the future to attack the scheme with a better and faster method. This is very misleading and a dangerous belief.

As a general conclusion, all the classical cryptographic systems are resistant to the attacks of classical computers only. At this point, we have to raise the question: Does there exist a cryptographic scheme at all that is proved to guarantee unconditionally secure communication in the Quantum Age? The answer is definitely yes: it is called *quantum cryptography*.

In today's communications networks, the widespread use of optical fiber and passive optical elements allows us to use quantum cryptography. In order to spread quantum cryptography, interfaces must be implemented that are able to manage together both quantum and classical channels. In practical implementations of *quantum key distribution* (QKD) protocols, Alice, the sender, uses *weak coherent pulses* (WCP) instead of a single photon source. As has been shown, WCP-based protocols have a security problem, since an eavesdropper can perform a photon number–splitting attack against the protocol. These kinds of attacks are based on the fact that some weak coherent pulses contain more than one photon in the same polarization state, which provides information to the eavesdropper without any disturbance. One of the main advantages of current practical QKD schemes is that the quantum communications in these methods can be implemented by using conventional optical devices, such as laser diodes, wave plates, beamsplitters, and detectors.

We will show that *quantum cryptographic* primitives can be extended to other types of secret message transmission. Quantum cryptography is just one possible application of the fundamental properties of quantum mechanics for secret information transmission; however, in the last decade many new, but not quantum cryptography–based, cryptographic primitives have been developed.

Some of the most important fields among the new, post-QKD results in secret quantum communications protocols are *quantum authentication*, *quantum fingerprinting*, and *quantum privacy protocols*. The theoretical background of *quantum digital signature* is based on classical public-key methods; however, classical keys cannot be used here. Although there have been many attempts to realize a practical quantum public key method, the complexity of the protocol is still so high that it is impossible to use it efficiently in practice. On the other hand, quantum fingerprinting is a much more achievable protocol. It makes it possible to generate a “hash” of a large data set, similar to classical hashing strategies. The hash of the quantum states can be computed in a relatively easy way, without extensive computational costs.

The development of quantum privacy is one of the most important results of the post-QKD research in quantum information processing. The privacy of the quantum channel can be ensured only if with every quantum state, the sender sends to the receiver two classical bits. The classical bits are derived from classical randomness, which randomness is shared between the parties. In the newer versions of quantum privacy protocols, the classical randomness can be changed to quantum randomness. We note that currently, the complexities of both the classical and the quantum-based privacy protocols are rather high. On the other hand, it has been proven that one classical bit per qubit is sufficient for an absolutely secure privacy communication, which allows using the protocol in various communications scenarios in future quantum networks. Privacy can be extended to remote database access, hence these protocols will have more importance in future quantum communications. In classical networks, private information retrieval is possible only if there is some shared randomness that can be encountered in the system. Recently, it has been shown that the privacy of “quantum servers” of a certain communication network can be ensured without shared information between them, and the privacy of the parties can be preserved if the quantum servers are cheating.

Digital signatures and the authentication of messages are well-known problems in classical communications methods, with many available protocols. These digital signatures and authentication schemes can be translated from classical to quantum systems; however, there are many differences. The *quantum authentication* can be realized in the case of quantum systems, too; however, the method requires both classical and quantum communications. An important result in this field is that the number of key bits required for the authentication is at least two times greater than the number of quantum states to be authenticated. In the case of a *quantum digital signature schemes*, the main task is not the integrity of the message, it is rather the validation of the personality of the sender. In quantum digital signature schemes, the public key consists of quantum states, hence the *no-cloning theorem* makes it impossible to distribute it among many parties. On the other hand, Alice can prepare the same state many times, hence these states can be used as public keys; however, the cost of the unconditional security of quantum public key methods is relatively high in comparison to classical schemes. These quantum protocols are currently still "under research," hence it could have application in advanced quantum communications schemes of the future.

Quantum secret sharing, *quantum data hiding*, and *quantum fingerprinting* are also very new fields in secret quantum communications. The idea behind quantum secret sharing is that the parties of the communication get an incomprehensible secret message, and the secret can be recovered only if the parties start to communicate with each other. The secret quantum message is encoded in a joint quantum state, and the reduced density matrix computed by an individual party gives only zero bit information from the secret. In the quantum data hiding protocol, the parties get classical information; however, the decoding of the message is possible only if the parties have a quantum channel. This type of security scheme can also be applied in the quantum secret sharing protocol. In the quantum secret sharing scheme the parties receive quantum states, and after this reception, the parties have to use classical communication. The properties of private quantum communications and the most relevant quantum protocols will be discussed in Chapter 8. In the first part of the chapter we overview the possible attacks against the quantum key distribution protocols, then we study the quantum bit commitment protocol, quantum fingerprinting, and quantum public key cryptography.

1.6 QUANTUM COMMUNICATIONS NETWORKS

The hardest problem in future quantum communications is the long-distance delivery of quantum information. Since arbitrary unknown quantum states cannot be copied, the amplification of quantum bits is more complex compared with classical communications. The success of future long-distance quantum communications and global quantum key distribution systems strongly depends on the development of efficient quantum repeaters. It is not simply a signal amplifier, in contrast to the classical repeaters.

There are several differences between a classical and a quantum repeater. The quantum repeater nodes create highly entangled EPR states with high fidelity of entanglement. The entangled quantum states can be sent through the quantum channel as single quantum states or as multiple photons. In the first case the fidelity of the shared entanglement could be higher; however, it has lower probability of success in practice, since these quantum states can be lost easily on the noisy quantum channel. In the second case, the loss probability is lower; however, the fidelity will not as high as in the single photon case. In order to recover fidelity of entanglement from noisy quantum states, purification is needed.

Sharing of quantum entanglement plays a critical role in *quantum repeaters*. The fidelity of the entanglement decreases during the transmission through the noisy quantum channel. Therefore, in practical implementations, the quantum entanglement cannot be distributed over very long distances; instead, the EPR states are generated and distributed between smaller segments.

A practical approach of the quantum repeater is called the *hybrid quantum repeater*. It uses atomic-qubit entanglement and optical coherent state communication. In practice, the repeaters are connected by optical fibers, through which the entangled quantum states are sent. Quantum repeaters use the *purification* protocol to increase the fidelity of transmission. The rate of entanglement purification depends on the fidelity of the shared quantum states, since the purification step is a probabilistic process. Moreover, the success probability of the purification of the entangled quantum states depends on the fidelity of the entangled states: if the fidelity of entanglement of the shared state is low, then the success probability of its purification will be also low. Another important disadvantage of the purification algorithm is that it requires much classical information exchange between the quantum nodes.

Quantum computing offers fundamentally new solutions in the field of computer science. The classical biologically inspired self-organizing systems have increasing complexity and these constructions do not seem to be suitable for handling the service demands of the near future. *Quantum probabilistic networks* may be able to replace classical solutions with significantly higher efficiency. Using the quantum probabilistic nature, truly random behavior can be added to the self-organizing processes of biological networks.

The cell-organized, quantum mechanics–based cellular automata models have many advantages over classical models and circuits. For a quantum cellular machine, every cell is a finite-dimensional quantum system with unitary transformations, and there is a difference between the axiomatic structure of classical and quantum versions of cellular automata.

In Chapter 9, we give a brief overview of the possible solutions of future quantum-based networks and long-distance quantum communications. In the first part of the chapter, we describe long-distance quantum communications and the quantum repeater, while at the end of the chapter, we discuss the basic properties of quantum probabilistic networks.

1.7 RECENT DEVELOPMENTS AND FUTURE DIRECTIONS

In the last chapter of our book, we present an overview of the "experimental side" of quantum computation, the recent developments and the physical implementations. Quantum information processing uses the results of quantum mechanics and integrates them with the elements of information processing. Quantum communications may have an important role to play in the future's secret quantum networks, in which truly unbreakable cryptographic schemes will be necessary. As an important future direction, quantum cryptographic schemes can be implemented to realize unconditionally secure communication. But the security of quantum cryptography cannot be the solution for every possible security problem.

In future telecommunications networks, practical quantum communications will be implemented in combination with classical systems, using the elements of classical data processing. These classical parts will be integrated into the less critical parts of the protocols, hence these solutions will not decrease the level of security. The currently implemented practical quantum networks all contain some classical elements, and in the future these schemes cannot be eliminated. In future quantum networks, the information will be protected by the no-cloning theorem.

The physical implementations of quantum communications networks will be based mainly on optical communications. Developments in the physical layer tend toward single photon sources, single photon detecting modules, and a reduction in the noise of the optical quantum channels. The loss due to the optical fibers determines the efficiency of the quantum communications, hence it will be an important task to develop implementable quantum repeaters in future. On the other hand, as opposed to the situation with classical bits, quantum bits cannot be copied, hence quantum memories will have an important role in the expansion of quantum repeaters. As the challenges of the physical layer become resolved, the next step could be the design of the communication between the physical and the higher layers, and the controlling and managing of the processes of the quantum layer by the classical one. All real life–based quantum communications networks are complex systems, with many degrees of freedom. The theoretical quantum protocols are just idealizations of the practical systems, without the imperfections caused by the environment. It is an important task in future developments to quantify experimentally the efficiency and the security that can be achieved in the noisy practical environment.

Another important direction is the development of a scalable quantum computer. Currently, only small scale implementations have been realized in the laboratory. The architecture of quantum computers can be based on various physical implementations, such as magnetic resonance, optical lattices, silicon-based approaches, electrons, and quantum cavities. In contrast to the laboratory environment, the development of scalable implementations is a more challenging problem. To realize quantum computers in practice, or to use the quantum Internet, more efforts will be needed. On the other hand, there is no other way. According to Moore's law, we will step into the Quantum Age, very soon.

The ways and steps we just started could be different, but one thing is certain: quantum information will be the key to the revolution of the future's information processing and telecommunications.