Quantum Communications in New Telecommunications Systems

To our mother, with profound gratitude and affection.

– Malek Benslama, Achour Benslama

Series Editor
Guy Pujolle

Quantum Communications in New Telecommunications Systems

Malek Benslama
Achour Benslama
Skander Aris

ISTE
WILEY

First published 2017 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

© ISTE Ltd 2017
The rights of Malek Benslama, Achour Benslama and Skander Aris to be identified as the authors of this work have been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

Library of Congress Control Number: 9781848219908

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-84821-990-8

Contents

Foreword

Four books devoted solely to satellite communications: this is the challenge set by Professor Malek Benslama of the University of Constantine, who understood that a new discipline was in the process of taking shape.

He demonstrated this by organizing the first International Symposium on Electromagnetism, Satellites and Cryptography in Jijel, Algeria in June 2005. The success the congress enjoyed, surprising for a first event, shows that there was a need to gather, in a single place, specialists in skills that were sometimes much removed from one another. The 140 accepted papers covered systems for electromagnetic systems as well as circuit and antennae engineering and cryptography, which is very often based on pure mathematics. Synergy between these disciplines is necessary to develop the new field of activity that is satellite communication.

The emergence of new disciplines of this type has been known in the past: for electromagnetic compatibility, it is as necessary to know electrical engineering for "driven modes" and "choppers" as electromagnetics ("radiating modes") and to be able to define specific experimental protocols. Further back in time, we saw the emergence of computing, which, at the start, lay in the field of electronics and was able, in the course of time, to become independent.

Professor BenSlama has the outlook and open-mindedness indispensable for bringing to fruition the synthesis between the skills that coexist in satellite telecommunications. I have known him for 28 years and for me it is a real pleasure to remember all these years of close acquaintance. There has not been a year in which we have not had an opportunity to see one another. First, for 15 years, he worked on the interaction between acoustic waves and semiconductors. He specialized in resolving piezoelectric equations (Rayleigh waves, creeping waves, etc.), and, at the same time, he was interested in theoretical physics. A doctoral thesis in engineering and then a state thesis crowned his professional achievements.

Notably, his examination committee included Madame HENAF, then Chief Engineer for the National Center for Telecommunications Studies. He was already interested in telecommunications, but also, with the presence of M. Michel Planat, responsible for research at CNRS, in the difficult problem of synchronizing oscillators.

It is with Michel Planat that he developed the way that will lead to quantum cryptography. He made this transformation over 10 years, thus moving without any apparent difficulty from Maxwell's equations to Galois groups. He is now therefore one of the people most likely to dominate all those diverse disciplines that form satellite telecommunications.

I wish, with all my friendly admiration, that these four monographs meet with a warm welcome from students and teachers.

Emeritus Professor Henri BAUDRAND
ENSEEIHT Toulouse

Preface

This book follows on from three other books published by ISTE [BEN 15, BEN 15, BEN 16]. I would like to express my respect and gratitude for this publishing house, which makes a decisive contribution to the publishing and distribution of French-speaking scientific authors. I could not forget Professor Guy Pujolle, Director of the *Networks and Telecommunications Series*, in which this book is published, I am infinitely grateful to him.

In a previous publication, we tackled the transitions from digital to quantum communications in the context of engineering; as the quantum aspect was not discussed sufficiently, we will try to address this lacuna through this new work. In fact, it seems opportune to deepen our knowledge of quantum engineering via a work targeting practical aspects while still integrating the aspect of formalism and paying attention to clarity, comprehension and the concepts' usefulness. This book therefore aims to address quantum communications and possible new applications in telecommunications. In collaboration with Professor Achour Benslama, who has been working on the question of the evolution of quantum mechanics, and Dr Aris Skander who has refined the laser and cryptography aspects, we will provide the scientific community with a work that aims for a synergy between the theoretical foundations of quantum communications and their current and future applications in the domain of telecommunications.

Malek BENSLAMA
Achour BENSLAMA
November 2016

Introduction

The initial idea behind writing this work was to explore technological advances in quantum communications. The main inspiration was the famous quantum computer and all the technology that might lead to its creation. We could not avoid either the formalism of quantum mechanics, or the need to find concepts similar to signal processing to ensure its feasibility in practice. Nor could we evade the consequences of discussions between proponents of determinism (Einstein, Rosen and Podolsky) or those of randomness (Heisenberg and the Copenhagen School). Our preference for practicality prevailed over the more formal aspect. In reading the works of philosophers of science, we will in particular cite Michel Bitbol who supported the assertion that quantum mechanics is a generalized probability theory, in which we found some solace; we can therefore speak of processes, expected values, covariance, etc., and signal theory is not far off. Only the important aspects were worth including in our work: contextuality, non-locality, and specific inequalities that may be temporal, spatial or random. To do this, we have paid particular attention to Bell inequalities (for space), Kochen–Specker (for contextuality) or Leggett–Garg (for time), and the violation have also been noted due to the need for comprehensiveness. Two concepts specific to the quantum domain have also been addressed: decoherence and entanglement. Using explanatory diagrams, we have shown the benefits of these two concepts, and their consequences.

For more than 40 years all of our computers have functioned thanks to silicon electronics, which has enabled us to move from having 2,000 transistors on a chip in 1971 to more than six billion today. But 10 years from now, this frantic progression towards miniaturization risks reaching its limits, as dictated by the laws of physics. From 22 nm today, the etching of electronic chips is at risk of dropping to 16 nm in

2016 and finally 5 nm around 2020, which is the equivalent of almost 50 atoms side by side.

But to arrive at such a level of integration, electronics and IT will be confronted by two formidable barriers: one is technology and the other is economics. Scientists believe that it will be very difficult, in fact impossible, to drop below this limit of 5 nm without radically changing the technological approach; as a new arrival in this nano-world, electronics is dominated by the laws of quantum physics.

Moreover, many analyses emphasize that Moore's law, which has governed developments in IT for almost half a century and predicts that the numbers of transistors on a single chip will double every 2 years, will also face the economic barrier of diminishing returns.

In concrete terms, when we have reached transistors of 10 nm, each reduction in the fineness of etching electronic circuits will demand greater and greater technological and industrial investments for an increase in speed and efficiency that is less and less perceptible to the consumer.

It is therefore absolutely necessary, for the reasons that have just been given, for IT to undergo major upheavals in the course of the next 10 years in order to prepare for the "after silicon" era, whose arrival is inexorably approaching.

Quantum communications can only be grasped through their essential element: the qubit and its derivatives (qudit, qutrit, ququad), as well underlying quantum circuitry. Quantum gates have therefore been postponed. Wigner distribution and the quantum Fourier transform have been developed.

The main applications for quantum communications in the domain of telecommunications are beginning to appear. For this, we will build on the developments achieved on quantum transistors, nanocrystals, and nanoclusters.

In optic fibers, we introduce the creation of light memories thanks to solitons, in which a laser beam circulates in a coiled electric fiber. In the near future, such lasers, threaded with optical solitons, may perhaps serve to store bits of information in looped fibers. The light will not only be a messenger: it will also be a memory. Thus, the recent marketing of the first LiFi (light fidelity) lamps, as well as terminals able to capture this new wireless technology using the LED light network (electroluminescent diodes) to transit and access data using the internet, will enable high-speed data transmission. This technology is faster than WiFi (wireless fidelity). Securing encrypted data and a specific location and ensuring its confidentiality, as only accessible in the light beam emitted by the LED, will be an important asset.

Some other advantages generated by this technology can be summarized by the following points:

– no interference with radio transmission equipment;

– constant data transmission speed;

– absence of risks to health, no radio or electromagnetic transmission.

The importance of creating memories was one of our first reasons for introducing solitons.

In circuits, an evolution is now occurring in the transition from charge electronics to spin electronics. Most spin electronics nanosystems suffer from the same limitations as those of conventional electronics: they are sensitive to the dispersions of magnetic properties that become inevitable when we approach nanometric sizes and the limits of nano-structuring technologies. An original way of overcoming these problems linked to miniaturization is using magnetic nanometric configurations that enter the class of magnetic solitons. The solution could come from solitons. A characteristic property of a soliton is that its nature confers on it a great immunity to imperfections that defects in material and thermal fluctuations can create.

Another advantage is that magnetic solitons do not require an electrical supply to sustain themselves once created. Mastering their existence and manipulation has thus opened a new paradigm for the electronics of tomorrow, giving rise to new functionalities for pursuing miniaturization beyond the limits which are visible today. This, for us, constitutes a second reason for processing solitons. The development in solitons will be tackled via optic fibers.

Some elements of quantum technology have reached maturity and are available commercially, such as quantum key distribution systems. Other elements of quantum technology are now becoming realized, such as large-scale secure networks, quantum lithography and quantum IT processors. Photonics will occupy a central role in these technologies in regard to high-speed transmissions and weak photon properties. We therefore retain the fact that quantum photon technology will be one of the main sources of development in quantum communications. This has been proved by quantum entanglement, which has been tested experimentally by using photons generated from atom cascades. Non-linear processes for spontaneous parametric conversions have been a source of photon pairs for experiments in generating quantum states from a brilliant laser beam, and crushed states. Parametric conversion has also been used for quantum teleportation. One can also consider the interaction of single photons with single atoms in an optic cavity, which will be a major technology for photonic quantum technologies.

We will process photonics using crystals in a dedicated chapter (Chapter 6), which will highlight their use for routers and wave-length demultiplexers (WDM).

Devices with photonic band gap can be used to create WDMs. Light sources need to have a broad wavelength tunability, low chirping and great stability in temperature. These devices include ultra-selective filters, which are very useful for dense WDMs.

At the level of radiation, it is useful to think of photonic band gap antennae, as well as photonic antennae, which will be an integrating element in quantum communications technology.

Over recent decades, substantial theoretical and experimental progress has been made in understanding the quantum nature of physical phenomena, which is the basis of current and future technologies. Quantum correlations, such as the entanglement of composite system states and the phenomenon of quantum discord, which captures other aspects of quantum correlations, quantum contextuality and, linked to these phenomena, uncertainty relationships for conjugated variables and entropies, such as Shannon and Reyi entropies, and inequalities for spin states, such as Bell inequalities, reflect the quantum properties of micro- and macro-systems. The mathematical methods necessary for describing all the quantum phenomena mentioned above were the subject of intense study at the end of the last century, and at the beginning of this century.

The other new direction in elaborating the mathematical approach to quantum physics is tomography, which offers a new vision of quantum states. In the tomographic image of quantum mechanics, states are identified with equitable conditional probability distributions, which contain the same information on the states as the wave function of the matrix density. Mathematical methods for the tomographic approach are based on studying the star product (associative product) of the quantification scheme. The star tomographic product provides an additional understanding of the associated product, which is linked to the existence of specific pairs of operators called quantifiers and de-quantifiers [MAN 13].

Theoretically, it is important to remember key facts. In his article, Eli Maor specifies how he has been able to understand Heisenberg's uncertainty principle [MAO 09]. Heisenberg's uncertainty principle, feted as perhaps the most important principle of modern physics, was the most elusive of all. You cannot simultaneously determine a particle's position and dynamic (i.e. speed) with absolute certainty. Any increase in the determinism of one of these quantities occurs to the detriment of the uncertainty principle of the others. This process immediately became one of the foundations of modern physics. Its influence on the way in which scientists think of

the world has become very pervasive. It reaches beyond physics and has become part of our everyday language.

In quantum information theory, the non-communication theorem is a result that gives conditions in which the instantaneous transfer of information between two observers is impossible.

[ARA 11] gives a no-go theorem for probabilistically checkable proof (PCP), or probabilistic proof. Finally, to conclude this introduction, we come to consider the evolution of quantum mechanics above all for aspects dedicated to quantum communications [BLI 29].

This book will include three main sections: a comprehensive review of the state-of-the-art in quantum communications, an analysis of current and future circuitry, and finally we close with quantum signal processing. On state-of-the-art quantum science, we will focus our enquiry on decoherence, which is the major characteristic of quantum communications. Two other quantum characteristics – the qudit and the qutrit – should be sufficiently explained on the basis of geometric concepts and their explanation should be correlated with the notion of the qubit. In the second section, we will handle all the quantum circuitry.

1

The State of the Art in Quantum Communications

1.1. Quantum mechanics as a generalized probability theory

We have borrowed part of Michel Bitbol's analysis of quantum mechanics analyzed as a probability theory. In his pamphlet, he says [BIT 98]:

"The argument that I will defend here makes two propositions. First, quantum mechanics is not just a physical theory that uses probability calculation; it is itself a generalized form of probability calculation, coupled with a probabilistic evaluation process via the set use of symmetries. Secondly, quantum mechanics does not merely have a predictive function like other physical theories; it is a formalization of the possibility conditions of any prediction focused on phenomena whose circumstances of detection are also production conditions".

In this spirit, we begin by quickly showing the architecture of standard quantum mechanics:

1) The formal core of this theory is a vector space defined on a set of complex numbers and provided with a scalar product otherwise known as Hilbert space.

2) Special operators are defined on this space, called "observables", which, through their "proper values", provide a list of the possible results of a measuring operation.

3) A vector of the Hilbert space, called a state vector, is linked to each preparation (that is to say, to the fixing of conditions that are a prerequisite for measuring).

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

4) By applying the Born rule to this state vector, we obtain a function that assigns probabilities to the results of any measurement carried out as a result of the preparation.

5) A variable space–time interval and diverse physical circumstances can separate the end of the operation from the measurement preparation and operation; we take account of this via an evolution equation for the state vectors.

Here, I would like to emphasize the major difference between the probability functions of classic probability theory, and those obtained from state vectors in quantum mechanics by applying the Born rule. The classic probability functions link a number between 0 and 1 to each "event" in the widest sense, defined by Kolmogorov as a sub-set of elementary events. The set of these event sub-sets includes the empty set and the comprehensive set and it is provided with a Boolean algebra structure by the union and intersection operations. In other words, the classic probability functions are defined on a Boolean algebra. On the other hand, when we take account of the Hilbert space properties, the quantum probability functions are not defined on a Boolean algebra; they are defined on different and richer structures called "orthoalgebras".

This structural disparity between the classic and quantum probability functions explains why it is not sufficient to assume that quantum mechanics uses probability theory. Quantum mechanics itself consists of a new and enlarged form of probability theory [BLI 29]. The new circuits are a conjunction of quantum theory and probability theory, as shown in Figure 1.1.

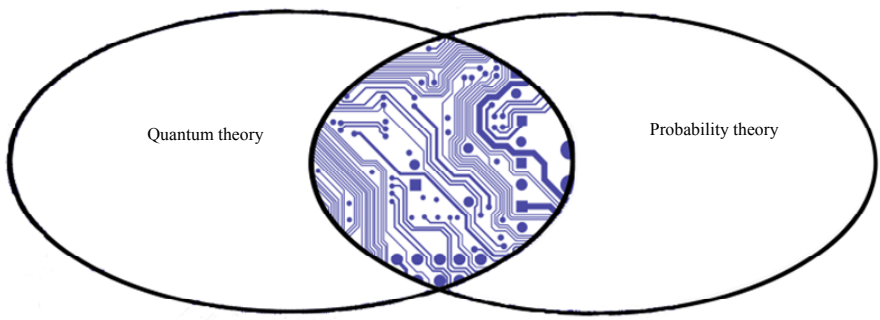


Figure 1.1. *Connection between quantum theory and probability theory*

The following references advance the same vision [THA 15, FER 08, FER 09] and [FER 11].

Starting from this analysis, it seems important to us to examine quantum communications on the basis of the probabilities and concepts related to this theory: covariance, correlation [FUR 12] inference and random processes, while including some concepts specific to quantum mechanics: contextuality [DZH 14], non-locality [RAB 14], paradoxes such as Schrodinger's cat, the Einstein, Podolsky and Rosen paradox, Bell inequalities [KRE 14, RAS 15] and decoherence [KOK 11]. Subsequently, we will try to create a synthesis between proponents of determinism and randomness.

Standard quantum mechanics undeniably violates the notion of separability that we have normally considered valid under classical physics. In relating the phenomenon of non-separability to the all-important concept of potentiality, we effectively create a coherent picture of correlations between the spatially-separated entangled enigmatic systems. Moreover, we support the idea that the generalized phenomenon of quantum non-separability involves contextuality, which, in turn, results in a relational, structural design of quantum objects, considered to carry dispositional properties [KAR 07].

1.2. Contextuality

Quantum computers promise enormous advantages over their classic counterparts, but the source of their power in quantum IT remains inaccessible. Here, we show a remarkable equivalence between the appearance of contextuality and the possibility of universal quantum calculation via the magic state that we call distillation, which is the main model for creating a quantum computer with tolerance to breakdown. Furthermore, this connection suggests a unifying paradigm for quantum IT resources: the non-locality of quantum mechanics is a particular type of contextuality, and non-locality is already known to be an essential resource for realizing the advantages of quantum communication. In addition to clarifying these fundamental questions, this work sets out the resource framework for quantum calculation, which has a number of practical applications, such as characterizing efficiency and compromising between distinct theoretical and experimental schema to reach a robust quantum calculation, and to place limits for the classic simulation of quantum algorithms [HOW 14].

1.3. Indeterminism and contextuality

These two historic remarks, one on the link between the concept of probability and the secondary concept of quality, and the other on calculating probabilities, designed as an instrument of predictive control for our situation of entanglement in

the network of natural relationships, will now help us to unravel two interpretative nodes of quantum physics, each relying on indeterminism.

The first involves the notion, very widely known from Heisenberg's founding work of around 1927–1930, of an uncontrollable disturbance that the measuring agent is supposed to exercise on the microscopic subject measured. It is interesting to note that this "disturbance" was assigned a double role by its creators.

On the one hand, underlined by Bohr at the end of the 1920s, uncontrollable disturbance is the reason why the quantum phenomenon is indivisible, that is to say it is impossible to distinguish what in the phenomenon results from the object and what results from the measurement agent. The disturbance would explain, in other words, taken this time from Heisenberg, that quantum physics causes the mode of secondary qualities to become generalized, with their inevitable reference to the context in which they are manifested, to the detriment of that of the primary intrinsic qualities. But, on the other hand, according to an article from 1927 in which Heisenberg shows the relationships known as "uncertainty" relationships for the first time [HEI 27], the disturbance also accounts for indeterminism in quantum physics. The incompressible and uncontrollable disturbance created by the measuring agent is what prevents the two groups of variables that make up a particle's initial state from being known completely; consequently, Heisenberg concludes, the principle of causality, which links an initial state and a final state, links them in a way which is binding and remains inapplicable in quantum physics. The model of the "disturbance" also enables a direct relationship between contextuality and indeterminism to be shown, since the disturbance results in the phenomena's contextuality as much as in indeterminism for their subject. Later on, at the beginning of the 1950s, Paulette Destouches-Février demonstrated much more rigorously a theorem according to which any predictive theory relying on phenomena defined in relation to experimental contexts, some of which are mutually incompatible, is "essentially indeterminist" [BER 49].

1.4. Contextuality and hidden variables

The question of knowing if quantum phenomena can be explained by classic models with hidden variables has been the subject of lengthy debate. In 1964, Bell showed that certain types of classic models cannot explain the predictions of quantum mechanics for specific states of distant particles, and certain types of hidden variable models have been experimentally excluded. An intuitive characteristic of classic models is non-contextuality: the property that any measurement has a value independent of the other compatible measurements carried out at the same time. However, a theorem drawn up by Kochen, Specker and Bell shows that non-contextuality is in conflict with quantum mechanics. The conflict lies in the structure

of the theory, which is independent of the properties of the special states. The question of knowing if the Kochen–Specker theorem could be tested experimentally has been discussed. The first tests for quantum contextuality have been suggested recently and undertaken with photons and neutrons. Here, we carry out an experiment with trapped ions, which shows a conflict between state independence and non-contextuality [KIR 09].

1.5. Non-locality and contextuality

We use the mathematical language of beam theory to give a unified treatment of non-locality and contextuality, in a framework that generalizes the familiar probability tables used in non-locality theory for arbitrary measurements: this includes Kochen–Specker configurations. We show that contextuality and non-locality, a particular case, correspond exactly to obstacles to the existence of global sections. We describe a linear, algebraic approach for calculating these obstacles, which permits a systematic treatment of non-locality and contextuality. We distinguish an adequate hierarchy of no-go theorem forces, and we show that the three main examples, taken from Bell, Hardy and Greenberger, and Horne and Zeilinger, respectively, occupy higher levels of this hierarchy. A general correspondence is shown between the existence of variable, local, hidden implementations using negative probabilities, and "no signaling"; this depends on a result showing the linear sub-spaces generated by the non-contextual and "no signaling" models. The maximal non-locality is generalized to maximal contextuality; it is characterized in purely qualitative terms, with Kochen–Specker results as generic. These models are independent proofs of maximal contextuality, and a new combinatorial state is given; it generalizes the "proofs of parity" much discussed in literature. This shows that quantum mechanics obeys "no signalling" families of commuting observables that are represented as a tensorial product of different factors [ABR 11].

Quantum contextuality is one of the fundamental notions in quantum mechanics. It has been shown that some tests of the Kochen–Specker theorem, such as those based on rays, can be converted into a non-state independent contextuality inequality. This question, namely if a proof of the Kochen–Specker theorem can always be converted into a non-contextuality inequality, remains open. In Yu's article, there is an answer to this question. The author shows that all types of proofs of the Kochen–Specker theorem, based on rays, or any other observable, can always be converted into independent non-contextuality inequalities. Furthermore, a constructive proof also provides a general approach for determining an inequality independent of state non-contextuality from a demonstration of the Kochen–Specker theorem [YU 15].

The Bell inequality (for space), Kochen–Specker inequality (for contextuality) and Leggett–Garg inequality (for time), are based on plausible, classic but entirely distinct hypotheses. For each of these inequalities, realization is equivalent to a joint probability distribution for all the observables in the experiment. This involves a joint distribution for all the pairs of observables, and this stands whether we know if they commute or not. This indifference is the basis for unifying the inequalities above in the general context of correlation inequalities. When the physical scenario is such that the correlated pairs are all compatible, the resulting correlation is of the "no signaling" type; it can be local or have multiple particles, corresponding to contextuality or to Bell inequalities. If the pairs are incompatible, the resulting correlation corresponds to the Leggett–Garg inequalities. If quantum mechanics violates all these inequalities, this will suggest a direct link between the theory's local, spatial and temporal properties [DAS 13].

Winter [WIN 14] gives an experimental test of the Bell-Kochen–Specker theorem following Meyer, Kent and Clifton's demonstrations, which ensures that predictions using quantum mechanics are indistinguishable from the non-contextual model.

In theoretical physics, a no-go theorem is a theorem that affirms that a certain situation is not physically possible. More specifically, this term describes results of quantum mechanics such as the Bell theorem and the Kochen–Specker theorem and governs the types of hidden variables admissible, which attempt to explain the apparent randomness of quantum mechanics as being a determinism involving hidden states.

In quantum information theory, non-communication theory is a result that gives conditions under which the instantaneous transfer of information between two observers is impossible.

1.6. Bell states

In the course of the last few decades, substantial theoretical and experimental progress has been made in understanding the quantum nature of physical phenomena, which is the basis of current and future technologies. Quantum correlations such as the entanglement of the states of composite systems and the phenomenon of quantum discord, which are linked to other aspects of quantum correlations, quantum contextuality and, linked to these phenomena, uncertainty relations for variables and combined entropies, such as Shannon and Reyi entropies, and inequalities for spin states, such as Bell inequalities, reflect the quantum properties of micro- and macro-systems. The mathematical methods needed to

describe all the quantum phenomena mentioned above were also the subject of intense study at the end of the last century, and at the start of the new century.

Another new direction in elaborating the mathematical approach to quantum physics is tomography, which offers a new vision of quantum states. In the tomographic image of quantum mechanics, the states are identified with equitable conditional probability distributions, which contain the same information on states as the wave function or the density matrix. The tomographic approach's mathematical methods are based on the study of the quantization schema's star product (the associative product). The tomographic star product provides an additional understanding of the associative product, which is linked to the existence of specific pairs of operators called quantifiers and dequantifiers [MAN 13].

1.7. Violation of the Leggett–Garg inequality

By weakly measuring the polarization of a photon between two strong polarization measurements, the author experimentally studies the correlation between the appearance of abnormal values in weak quantum measurements [GOG 11]. A quantitative formulation of the latter concept is expressed in terms of a L-G (Leggett–Garg) inequality for the results of subsequent measurements of an individual quantum system. We experimentally violate the Leggett–Garg inequality over several measurements. Moreover, we demonstrate experimentally that there is a correlation between obtaining unexpected weak values and violating the Leggett–Garg inequality [GOG 11].

Assano and coauthors interpret the Leggett–Garg inequality as a contextual probabilistic inequality in which the collected data are combined in experiments in three different contexts.

In the original version of this inequality, the contexts have a temporal nature, they are represented by three pairs (t_1, t_2), (t_2, t_3), (t_3, t_4) with $t_1<t_2<t_3<t_4$. They generalize the Leggett–Garg conditions of macroscopic realism and non-invasive measurability in a general contextual framework. Their formulation is developed in purely probabilistic terms, the existence of a context independent of a probability distribution (two-dimensional) and the possibility of reconstructing marginal probability distributions from P. They determine an inequality analogous to L-G, which they call the contextual L-G, and as a quanticity test, they use statistical data collected in a series of experiments in recognizing ambiguous figures. In the experimental study, the figure under examination is Schröder's stairs, which is shown with rotations from different angles, the contexts are coded by dynamic rotations in three directions: clockwise,

anti-clockwise, and in a random direction. The data demonstrate a violation of the contextual L-G inequality for the combinations of contexts mentioned above [ASA 14].

1.8. Violation of the Bell inequality

Non-local correlations between spatially separated systems have been discussed broadly in the context of the Einstein, Podolsky and Rosen paradox (EPR) and Bell inequalities. Many ideas and experiments intended to test the hidden-variable theories and violation of the Bell inequalities have been mentioned, usually these photons consist of correlation, although recently an experiment was carried out with Be^{+} (Beryllium ions). Nevertheless, there is considerable benefit in showing that these correlations (resulting from quantum entanglement) are not just a particularity of photons. Here, we measure the correlations between simple neutrons' two degrees of freedom (including spatial and spin components); this removes the requirement for a source of neutrons in entangled pairs, which present a considerable technical challenge. An inequality equivalent to Bell is introduced to clarify the correlations that can supervene between observables of independent degrees of freedom. We demonstrate the violation of this Bell inequality as follows: the measured value is 2.051 ± 0.019, clearly higher than the value of 2 predicted by the classic hidden variable theories [HAS 03].

Experimental situations in which quantum effects are observed pose a fundamental question to be taken into consideration: this is the compatibility between the description of phenomena and the objective reality hypothesis. This work tackles Bohm's ontological interpretation of quantum mechanics, concentrating on the use of the term "trajectory" and the difficulties associated with connecting it to a real (objective) trajectory. The conclusion is that the realistic interpretation applied to Bohm trajectories is very debatable [BOS 13].

Bohm gives an interpretation of quantum theory in terms of hidden variables [BOH 52]. Another, equally interesting article on the significance of electromagnetic potentials in quantum theory is given by Aharonov and Bohm. In this article, the authors discuss some useful properties of electromagnetic potentials in the quantum domain [AHA 59].

1.9. EPR paradox

This is a major article known as the EPR paradox. The authors stipulate that in a complete theory, there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of making

a prediction with certainty without disturbing the system. In quantum mechanics, for the case of two physical quantities described by non-commuting operators, knowing one precedes knowing the other. Therefore, either the description of the reality given by the wave function in quantum mechanics is not complete or these two quantities cannot simultaneously have reality [EIN 35]. An experiment showing the EPR paradox has been carried out by Birgit Dopfer [DOP 98] and is shown on Figure 1.2.

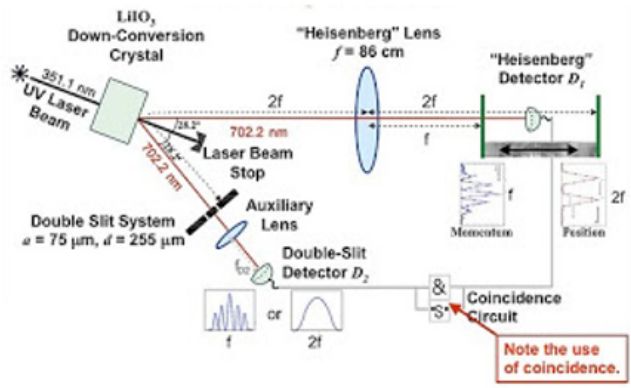


Figure 1.2. *Einstein-Podolsky-Rosen experiment according to [DOP 98]. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

The EPR paradox, an abbreviation of Einstein-Podolsky-Rosen, is a thought experiment developed by Albert Einstein, Boris Podolsky and Nathan Rosen; its first goal was to refute the Copenhagen interpretation of quantum physics. The Copenhagen interpretation is opposed to the existence of any state of a quantum system before any measurement. In effect, there is no proof that this state exists before it is observed, and assuming it does raises certain contradictions.

Indeed, if two particles are transmitted and a conservation relationship exists between one of their properties (for example, the sum of their spins should be null, that is to say there should be quantum entanglement of the state of these two-particle system), knowing the state of the first after measuring it tells us the state of the second particle before a measurement is later made on it, whereas – according to the Copenhagen interpretation – the measured value is determined randomly at the moment of measurement. If the measurement on the first particle has given "+", and the first particle is thus now in state "+", the measurement on the second will always give "–".

One of the problems is that this latter particle can, at the moment of measurement, be located at as large a distance as desired in the observable universe

from the first. The world line that links the two events, “measurement on particle 1” and, “measurement on particle 2” in space–time can be a space curve, and the second particle therefore absolutely cannot, in the latter instance, “be informed” in any way whatsoever, of the state that the first was in after measurement. How can we believe, in these conditions, that the state in which the second particle is found after measurement was not determined from the start, in contradiction with the Copenhagen representation?

This paradox was developed by Albert Einstein and two of his collaborators, Boris Podolsky and Nathan Rosen, to expose what appeared to be a contradiction in quantum mechanics, or at least a contradiction of at least one with the three following hypotheses:

1) It is impossible for a signal to exceed speed c (relativistic causality).

2) Quantum mechanics is complete and describes reality entirely (no hidden local variable).

3) The two distant particles form two entities that can be considered independently of one another, each being localized in space–time (locality).

The EPR argument, as presented in 1935, is based on the following reasoning.

First of all, we must remember that the uncertainty principle states that it is impossible simultaneously to know the precise value of two physical quantities called incompatibles (typically, the speed and position of a particle). The more precisely one quantity is measured, the less determinate the measurement of the other.

The EPR draws two mutually exclusive statements from this principle:

1) The description of reality given by quantum mechanics is not complete.

2) The two incompatible physical quantities do not simultaneously have an objective reality.

The Copenhagen interpretation reaches the conclusion that (2) is true and (1) is false, so the EPR intends to demonstrate that (1) is true and (2) is false.

To do this, they refine a thought experiment that leads to the simultaneous determination of two non-commutable physical quantities, and so lead to the conclusion that (2) is false and consequently (the two statements being mutually exclusive) (1) is true.

To demonstrate that (2) is false, it is vital to define precisely what the notion of the "reality" of a physical quantity is (for example, the "position"). EPR reveals a sufficient "reality":

If, without disturbing a system's state at all, it is possible to predict the value of a physical quantity of this system with certainty (with a probability equal to 1), then there is an element of reality corresponding to this physical quantity.

The thought experiment suggested in 1935 is quite complex, but can be described more simply without changing its meaning (see Figure 1.3).

If P_1 and P_2 are two photons entangled in such a way as to have a total angular moment equal to zero (anti-correlated spins), then the two non-commutable physical quantities used in the reasoning are: (1) The spin measured in a direction Sx (2) The spin measured in another direction Sz.

If P_1 is measured along to Sx, then – without disturbing P_2 (the locality principle is assumed) the measurement of P_2 is necessarily known along this axis (the opposing axis). Similarly, if P_2 is measured along to Sz, then – without disturbing P_1, the measurement of P_1 is necessarily known according to this axis (the opposing axis again).

Therefore, measuring P_1 along one axis and P_2 along the other enables the value of two physical quantities to be predicted with certainty. These two quantities therefore possess an objective reality, and consequently (2) is false and (1) is true.

This is the paradox initially created by EPR.

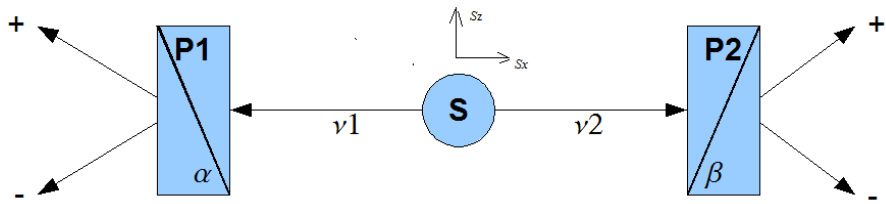


Figure 1.3. *Pictorial explanation of the EPR paradox*

2

Concepts in Communications

2.1. Quantum limits

Quantum coherence and quantum correlation applications in optics have been discussed by [KNI 01]. Coherent states are an ideal tool for handling the boundary between classic and quantum properties; it can be shown that by using coherent states, analytical solutions can be found to previously unsolvable nonlinear quantum problems. Quantum optics has generated new applications that use the possibilities of quantum states of light, such as coherence and quantum correlation. The latter is known as entanglement. It can be shown how it is possible to obtain images of objects at weak intensity with a sensitivity that exceeds the standard quantum limits. The authors also show that the biphotons that are created in the process of parametric decay exhibit a space–time correlation phenomenon, which is called entanglement. Applications based on the impossibility of cloning unknown quantum states are unique; they have been developed in the field of quantum cryptography. An EPR experiment with entangled and polarized photons has been developed to test its feasibility. In line with this, the quantum correlations between spatially separated events are due to the propagation of a signal in superluminal communication in a chosen context: the coincidences between the entangled photons pass through two polarizers aligned along an east–west axis and are measured as a time function over 21 sidereal days. No deviation from this prediction of quantum theory has been observed. Taking account of the experimental uncertainties, we infer that if a chosen framework for super-luminal signals exists, then this moves at a velocity v depending on the Earth. The velocity module of quantum communications in this context is greater than $v_t \approx 0.6 \times 10^4$ c for $v < 0.1$ c for any arbitrary direction of v. A lower limit for the velocity of quantum communications has been identified by [COQ 01]. Another aspect in determining limits has been observed with the famous g factor in quantum communications for semiconductors III.V [KAS 01].

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

A practical implementation of quantum communications is expected, to demand the preservation of entanglement in photodetectors in which the quantum information is transmitted by polarizing a photon through an optic fibre and transferring it to the spin of one electron spin in a semiconductor. To maintain the entanglement, the photodetector should entirely absorb the two states of electron spin, and thus the g factor g of the electron should be made for $g_e \approx 0$. The effective mass's band structure can also govern the g factor.

The transfer of quantum information in a resonator coupled with a wave guide has been addressed by [IAF 96]. It proposes an efficient scheme for implementing quantum information in a one-dimensional resonator paired with a wave guide. It shows that on the basis of dipole–dipole interaction between the atoms linked to the cavity modes, Raman transitions between the atoms trapped in the different nodes can take place. The quantum information can be transferred directly between the opposite sides of the paired guide without introducing intermediary nodes via the Raman transitions or stimulated adiabatic Raman passages. In principle therefore, this schema is a protocol stage, which can lead to useful applications in quantum communications.

High-performance receivers for optical communications are also an essential source for quantum communications according to [KNI 00], in which the principles of optical detection are reviewed, and where the practical creation of devices and receivers for digital optical communications are discussed. The emphasis is on signal processing techniques for advanced electronic or optoelectronic receivers. They are currently providing performances that are approaching the basic limits imposed by the considerations of quantum mechanics. The procedure follows a direct detection process.

Direct detection can be seen as a simple mapping of photons to conduction electrons.

Let P the level of the incident optical power and í the optical frequency linked to the wavelength in free space l by c = ie, where c is the speed of light in the vacuum. If h is the Planck constant, then the energy per photon is hi = hc/e and the arrival rate of the photons is given by:

$$\frac{P}{h\nu} = \frac{P\lambda}{hc}$$

Each photon detected produces exactly an exterior electrical carrier, but not all the photons are detected. The carrier's generation rate is therefore lower than the arrival rate of the photons as determined by the probability of detection known as the quantum efficiency ç. The carriers' generation rate is therefore:

$$\eta.\frac{P\lambda}{hc}$$

Each electronic carrier transports a unit of electronic charge of q coulombs and the significant rate of charge flow is the photocurrent I, which is given by:

$$\mathrm{I} = \eta.\frac{q\lambda}{hc}P$$

The ratio of I/P to A/W is known as the R response detector. Since ç ≤ 1, the response is limited at its upper limit by:

$$R \leq \frac{q\lambda}{hc}$$

which is proportional to the wavelength.

This latter characteristic simply reflects the fact that large wavelengths correspond to low optical frequencies, that the energy per photon is lower and we therefore have a high rate of photons for a given level of optical power. Current fibre optics systems operate in a wavelength interval ranging from 850–1,550 nm, and current detectors can have quantum efficiencies approaching the unit. As a consequence, responses in the region of 0.5–1.0 A/W are typical, and they depend on the wavelength used.

2.2. Qubits

A bit is a mathematical object that enables the state in a classical physical system to be described. At a given instant, it takes 0 or 1 as a value. The quantum bit, called a qubit, describes the state of a quantum system. It can take the value 0 and 1 as a classic bit, but also all the intermediary values, a linear combination of states 0 and 1. Dirac notation comprising bras and kets is used. Figure 2.1 explains the transition

from the classic to the quantum vision. The main works relating to this theme are listed in the following references: [ELD 01, ELD 02, KNI 11, NIE 10].

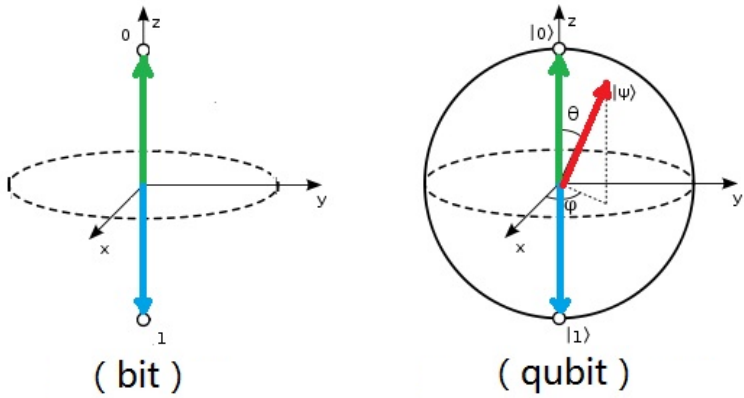


Figure 2.1. *Transition from classic bit to quantum bit*

Qubits are (Hilbert) space vectors whose 2n dimension increases with their number n, a great novelty compared to classic space. They exploit the wave properties (which is not the case with bits) of entanglement and non-locality (a phenomenon unknown in classical physics). On the contrary, they are extremely fragile, being coupled with the classic environment by a process known as decoherence. The idea of quantum calculation for simulating physical phenomena is attributed to Richard Feynman, but the real impetus was given in 1994 when Peter Shor demonstrated the possibility of factorizing large numbers in polynomial time. We will start by illustrating how finite group theories and Lie group theories are useful for understanding the classic/quantum interface.

The classic bit takes two values, “0” or “1”. The quantum bit or qubit can also be found in two states “0” or “1”, which are now quantum system states. To distinguish them from classic states, they will be written $|0\rangle$ and $|1\rangle$.

The calculators are obtained by combining certain elementary logic gates. To overcome the problem of decoherence, silicon is used. Qubits can be carried by photons [WAN 13a] or electrons. In Figure 2.2, we show a photo representing a circuit with the introduction of qubits.

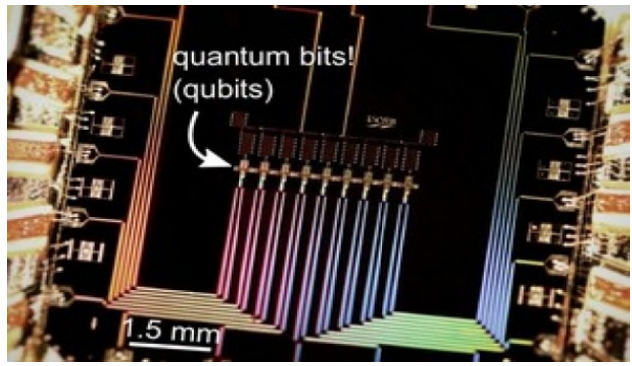


Figure 2.2. *Photograph of a circuit showing the introduction of qubits*

In some circuits with solid semiconductor based qubits, physicists encounter problems, as the presence of nuclei endowed with spin would disturb qubits carried by electrons. However in the case of silicon isotope 28, this problem does not exist, as the spin of this element's nucleus is null. By placing electrodes on a piece of silicon-28, researchers have been able to manipulate the spins of pairs of electrons trapped in this material [MAS 07]. More precisely, they used a technique known as electron spin resonance (ESR). They have been able to show that the qubit manipulations they were able to make reproduce the information processing expected from a CNOT quantum gate. This was a first with silicon and the result is encouraging.

Figure 2.3 shows this achievement.

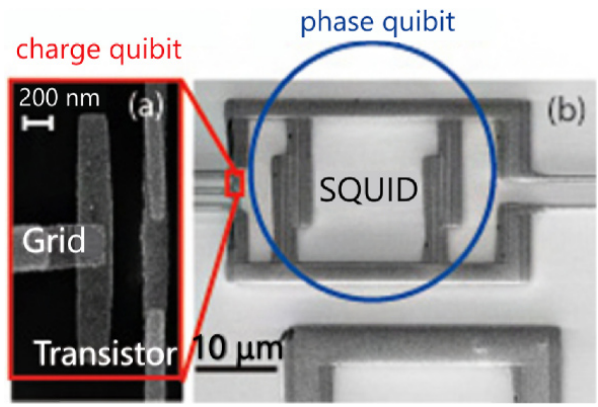


Figure 2.3. *Photo of a circuit showing the production of a qubit on a transistor*

In fact, for such a CNOT gate to be really usable, the electron pairs' qubits should be entangled. Researchers have still not been able to show that this is the case. If they succeed, physicists would then, in principle, have with this gate and other items all they need to construct a real silicon quantum computer chip able to contain millions of qubits [XU 13]. An example of a qubit carrying circuit is shown in Figure 2.4.

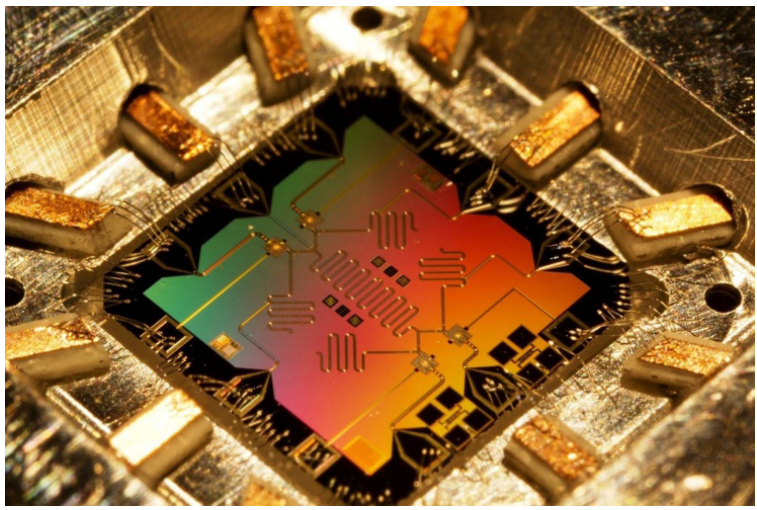


Figure 2.4. *An example of a circuit capable of carrying qubits*

A qubit is a quantum system with two dimensions. Its Hilbert space is composed of two proper states forming a base. They are orthogonal and are written $|0\rangle$ and $|1\rangle$. All the qubits are expressed in this base.

$$\left|\text{Qubit} \geq \cos\theta\right|0> + e^{j\varphi}\sin\theta\left|1>\right| \qquad [2.1]$$

with $0 \leq \theta \leq \pi/2$ and $0 \leq \phi \leq \pi/2$.

The angles θ and φ are two independent parameters characterizing a unique point on a unit sphere R^3, called a Bloch sphere, with the Cartesian coordinates:

$$X = \sin 2\,\theta \cos\varphi,\ y = \sin 2\,\theta \sin\varphi,\ z = \cos 2\,\theta \qquad [2.2]$$

A qubit is represented on this sphere in Figure 2.5. In this representation, $|0\rangle$ and $|1\rangle$. have the respective coordinates (0, 0, 1) and (0, 0, −1).

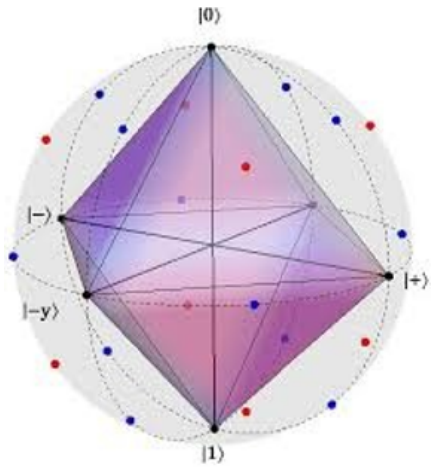


Figure 2.5. *Bloch sphere and representation of qubits. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

The principle of symmetry in the theory of multi-qubit systems has been the subject of work by Herbrüggen *et al.* on controllability and observability in multi-spin systems in varied symmetry architectures [HER 10]. What we note as the main result is the evolution of the Bloch sphere, following the increase of the number of qubits that we show in Figure 2.6.

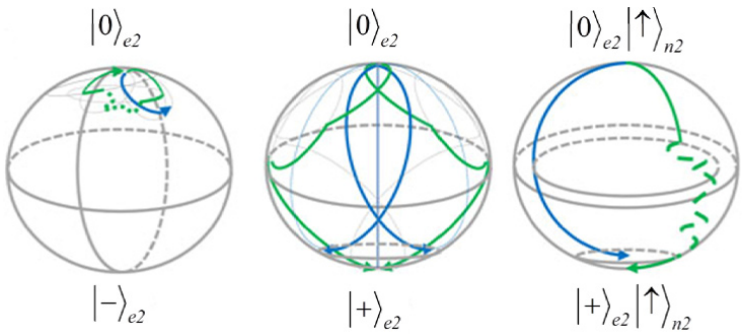


Figure 2.6. *Evolution of the Bloch sphere for multi qubits. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

The circuitry used to obtain the qubits comprises first an initialization process in which pulses are sent on a nonlinear optical crystal (BaB_2O_4), which will serve to separate two rays through two optical beam splitters PBS and PBS2 preceded by two filters. Four half-wave plates, HWP will generate the qubits [JOZ 08].

The second process comprises a phase estimation including four beam splitters and CNOT gates. Finally, the measuring process involves polarizers, a quarter wave plate and photodetectors. The complete process is shown in Figure 2.7.

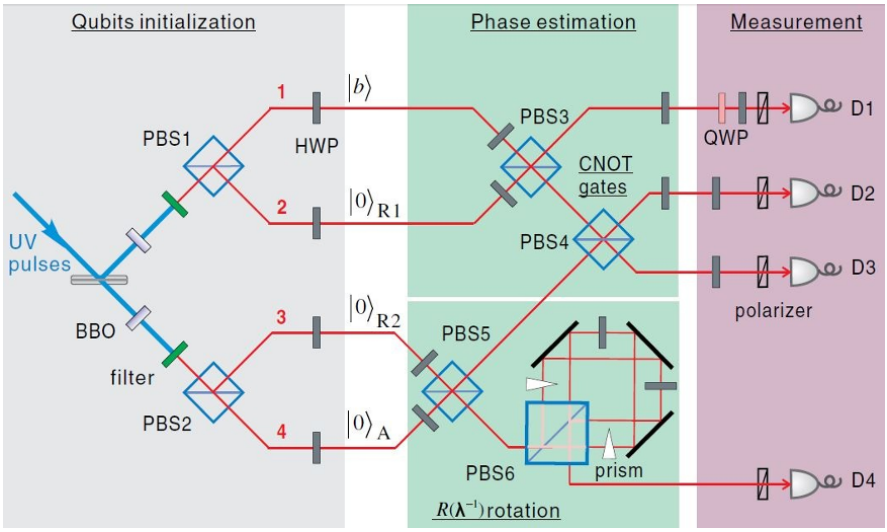


Figure 2.7. *Experimental process of initialization, phase estimation and qubit measurements*

2.3. Qudit and qutrit

2.3.1. *Qudit*

In a two-level quantum system, the name qudit is used. Similar to a qudit, a qutrit is a unit of quantum information in a quantum system with three levels. In the case of a system with four levels, we speak of a ququad.

Several works have highlighted the coding of qudits using photons emitted on demand from a system of atoms in a cavity [HOL 13]. The method used is, however, limited by the probabilistic nature of the sources of the spontaneous parametric conversion. In Figure 2.8(a), we show the experimental measuring device according to [HOL 13] and in Figure 2.8(b), the results thus obtained as well as the different phases developed by [HOL 13].

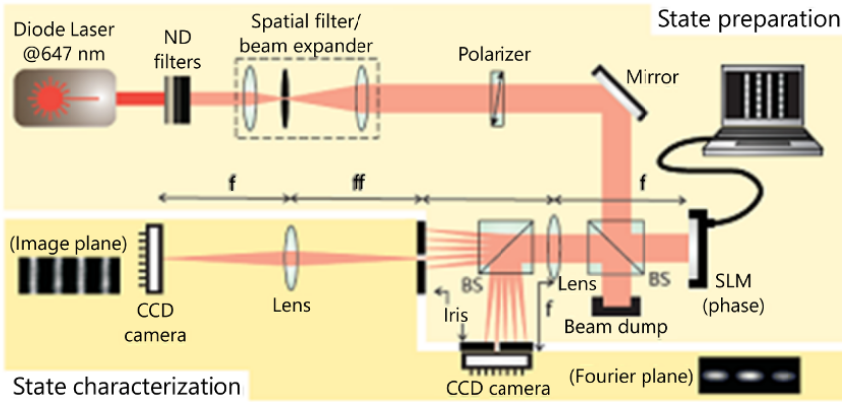


Figure 2.8(a). *Experimental setup*

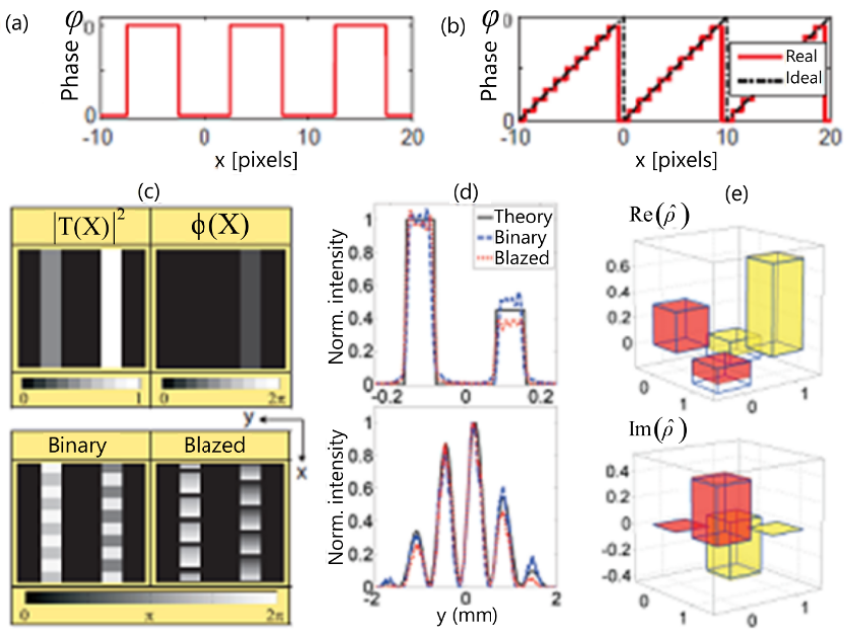


Figure 2.8(b). *Illustration of qudits*

D	2	3	4	5	7
States	561	24	70	25	94
F_{bin}	0.996	0.995	0.985	0.968	0.970
F_{bia}	0.996	0.996	0.991	0.971	0.977

Table 2.1. *Average qudits levels*

The reversal of the optimal asymptotic quantum channel for sets of qudits and multimode quantum states has been carried out by [BOW 12].

A new strategy for sending several senders to a receiver over arbitrary distances of two-qudit states in a determinist fashion has been tested successfully [JIA 13]. The regime is then extended arbitrarily to several qudits.

In quantum information processing, qudits are an extension of qubits that could make some tasks faster. The performance of a superconducting phase qudit with a number of levels, D to D = 5, has been demonstrated and means of manipulating and measuring the state of the qudit, including the simultaneous control of several transitions [NEE 09], have been demonstrated.

A classic algorithm that permits the design of a quantum circuit for the algorithmic quantum channel simulation of arbitrary qudits is given by [WAN 15, JOZ 98].

Fast decoders for qudit-based topological codes have been the subject of work by Anwar *et al.* [ANW 14]. On the same aspect of decoding, it is important to indicate the work of Hutter *et al.* on hard-decision renormalization group decoders [HUT 15]. These decoders are as useful for qudits as for quantum error correction for non-Abelian groups.

The use of elementary quantum systems for coding information is the key to several new approaches to quantum IT, as the technique used is linear, and based on optical quantum computing (IQC) in photonic circuits. Although this method is scalable in principle, in practice, it is limited by the stochastic nature of the spontaneous parametric conversion of the sources used to load the circuits. These sources produce simultaneous pairs of photons, one used as a messenger, the other to initialize a qubit.

In Figure 2.9, we show the experimental section and the results obtained by [NIS 13, JIA 13].

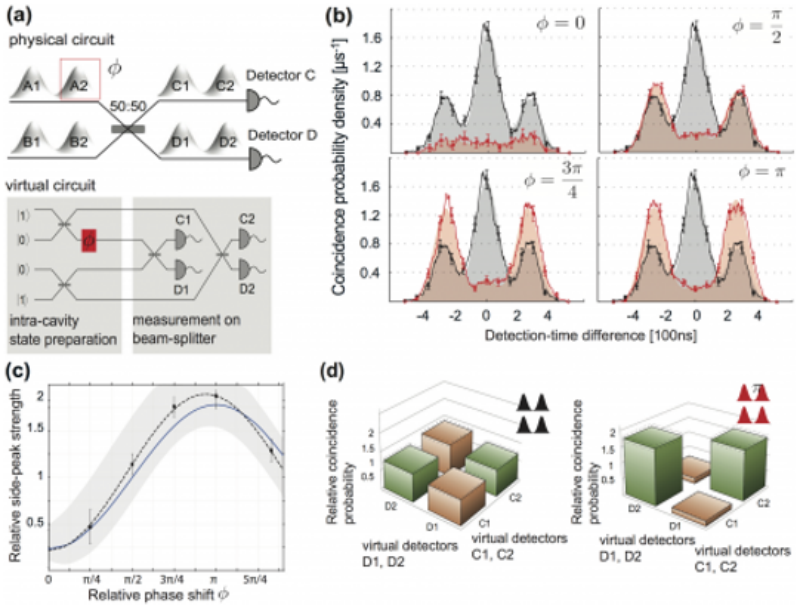


Figure 2.9. *Different qubits' measurement phases. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

2.3.2. *Qutrit*

A qutrit has three orthogonal base states or vectors, often written $|0\rangle$, $|1\rangle$, and $|2\rangle$ in Dirac notation in bra and ket. It is often represented as a linear combination of three states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \qquad [2.3]$$

The coefficients have probability amplitudes whose quadratic sum is equal to one.

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1 \qquad [2.4]$$

Qutrits' base states are orthogonal. The qubits are obtained using Hilbert spaces H_2, corresponding to the up-spin and the down-spin. Qutrits demand a Hilbert space with a higher dimension known as H_3. A chain of n qutrits represents 3^n simultaneously different states.

Qutrits have several particular characteristics when they are used for storing quantum information. For example, they are more robust against decoherence under

certain environmental interactions. In reality, direct manipulation of qutrits could be difficult, and one way of achieving this is to use an entanglement with a qubit.

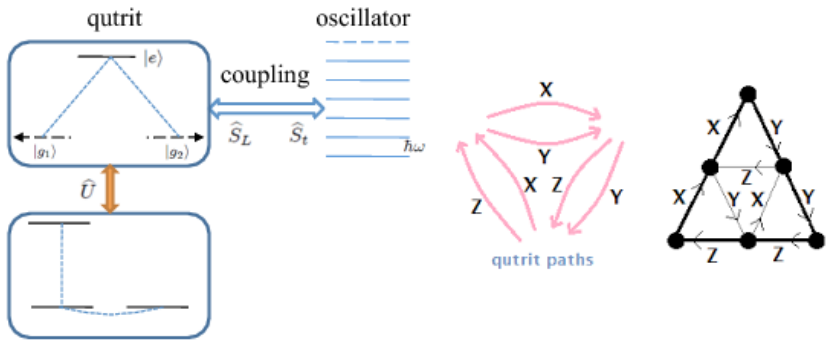


Figure 2.10. *Representation of qutrits*

2.4. Pauli matrices

2.4.1. *Definition*

Pauli matrices form the basis of the SU(2) group Lie algebra. Group SU(2) constitutes a unitary group of degree 2, which is the group of unitary matrices with complex coefficients with the dimensions 2×2 and the determinant 1. The Lie algebra corresponding to SU(2) is written su(2). It is an algebra of complex 2×2 traceless anti-Hermitian matrices, the standard commutator serving as Lie bracket.

Pauli matrices are defined as the set of the following complex matrices with the dimensions 2×2:

$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad [2.5]$$

$$\sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad [2.6]$$

$$\sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad [2.7]$$

These matrices are used in quantum mechanics to represent the particles' spin.

2.4.2. *Properties of these matrices*

$$\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \qquad [2.8]$$

$$ó_1ó_2 = isó_3, \quad ó_3ó_1 = isó_2, \quad ó_2ó_3 = isó_1, \quad ó_isó_j = -ó_isó_j \quad \text{for } i \neq j. \qquad [2.9]$$

$$\begin{aligned} \det(\sigma_i) &= -1 \\ Tr(\sigma_i) &= 0 \\ for\, i &\in \{1;\ 2;\ 3\} \end{aligned} \qquad [2.10]$$

Consequently, the proper values of each matrix are ±1.

Pauli matrices obey the following commutation and anti-commutation relations:

$$\left[\sigma_i, \sigma_j\right] = 2i\epsilon_{ijk}\sigma_k \qquad [2.11]$$

$$\left[\sigma_i, \sigma_j\right] = 2\delta_{ij}.I \qquad [2.12]$$

where ε_{ijk} is the Levi Civita symbol, δ_{ij} is the Kronecker symbol and I the identity matrix.

The previous relationships can be verified using:

$$\sigma_I\, \sigma_j = i\varepsilon_{ijk}\, \sigma_k + \delta_{ij}\, I. \qquad [2.13]$$

These commutative relationships are similar to those of the Lie algebra SU(2). SU(2) can be interpreted as the Lie algebra of all the linear combinations of the imaginary i times the Pauli matrices $ió_i$, otherwise known as traceless anti-Hermitian 2×2 matrices. In this sense, the Pauli matrices generate SU(2). Consequently, $ió_j$ can be seen as the infinitesimal generators of the corresponding Lie group SU(2).

For a rotation vector in three dimensions $\vec{\omega}$ and $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$, the vector composed of Pauli matrices, there is the following relationship:

$$e^{-i\vec{\sigma}\frac{\vec{\omega}}{2}} = I\cos\left(\frac{\omega}{2}\right) - i\ \hat{\omega}\vec{\sigma}\sin\left(\frac{\omega}{2}\right)$$

where ù is the rotation angle (the norm of $\vec{\omega}$) and $\hat{\omega} = \frac{\vec{\omega}}{\omega}$.

The $i\acute{o}_i$ represent the rotation generators on spin ½ particles. The state of these particles is represented by spinors with two components, which is the basic representation of SU(2). An interesting property of spin 1/2 particles is that they must undergo a rotation of π radians in order to return to their original configuration. This is due to the fact that SU(2) and SO(3) are not globally isomorphic, despite the fact that their su(2) and so(3) generators are isomorphic. SU(2) is, in fact, a two-degree overlap of SO(3), to each element of SO(3) there correspond two elements of SU(2).

2.5. Decoherence

Quantum calculation of probability concerns phenomena whose occurrence is suspended when an appropriate context intervenes at the intervention of an appropriate context. The problem is that as a physical theory, quantum mechanics has a vocation for universality. The meta-contextual calculation of probability, which is its main component, should in these conditions be applicable without restriction and at any scale. But, in our familiar environment, isn't classic (Kolmogorovian) probability theory perfectly usable? And doesn't this classic theory function, unlike its quantum equivalent, in such a way that there is no reason not to assume that it expresses a partial ignorance on the subject of intrinsic properties and standalone events? There is therefore a problem with compatibility between the quantum calculation of probabilities, valid in principle on any scale, and the classic calculation of probabilities, valid in practice on our scale. Decoherence theories aim mainly to prove this compatibility. In fact, they enable it to be shown how to apply to them to complex processes involving an object, a measuring device and a vast environment. Quantum probability calculation is reduced to a very weak, close approximation classic probability calculation. This is shown by a near disappearance of typical interference in terms of quantum probability calculation, and isomorphic interference in those of a wave process, in favour of the classic additivity rule for the probability of a disjunction being quasi-valid.

The theory of decoherence was introduced by H. Dieter Zeh in 1970 [ZEH 70]. It was first confirmed experimentally in 1996 [ZUR 05]. [SCH 07] is a clear and very accurate reference work on decoherence.

Quantum decoherence is a theory which is likely to explain the transition between the quantum physical rules and classic physical rules such as we know them, at a macroscopic level. More specifically, this theory provides an answer, considered to be the most complete to date, to the paradox of Schrödinger's cat and to the problem of quantum measurement.

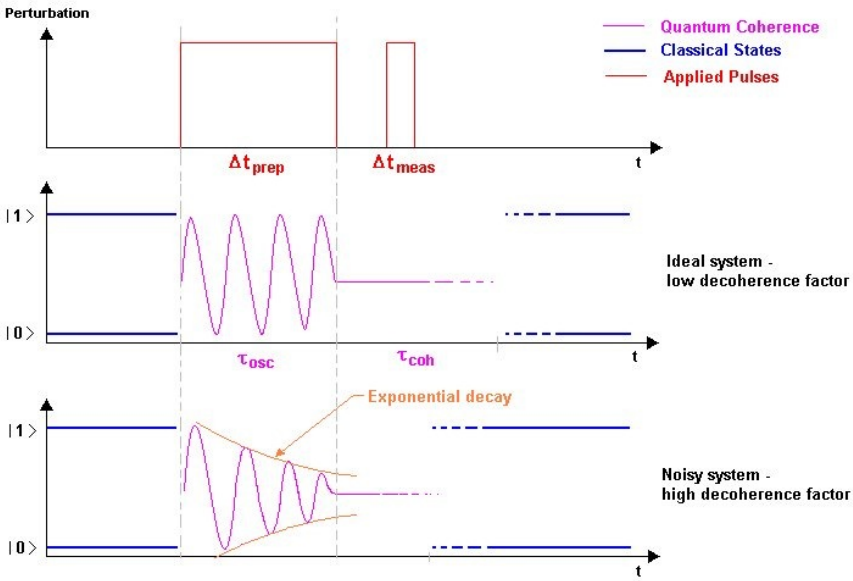


Figure 2.11. *Comparison of decoherence factors. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

Zeh points out that the energy levels in macroscopic systems are so close to one another that even very small fluctuations can affect them. They can therefore never be considered as truly isolated from their environment. The result is that, in what we have called the second point of view during measurement, the large system S should also include this environment. It is therefore necessary to apply Schrödinger's equation to the wave function in the frame S, of the device A and the environment E. This leads after the instant t to an entangled state of the system, the device and the environment. However, during measurement it is enough to observe the system and the device, and the environment can be left aside. The reason for this is, on the one hand, that the environment does not interest us, and on the other hand that we would not be able to measure the sizes attached to its different components. The system and device are therefore separated from their environment. Indeed, quantum mechanics tells us that when we are only interested in a sub-system of a large system, it is possible to obtain its state from the large system's state by carrying out a mathematical operation – which is called "taking the partial trace" – on the overall state. And it is here that Zeh's suggestion reveals its pertinence, since it is possible to show – Zurek was one of the first to do this at the

beginning of the 1980s – that the state thus obtained is identical – subject to some reservations that we will see later on – to that obtained by the principle of reducing the wave packet. The evolutions of the Schrödinger equation and the evolution by the principle of reducing the wave packet can finally be reconciled. Decoherence theory is an enormous advance in resolving the problem of measurement. First of all, the state obtained for the system and the device by using decoherence is not exactly identical to that obtained by applying the principle of reducing wave packets. Decoherence shows us that while the correlations between the different possible states very rapidly become negligible, these correlations do not totally disappear; they simply become too low to be measurable. Moreover, if we are interested in a unique system and not in a group of systems, the state we obtain after decoherence should be interpreted as the fact that the system is in a sort of coexistence, without correlation, of different possible states rather than a single state chosen from among the possible states. This difficulty is named the "or–and" problem by Bell. It is sufficient for us to indicate that these two differences between the states produced by applying decoherence and those produced by applying the principle of reduction show that the answer is not as near as some physicists appear to think.

2.6. Entanglement

Quantum entanglement is a phenomenon observed in quantum mechanics in which the quantum state of two objects should be described as a whole, without one object being separated from the other, although they can be separated spatially. When quantum objects are placed in an entangled state, there are correlations between the physical properties observed in these objects that would not be present if these properties were local. Consequently, even if they were separated by large spatial distances, the two entangled objects O_1 and O_2 are not independent and $\{O_1+O_2\}$ must be considered as a single system.

The phenomenon of entanglement and the EPR paradox have mystified physicists since Einstein, Podolsky and Rozen published their idea in 1935 [EIN 35]. Since then the existence of entanglement has become well-established, both theoretically and experimentally. In fact, quantum entanglement is seen as a cardinal resource in quantum communication. Using quaternions, Singh [SIN 09] studies the geometry of single or two-qubit states of the quantum calculation. Via Hopf fibration [MOS 01], he identifies the geometrical manifestations of separability and two-qubit entanglement. He then introduces the salient features of the EPR experiment and the Bohm version in terms of spins [BOH 52, AHA 59]. Possible schemas of the resolution of the EPR paradox in terms of Bohr's complementarity principle, retroaction time and Bohm's quantum potential are also discussed. The

anomalies resulting from Von Neumann's quantum measurement scheme are also tackled.

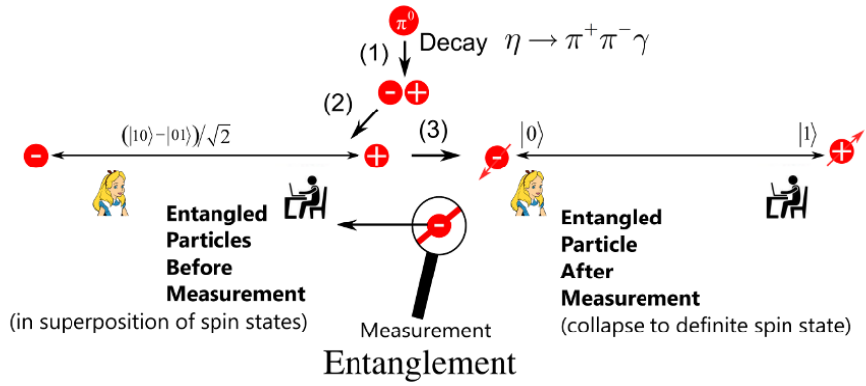


Figure 2.12. *Diagram showing entanglement*

Researchers from ESA have been able to set a new quantum teleportation record by maintaining a state of quantum entanglement between two particles 143 km apart. This major advance opens the way for the possibility of transmitting and encrypting information using the laws of quantum physics.

In conformity with quantum theory, the two particles in question, although apparently separated by a great distance, remain correlated and, in fact, form a common entity. Thereby, any action on one of these particles will instantly have an effect on the other, whatever the distance that separates them and without this phenomenon violating the limit speed of light.

For this new experiment, researchers were able to produce and emit photons (the main constituent of light and the vector of electromagnetic interaction) in opposite directions while maintaining their entangled state and their quantum "coherence" up to the distance of 143 km.

This experiment therefore confirms that it is possible to envisage quantum communications over large distances and researchers from ESA will now attempt to carry out a quantum communication between the earth and a satellite in orbit. But the real issue of these studies is the refinement of a quantum information encryption method.

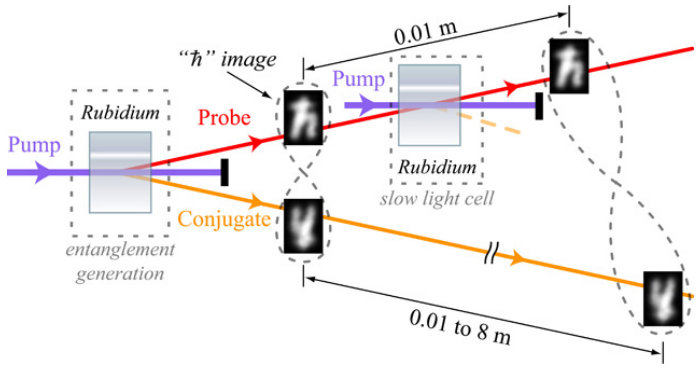


Figure 2.13. *Device for generating entanglement*

3

Quantum Signal Processing

Pitowski has developed a thesis according to which the formalism of the Hilbert space in quantum mechanics is a new probability theory. The theory, like its classic homolog, is made up of an algebra of events and the probability measurements are defined in it. This theory is constructed using the following steps [PIT 89]:

– The algebra of events is introduced by Birkhoff [BIR 31] and Von Neuman [NEU 33]. All the axioms, except the one that expresses the uncertainty principle, are shared with the classic event space. The only models for the set of axioms are networks of subspaces of interior products over a body, K.

– Gleason's theorem [GLE 57] completely characterizes the probability measurements of the algebra of events in such a way that the Born rule is determined.

– Gleason's theorem is a mathematical result, which is of particular importance for the domain of quantum logic. This proves that the Born probability rule of obtaining specific results for a given measurement naturally follows on from the structure formed by the network of events in a real and complex Hilbert space.

GLEASON'S THEOREM.–

We study the origin of the Born probability rule $\rho = |\psi|^2$ in the formulation of a Broglie–Bohm pilot-wave quantum theory. It is argued that quantum probabilities persist dynamically, and have a similar status to ordinary thermal probabilities in statistical mechanics. This is illustrated by digital simulations for two-dimensional systems. We show that a simple initial set, with a nonstandard distribution $\rho \neq |\psi|^2$ of particle positions, evolves toward a quantum distribution with great accuracy. The relaxation process $\rho \rightarrow |\psi|^2$ is quantified in terms of a function, H (equal to less than the relative entropy of ψ according to $|\psi|^2$), which decreases exponentially with respect to time, with a time constant equivalent to the theoretical estimation [VAL 05].

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

In his article, [COL 11] gives us an exact formula for the moments of random quantum channels. The benefit of this study is that an application for the random matrix model has been obtained using a Gaussianization method.

[KUM 98], in his introductory article, presents the fundamental ideas behind quantum probabilities.

[TOL 13] gives us an article that examines the new, fundamental aspects of emergence and information using new approaches in quantum mechanics, whose origin goes back to the Aharonov group. He notes that the most important implication of the Bohm–Aharonov effect is the existence of nonlocal interactions that do not violate causality.

3.1. Wigner distribution

Wigner distribution was introduced by Eugene Wigner in 1932 in the context of quantum physics, to introduce quantum corrections to statistical physics. His aim was to replace the wave function in the Schrödinger equation with a density probability in the phase space [WIG 32].

This function is created by construction at real values. But due to the representation base's redundancy, as expressed by the uncertainty relationships, this function can take negative values. This means that these negative "probability" values are only present on small scales, below h/2π the (Planck constant), when the classic representation in the phase space reaches its limits. The negative values convey the presence of quantum interferences in the phase space.

In a one-dimensional space, for a wave function ψ (x), P(x, p) is written:

$$P(x,p) = \frac{1}{\pi\hbar}\int_{-\infty}^{+\infty} \psi^*(x+y)\psi(x-y)e^{\frac{2ipy}{\hbar}}dy \qquad [3.1]$$

In signal processing, the Wigner distribution is currently used as a quadratic time–frequency representation derived from the notion of autocorrelation. The Wigner distribution linked to a time signal x(t) is written:

$$W(t,f) = \int x(t+\frac{\tau}{2})x^*(t-\frac{\tau}{2})e^{-i2\pi\tau f}d\tau \qquad [3.2]$$

This distribution shows a remarkable property, which is that it can be defined in an equivalent manner to the frequency version of the signal $\hat{x}(f)$, obtained by the Fourier transform (TF):

$$W(t,f) = \int \hat{x}(t+\frac{\eta}{2})\hat{x}^*(t-\frac{\eta}{2})e^{-i2\pi\eta f}\,d\eta \qquad [3.3]$$

This distribution can be interpreted as the signal's power spectral density. However, the phenomena of interference between time and frequency tend to reduce this representation's legibility.

Interferences are often reduced by using a convolution kernel relative to two variables W(t,f)*∠(t,f). It is through this process that the Cohen class is built [COH 89] (quadratic distributions respect the properties of invariance in translation and modulation), a set that includes and generalizes the Wigner distribution.

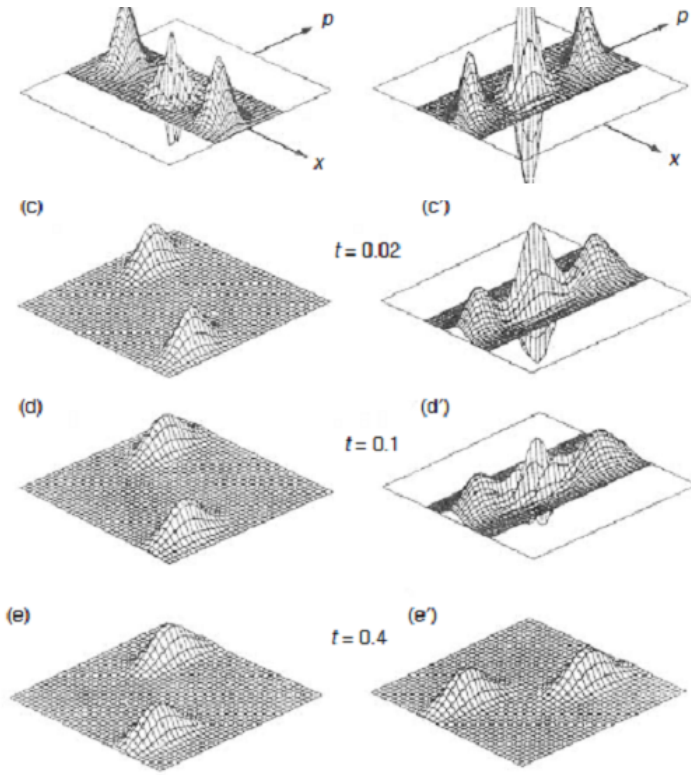


Figure 3.1. *Wigner distributions, and their decoherence for coherent superposition*

3.2. Quantum Fourier transform

Consider a register, comprising n qubits, which evolves in a Hilbert space with N = 2n dimensions. Its state vector is written. As shown by [BEN 04]:

$$|\psi\rangle = \sum_{j=0}^{2^n-1} c_j \lceil j\rangle \qquad [3.4]$$

in the s abridged notation where the 2n base vectors, $|j>$, are ordered according to the binary writing of $|0> = |00..>$ to $|2n\text{-}1> = |111..1>$. On this basis, the state vector is completely characterized by the suite of amplitudes [cj} of length 2n. The state vector's quantum Fourier transform is defined:

$$|\tilde{\psi}\rangle = \sum_{j=0}^{2^n-1} \tilde{c}_k \lceil k\rangle \qquad [3.5]$$

where suite $\{\tilde{c}_k\}$ is the discreet Fourier transform of suite $\{c_j\}$

$$\tilde{c}_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} exp\lfloor 2i\pi \frac{jk}{2^n} \rfloor c_j \qquad [3.6]$$

Here is the operator, F, that transforms $|>$ into $|\tilde{\psi}\rangle$, it is unitary:

$$\hat{F} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \quad \sum_{k=0}^{2^n-1} exp\lfloor 2i\pi \frac{jk}{2^n} \rfloor \; |k\rangle\langle j| \qquad [3.7]$$

$$\rightarrow \hat{F}|\psi\rangle = |\tilde{\psi}\rangle$$

We are interested in the result applying $\hat{F}$ to any of the 2n basis vectors, for example,

$$|\hat{l}> = \frac{1}{\sqrt{2^n}} \left(|0\rangle + exp\left[2i\pi \overline{0.l_n} \,|\, 1\rangle\right] \otimes |0\rangle + exp\left[2i\pi \overline{0.l_{n-1}l_n} \,|\, 1\rangle\right] \right.$$

$$\left. \otimes .. + exp\left[2i\pi \overline{0.l_1 l_2 .. l_n} \,|\, 1\rangle\right] \right) \qquad [3.8]$$

This factorization is essential for a recursive design of the quantum circuit capable of implementing the quantum Fourier transform whatever the number, n, of qubits that make up the registry. The corresponding quantum network uses n Hadamard gates and n(n-1)/2 gates induced under controlled phase-shifts of the type, π/2j (j = 0,1,2,..) (n = 4 in the example shown in Figure 3.2):

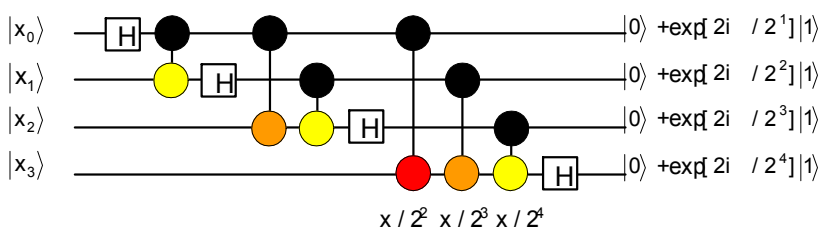


Figure 3.2. *Quantum network corresponding to four Hadamard gates*

Figure 3.3 gives an application of quantum Fourier transform based on shift register.

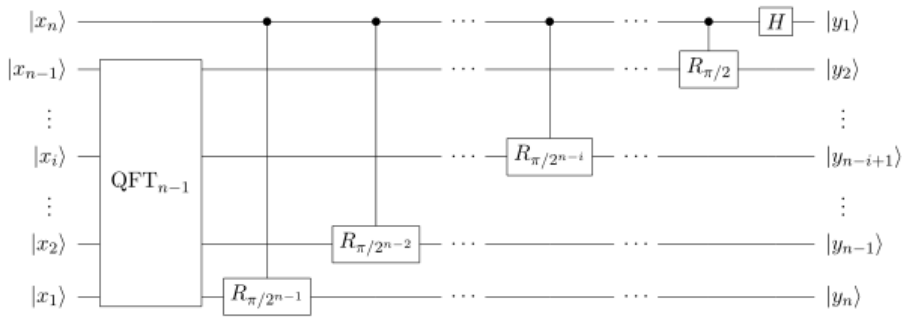


Figure 3.3. *Application of the quantum Fourier transform*

The following figure gives a representation of the spectrum of the quantum Fourier transform.

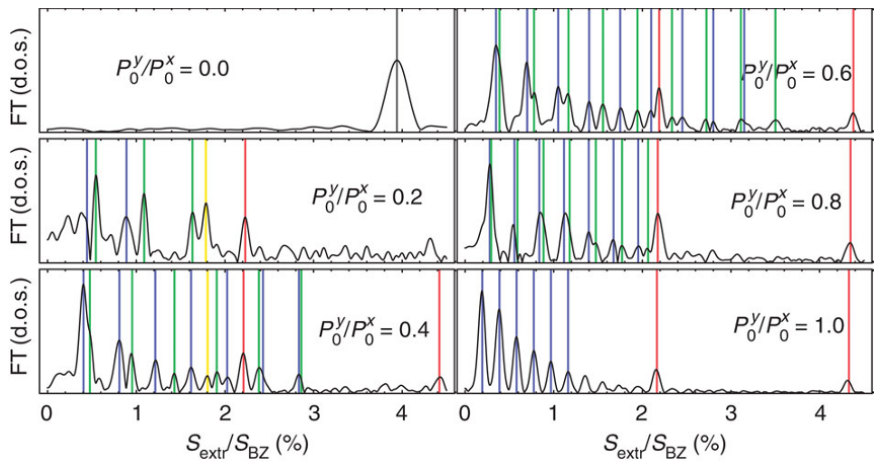


Figure 3.4. *Spectrum representation of the quantum Fourier transform. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

3.3. Gauss sums in a quantum context

Gauss sums occur in many physical phenomena [ANT 12, JON 08]. They are similar to Fourier sums with the clear difference that the index of summation appears in the quadratic phase in a location in a linear manner. Consequently, we study the factorization properties of different Gauss sums, such as the continuous Gauss sum:

$$S(\xi, N) = \sum_{m=-\infty}^{+\infty} \omega_m \, exp\left[2\pi\left(m + \frac{m^2}{N^2}\right)\xi\right] \quad [3.9]$$

We first analyzed this sum in the context of quantum carpets, which show the probability density of a wave packet in a box depending on the time τ and in space. The continuous Gauss sum is produced when we analyze the wave packet's autocorrelation function. Here, the number N that was taken into account is coded in the system's timescales, and the test factor ξ represents the time according to the autocorrelation function. This function's factorization capacities are visible in the following image. Here, the factors of N = 91, such as ξ = 7 or 13 are indicated by Gaussian peaks, whereas for the non-factors the signal does not show particularities.

Other possible physical realizations of this Gauss sum are, for example:

1) Two-photon transitions in a ladder system with multiple levels induced by a pulsed laser pulse.

2) A one-photon transition with pulse compression in an atom at two levels with a periodically modulated excited state.

3) A linearly chirped one-photon transition driven by a sequence of ultrashort pulses.

Another type of Gauss sum is the truncated Gauss sum:

$$A_N^{(M)} = \frac{1}{M+1}\sum_{m=0}^{\infty} exp\left[2\pi i m^2 \frac{N}{L}\right] \quad [3.10]$$

Here N's cylinder and L are exchangers. If l is a factor of N, all the phases are multiples of 2π and therefore all the terms interfere in a constructive manner and the sum is equal to the unity. In all the other cases, the terms interfere in a destructive manner and the signal decreases, as Figure 3.5 shows.

For an upper limit, M, thus selected, the signal for the non-factors is less than $1/\sqrt{2}$. In the interval, several experiments have already successfully shown factorization with the help of a truncated Gauss sum. Many different physical

systems have been used for these experiments, such as cold atoms, Bose–Einstein condensates, ultrashort laser pulses and classical light.

Moreover, we are interested in the combination of entanglement and Gauss sum factorization. We hope to generate a velocity in this way.

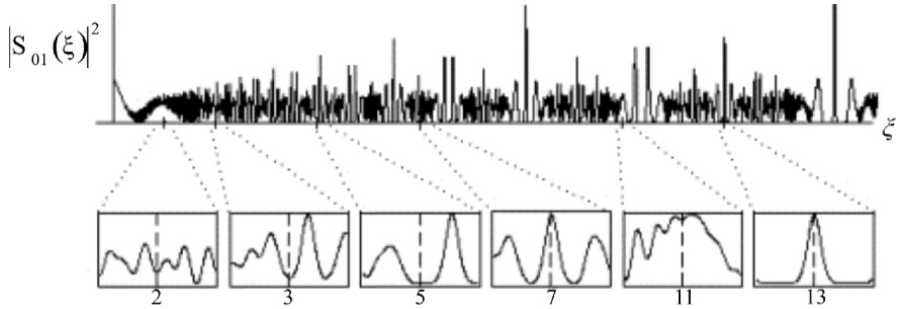


Figure 3.5. *Representation of Gauss sums in a quantum example*

3.4. Geometry for quantum processing

Heisenberg's view is the following: physical quantities in quantum mechanics can only be processed with a non-commutative algebra. This leads us, according to Alain Connes, to envisage that quantum mechanics can only be understood, from a geometrical point of view, via a non-commutative geometry. Until the discovery of quantum mechanics in 1925, classic geometry was based on duality, proposed by Descartes, and the introduction of Cartesian coordinates, between geometry and commutative algebra. Commutative algebra, which we have all learnt at school, is an algebra in which the product of two algebraic quantities does not depend on the order of terms, that is to say that A times B is equal to B times A.

With the discovery of quantum mechanics by Heisenberg, the geometric space of the states in a microscopic system, an atom for example, is enriched with new properties by its coordinates, such as the moment and position, which no longer commute. The aim of non-commutative geometry is to generalize the duality between geometric space and algebra in the more usual instance, where the algebra is no longer commutative. This leads to two fundamental mathematical concepts being modified, those of space and symmetry, and to the set of mathematical tools being adapted to these new paradigms, including calculus and cohomology. Far from being a simple generalization, the theory's initial benefit arises from entirely

new and unexpected phenomena that have no counterpart in the "classic" commutative instance.

The first of these phenomena is the natural appearance of "time" from noncommutativity. This is a key result of Alain Connes's work, which enabled him to provide a classification of operator algebras (Von Neumann algebras). Classic (commutative) Riemannian geometry, which arose from the discovery in the 19th Century of non-Euclidian geometry and provides a framework for Einstein's general relativity, has thus been generalized in the "quantum" context. The key notions of measuring distances and curvature are understood in a noncommutative context but acquire a new meaning. In fact, the transition from measuring distances in Riemannian geometry to measuring distances in noncommutative geometry is an accurate reflection of the evolution of the definition of the meter in the metric system (1960). The original definition of the meter, around the end of the 18th Century, was based on the "mètre des archives" defined as a fraction (1/40,000,000) of the greatest length that can be measured directly, namely the earth's circumference. A radical change occurred in 1960: the meter was redefined as a multiple of the wavelength of an orange spectral ray of krypton isotope 86. More recently, in 1983, the definition currently in use was reached; it uses the spectrum of a cesium atom and is expressed in a unit of time using the speed of light as a conversion factor to link time and length. The transition from Riemann geometry to non-commutative geometry is an exact parallel of the evolution of the yardstick, above. The measurement of distances uses operator algebra. A notion of geometric space, of spectral nature, with very great flexibility, is thus obtained.

Noncommutative geometry is used for spaces with noninteger dimensions, spaces with finite dimensions, and above all, "quantum" type spaces, and finally space–time itself if we take account not only of the electromagnetic force (which led Poincaré, Einstein and Minkowski to their space–time model) but also weak and strong forces that lead to a non-commutative space–time model. In the general theory of noncommutative spaces, the notion of point is replaced by that of the "state" of the system, which, in part, plays the role of a "points cloud" and which is of "quantum" type. Nevertheless, the measurement of distances, thanks to its spectral formulation, continues to have a direction and is reduced to the length of the shortest path between two points in the classic instance. This new geometry extends classic Riemann geometry, but each of the classic notions acquires a new meaning. For example, the curvature of a space, which plays an essential role in the formulation of Einstein's equations of general relativity, continues to have a purpose but becomes, for a four dimensional space, the calculation of this space's surface. In particular, this enables the theory that pairs Einstein's gravitation with the standard model of elementary particles to be reformulated in a very simple and purely geometrical fashion.

Alain Connes has recently worked on understanding of “renormalization”. In the first instance, in collaboration with D. Kreimer, he linked the “slight of hand” used by physicists to eliminate infinite quantities to Hilbert’s 21st problem. In fact, more recently, in collaboration with M. Marcolli, A. Connes has discovered the significance of the Riemann–Hilbert correspondence involved in this physical problem and this led them to identify a symmetry group that had been “guessed at” by P. Cartier under the name “cosmic Galois group”. This established an entirely unexpected link between Galois’s theory, in its most sophisticated form, and the area of quantum physics which is best tested by experimentation.

4

Quantum Circuits

4.1. Reversible logic

Unlike classical circuits, which are, banally, totally irreversible, quantum circuits can be reversible in so far that the initial state can be determined from the final state.

The reasoning always begins from the space of the states, which is a purely quantum space. In fact, classical logic always assumes that an event is true or false, and that there is no third option, i.e we have 1 for a true event and 0 for a false event. In the quantum domain, intermediary states can exist; they appear on a Bloch sphere. There is a more exhaustive explanation in [JAY14].

4.1.1. *Physical reversibility*

The known physical laws are reversible. This is also the case for classical mechanics, based on the Lagrangian/Hamiltonian dynamic, and for standard quantum mechanics, in which closed systems evolve according to unitary transformations, which are bijective and reversible. Consequently, when a physical system carries out an irreversible calculation, correspondence with the calculation model indicates that the system cannot remain closed. More precisely, since an irreversible calculation reduces the space of information-bearing physical state space, their entropy should decrease, while increasing the entropy of states that do not carry information, representing the thermal part of the system.

In 1961, Landauer studied this thermodynamic argument [LAN 61], and suggested the following principle: if a physical system carries out a classic, logically irreversible calculation, it should increase the entropy of the environment with a

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

minimum quantity of heat released of kT × ln(2) per bit lost (where k is the Boltzmann constant and T the temperature, that is to say around 3×10^{-21} J at ambient temperature), which emphasizes two facts:

– a calculation's logical irreversibility involves the physical irreversibility of the system that carries it out (the information is physical');

– logically reversible calculations can, at least in principle, be intrinsically nondissipative (which is in relation with Carnot's theorem on thermal motors, showing that the most efficient motors are reversible, and Clausius's theorem, attributing a null change of entropy to reversible processes).

4.2. Reversible circuits

Landauer also remarked that any irreversible calculation can be transformed into a reversible calculation by including it in a more extensive calculation in which no information is lost, in other words by reproducing each output in the input (adding sources) and each input in the output (adding wells) [LAN 61].

The additional bits of information, like Ariadne's thread, ensure that it is possible to reverse the calculation course: they are the excess from the entrance and the program from the exit. Rather than losing them in the environment, they are maintained in the calculation's controlled space.

The Toffoli gates are reversible and universal primitive functions, which mean that any reversible function can be constructed in terms of Toffoli gates. The Fredkin gate is another example of a reversible and universal primitive. It exchanges both its inputs according to the state of a third, control input, thus enabling any calculation to be incorporated in a vectoring transporting the conserved signals.

4.2.1. *Reversible calculation models*

The ballistic model invented by Fredkin and Toffoli was one of the first calculation models to aim for implementation with reversible physical components. Based on the laws of classical mechanics, it is equivalent to the formalism of the kinetic theory of perfect gases. The presence of rigid spheres in movement at specified points is defined as 1 and their absence as 0. Interactions by collisions at right angles enable the construction of different primitive functions, such as for example the universal gate at two inputs and three sorties introduced by Feynman, who, with Ressler, also suggested a ballistic version of the Fredkin gate.

In practice, a calculation carried out by these spheres would be very unreliable, as the instability resulting from the smallest disturbances would rapidly generate chaotic gaps, producing an output saturated with errors. The errors can be corrected (for example, by adding potentials to stabilize the paths), nonetheless, the process of correcting is itself irreversible and dissipative – as it should delete the erroneous information. Consequently, correcting errors seems to be the only aspect of calculation that defines a limit lower than the dissipation of energy.

The inclusion method is, however, insufficient for constructing a physically reversible universal computer, as the increasing quantity of information that would need to be reproduced for each event would saturate any finite memory. Then, the calculation would end – unless the memory was irreversibly erased, but then the dissipation would simply be postponed, and not canceled.

This seemed to exclude the possibility of constructing reversible computers, until Bennett [BEN 92] found a remarkable solution, demonstrating that it is possible, at least in principle, to carry out an unlimited number of calculations without any dissipation of energy.

The reversible system should calculate the inclusive function twice: the first time beforehand to obtain and save the result of the calculation and the second time afterward, as a mirror-image calculation of the reverse function, de-calculating the first step and returning the closed system to its initial state.

4.2.2. *Reversibility in quantum calculation*

Quantum calculation benefits from the physical effects of superposition and entanglement, which leads to a qualitatively new calculation paradigm. In quantum calculation models, all events occur through unitary transformations, thus, all the quantum logic gates are reversible.

Quantum systems are less sensitive to some types of error that affect classical calculations, as their discreet spectrum prevents chaotic trajectories. For example, a quantum ballistic model is more reliable than its classical counterpart.

However, quantum systems are affected by new sources of error, a consequence of interactions with the environment, such as the loss of quantum coherence. It is possible to correct generic quantum errors up to a limit by reconstructing a quantum state exempt from error, at the cost of carrying out an irreversible quantum deletion of the erroneous quantum information [CAL 92].

4.3. Quantum gates

4.3.1. *Hadamard gate*

The Hadamard gate is a gate acting on a single qubit that carries out the following transformation:

$$|0> \rightarrow \frac{(|0>+|1>)}{\sqrt{2}} \qquad [4.1]$$

$$|1> \rightarrow \frac{(|0>-|1>)}{\sqrt{2}} \qquad [4.2]$$

Its schematic representation is shown in Figure 4.1.

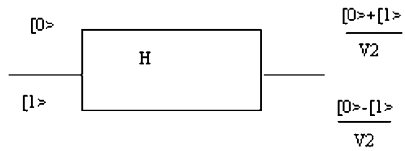


Figure 4.1. *Diagram of a Hadamard gate*

From a qubit in state |0>, a superposition with weight equal to states |0> and |1> is then prepared. In a case where the qubit is a ½ spin, the Hadamard transformation is obtained by a combination of rotations. Figure 4.2 shows the diagram of a Hadamard gate according to Bloch sphere.

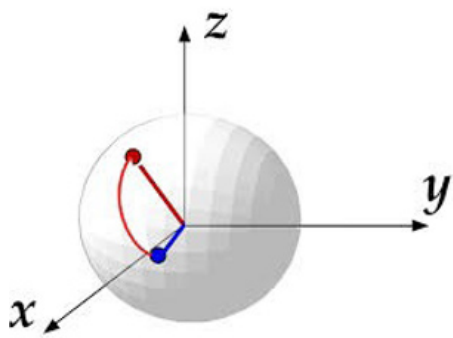


Figure 4.2. *Diagram of a Hadamard gate by a Bloch sphere*

4.3.2. *Pauli-X gate*

The Pauli-X gates acts on a single qubit. It is the quantum equivalent of a NON gate. It corresponds to a rotation of the Bloch sphere around the X axis. It is sometimes called a bit-flip.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad [4.3]$$

Its schematic representation is shown in Figure 4.3:

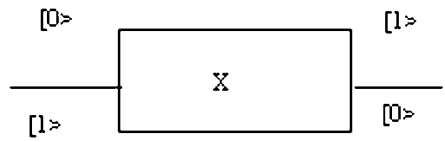


Figure 4.3. *Diagram of a Pauli-X gate*

4.3.3. *Pauli-Y gate*

The Pauli-Y gate acts on a single qubit. It corresponds to a rotation around the Y axis of the Bloch sphere.

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad [4.4]$$

Its schematic is shown in Figure 4.4.

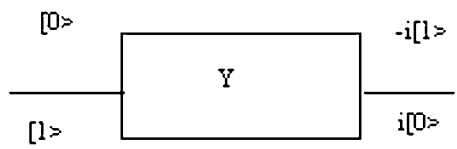


Figure 4.4. *Diagram of a Pauli-Y gate*

4.3.4. *Pauli-Z gate*

The Pauli-Z gate acts on a single qubit. It corresponds to a rotation around the Z axis of the Bloch sphere.

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad [4.5]$$

Its schematic representation is shown in Figure 4.5 and the diagram is done according to the Bloch sphere.

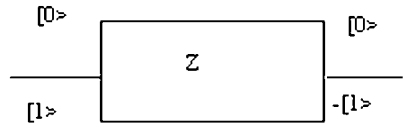


Figure 4.5. *Diagram of a Pauli-Z gate*

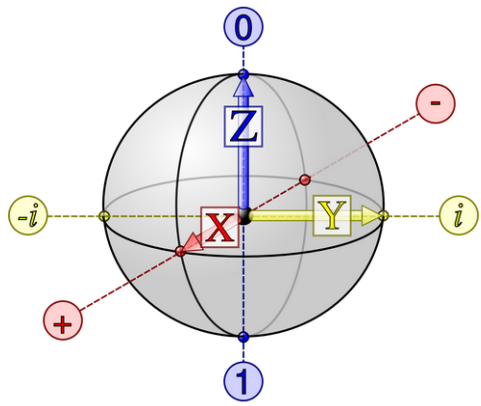


Figure 4.6. *Representation of a Pauli gate by a Bloch sphere*

4.3.5. *Swap gate*

The Swap gate switches two qubits. It enables qubits to be exchanged in a circuit. It is defined in the computational base by:

$$SWAP|x, y >= |y, x > \quad [4.6]$$

It is a unitary operation; it can be carried out thanks to the Heisenberg Hamiltonian with:

$$H = \frac{h}{2\pi} J \vec{\sigma}_1 \vec{\sigma}_2 \qquad [4.7]$$

The σ correspond to the Pauli matrixes.

4.4. Toffoli gate

The Toffoli gate, also called a CCNOT gate, is a grid with 3 bits, which is universal for the classical calculation. Any reversible circuit can be constructed from the Toffoli gate; it acts as NON gate with dual control. The quantum Toffoli gate is defined for 3 qubits. If the first two bits are in state 1, it applies a Pauli-X on the third bit, if not it does nothing. Given that it is the quantum analog of a classic gate, it is completely defined by the truth table (Table 4.1).

INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Table 4.1. *Truth table of Toffoli gate*

The reversible Toffoli gate can implement all the Boolean functions. This gate has a direct quantum equivalent showing that the quantum circuits can carry out all the operations carried out by classical circuits. The quantum logic gates are represented by unitary matrixes (see Pauli matrixes). Figure 4.7 represents the Toffoli gate, and Figure 4.8 the same gate with a coding process.

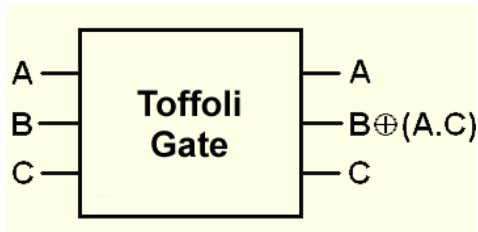


Figure 4.7. *Diagram of a Toffoli gate*

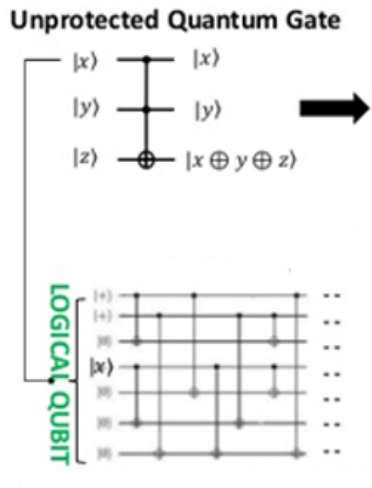


Figure 4.8. *Representation of a Toffoli gate in the case of protection by coding*

4.5. Deutsch gate

The Deutsch gate is a quantum gate that is based on the idea of a Toffoli gate. It is a gate with three inputs in which the two high inputs control the action of the lower line. But this time, the action is not a change-over. Rather, it is a spin rotation; it has a rotation angle θ around the X axis. Figure 4.9 shows a schematic representation of the Deutch gate.

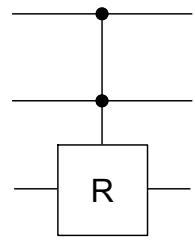


Figure 4.9. *Diagram of a Deutsch gate*

Operation R is given by the formula:

$$R = -ie^{i\left(\frac{\theta}{2}\right)\sigma_x} = -i\left(\cos\frac{\theta}{2} + i\sigma_x \sin\frac{\theta}{2}\right) \quad [4.8]$$

Furthermore, we assume that angle θ is incommensurable with π, that is to say that it is not a rational fraction of π.

The Deutsch gate possesses the following property:

θ is not a rational fraction of π. If R takes a qubit |s>, it will end by reaching the value $e^{i\lambda\sigma x}|s>$.

4.6. Quantum dots

A quantum dot (QD) is a semiconductor nanostructure. Due to its size and characteristics, it acts as a potential well that holds the electrons (and the holes) in the three dimensions of space, in a region of a size in the order of the electrons' wave length (de Broglie wave length), which is some tens of nanometers in a semiconductor. This containment gives the quantum dots properties similar to those of an atom, which is why quantum dots are sometimes called "artificial atoms".

Quantum dots were discovered in part by chance by the Russian researcher Alexei Ekimov at the end of the 1970s in the Optical Institute in Leningrad. While he was studying different possible alloys for microelectronics, he highlighted the astonishing optical properties of minuscule crystals of cadmium selenide. In 1985, the researcher published a scientific article that would then form the foundation for quantum dots [EKI 85]. Concretely, the quantum box is a crystalline structure of cadmium selenide measuring tens of nanometers (a billionth of a meter) whose electrons are excited by light. This crystal, formed of only a few atoms shows quantum behavior and so emits a fluorescent light whose wavelength varies

according to its size. With a diameter of 2 nm, it thus emits a blue light, whereas it will be red with a diameter of 6 nm. Other parameters influence fluorescence, such as the dot's composition and shape.

Quantum dots are solid material structures of very small size, endowed with remarkable properties, essentially because of this small size. Their dimensions are measured in nanometers, that is to say in billionths of a meter and they contain a small number of atoms in the range of a hundred to a hundred thousand. QDs can have more or less complex structures. The most simple are just nanocrystals, that is to say a regular grouping of atoms arranged in precise geometric patterns, like ordinary crystals, but with much reduced dimensions. The most studied materials are semiconductors, in particular cadmium-based compounds, such as cadmium selenide.

The laws of physics mean that these reduced dimensions profoundly modify the behavior of the electrons gravitating around these atoms' nuclei. Their confinement imposes new rules of play that result in very interesting, unstudied electric and optical properties. Researchers explain that in some ways, a QD behaves like a large, artificial atom. Quantum dots have shown exceptional properties.

QDs' most studied and used property is their fluorescence. The scientific community has discovered that a quantum dot, excited by an incident light, emits light on a very precise frequency that depends only on its size. As it has been possible to control the size of QDs since 1993, researchers have begun to produce, at will, QDs that emit light of any color, from ultraviolet to near and far infrared, passing, obviously, through the visible spectrum. A more complex form of QD carries, in addition to a nanocrystal, a "shell" made up of a second material, which in some way protects and so reinforces the properties of the "core" that it contains. Molecules can still be attached to this shell, generally carbon chains called "ligands", which, notably, enable the QD to be attached to certain sites.

From the simple nanocrystal, research has thus led to the functionalized quantum dot, capable especially of fixing itself on cells that show certain characteristics, for example cancerous cells, and enabling them to be located, thanks to their fluorescence. Other work has also enabled the shape of QDs to be controlled. Teams have thus published solutions for making cylinders, tetrapods and platelets. These new shapes give these QDs unforeseen properties. The first QDs were essentially created from compounds of cadmium, a heavy metal, thus requiring precautions. Many studies have successively shown that it is possible to use other materials, including less harmful and more common chemical elements (Figures 4.10(a) and (b)).

It is still possible to add a great deal to the list of applications for quantum dots. New lasers have come to light in this way. New light sensors, based on QDs, should also find multiple uses. But much greater shifts are possible. Thus, some imagine that a new era in electronics may open up. At the very moment when the electronic industry has pushed the miniaturization of chips so far that some devices no longer function according to the usual laws, it could acquire a new lease of life with these minuscule QDs endowed with useful properties.

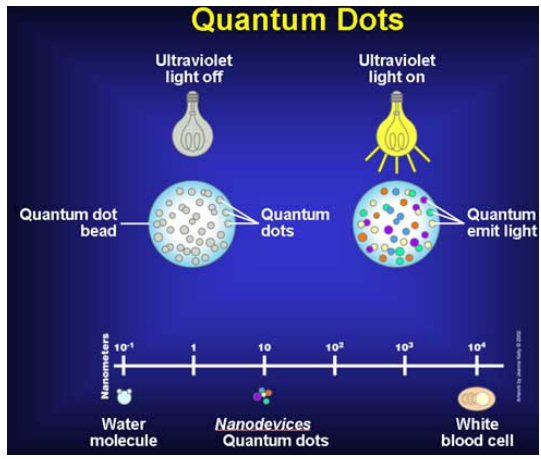


Figure 4.10(a). *Representation of quantum dots and comparison with other structures*

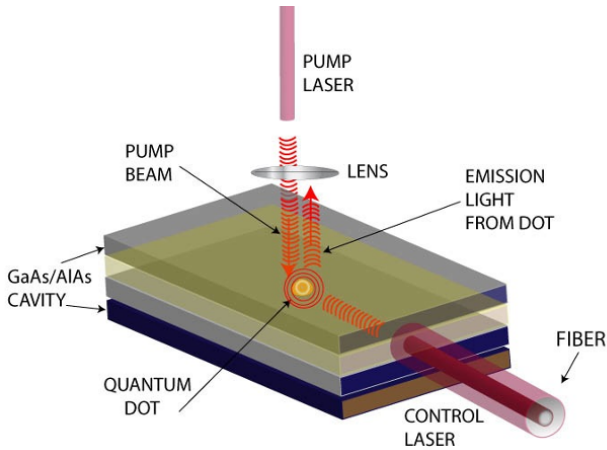


Figure 4.10(b). *Positioning of quantum dots on semiconductor components*

4.7. QCA

In quantum calculation, the quantum finite automaton or quantum state machine is the quantum analogue of the probabilistic automaton or Markov decision process. It is linked to the quantum computer in a similar way to the finite automaton, which is linked to the Turing machine. Many types of automata can be defined, including the measurement of one or many automata. A quantum finite automaton can be understood as the quantization of finite sub-offsets or as a quantization of Markov chains. The study of quantum languages for these automata remains a very active research domain.

To understand quantum finite automata, we can begin with a theoretical interpretation of a deterministic finite automaton that can be represented as a directed graph, with the states shown as nodes in the graph, and arrows representing the state transitions.

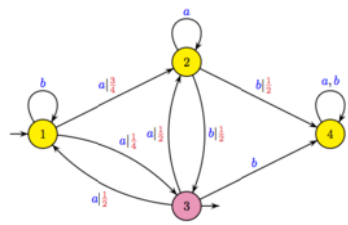


Figure 4.11. *Representation of a quantum simplified automaton*

5

Optical Fibers and Solitons

5.1. Introduction

It is currently very attractive to transmit information over long distances using optical fibers, on account of the large volumes of information that such systems can handle. However, it has not been possible to remove dispersions completely. Dispersions cause the pulse intrinsic to the fiber to broaden, leading to a reduction in the transmission's agility. Consequently, they constitute a brake on the propagation of a substantial data stream (10 megabits); several methods have been developed to obtain performances in the order of 10 gigabits and to decrease the dispersion rate, including among others the single-mode fiber. In this work, it was initially thought to include the nonlinearities resulting from the Kerr effect to increase the data stream; this path reaches saturation thresholds, which has driven researchers toward new directions for optimization.

Theoretical physics has put forward a solution likely to resolve the problem, the new concept being the soliton defined as follows: a soliton is a solitary wave, a solution to some evolution of nonlinear and dispersive differential equations. The soliton emerges from collision with a similar solitary wave, without changing shape or velocity. This chapter will focus on developing an analysis of soliton propagation in nonlinear optical fibers. The interest of this study lies in modeling propagation phenomena; this is examined in a nonlinear instance, which is the only possibility likely to enable us to obtain solitons. We will study soliton propagation in a single-mode fiber, the effect of losses in this fiber, instability in modulation, the amplification of solitons and random variation in the fiber's parameters. The chapter will be divided into four sections.

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

The first section will outline optical fibers, their structure and the effects of loss and dispersion on them. The second section tackles different nonlinear equations. Particular attention is paid to equations that give soliton solutions. The difference between the equations and their structure is analyzed. The third section concerns nonlinear propagation in an optical fiber. To do this, we highlight two characteristics: dispersion and non-linearity, whose conjugation following a careful balance conditions the soliton's appearance. Oscillation and autofocalization are then reviewed. The fourth section tackles both results and interpretation. The physical mechanism for forming solitons is analyzed, before the different methods of increasing solitons' size and studying the benefit of modulation instability in the formation of soliton streams are undertaken. At the same time, we show the benefit of quantum communications.

Typically, an optical fiber can support a large transmission band (0.1–1,000 GHz) with low loss per unit of length (0.15–5 dB/km) and can tolerate electromagnetic interference. Thus 0.1% of the carrier's frequency can produce a bandwidth higher than 1,000 GHz.

Because optical fibers that propagate in a single mode are promising avenues of transmission for the future of long-distance, high-capacity communications [MAL 10, TUR 12], there are many reasons to study such fibers' propagation characteristics.

5.2. Optical fibers

Optical fibers are dielectric wave guides designed to guide light waves along their length. Generally, an optical fiber consists of a cylindrical core with the refraction index n_1 surrounded by an index sheath n_2, with $n_1 < n_2$. If n_1 and n_2 are both uniform across a section, the fiber is called a step-index, but if n_1 varies with the core's radius, it is called a gradient index. Additionally, if the core's diameter is small, the fiber is single-mode; if the core's radius exceeds 10, it is often a multi-mode fiber. If $n_1 > n_2$, the light source penetrates the fiber at an angle close to its axis, and the light waves will be confined to the fiber's core.

Of course, like any other means of transmission, the optical fiber suffers losses of power and signal dissipation along its course of propagation; and it is the extremely low losses, and the possibility of there being a zero-dispersion point at certain wavelengths, that has led to optical fibers being adopted to replace previously extant transmission systems.

Commercial communication systems using optical fibers operating at $0.8 < \lambda < 0.9$ μm are the first generation; those of the second generation operate at $\lambda \approx 1.3$ μm, to benefit from the advantage of low losses of fiber, and the zero-dispersion point. These systems use single-mode fibers with conventional lasers as a light source.

For telecommunication systems with optical fiber, the trend for the future is to use $\lambda \approx 1.55$ μm, to take full advantage of the ultra-low losses at this wavelength; this is the third generation, where the fiber is used for broadband or high-speed applications [WAN 13b].

5.2.1. *The fiber's parameters*

So the fiber consists, as we have just seen, of an index core n_1 slightly higher than n_2, the cladding index, and the boundary between the core and the cladding can be sudden or gradual; generally, the optical fibers are of two types: single-mode fibers and multimode fibers. In our work, we are interested in the characteristics of the single-mode fiber.

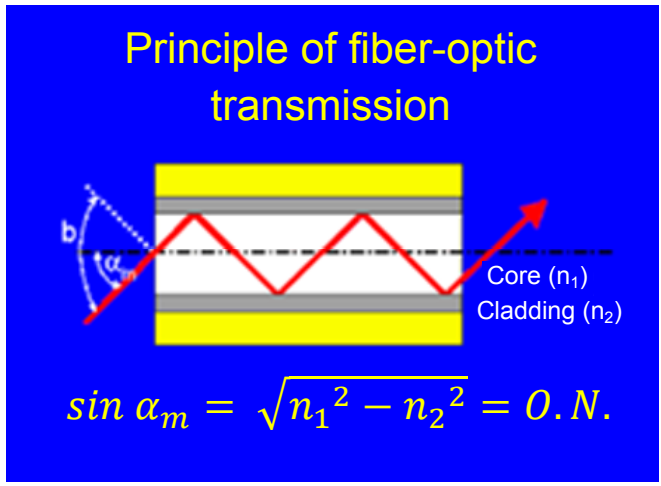


Figure 5.1. *Principle of fiber-optic transmission. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

The single-mode fiber's core has a smaller diameter and can only support a single propagation mode, it obeys two mutual orthogonal polarizations, and is always a step index fiber.

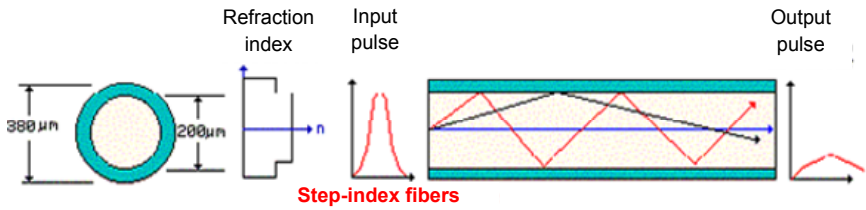


Figure 5.2. *Characteristics of step index fiber*

There are other varieties of optical fiber, among them, we highlight fibers with gradient index and single-mode fibers. Figure 5.3 gives a summary of these fibers.

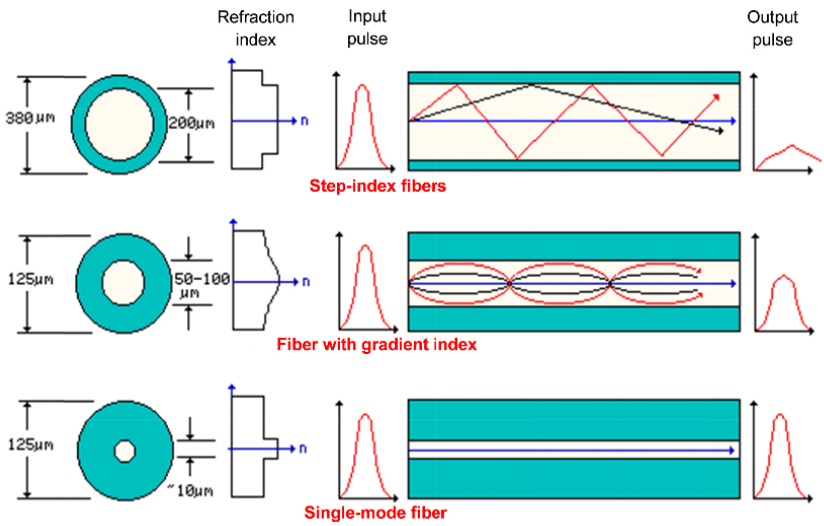


Figure 5.3. *Different varieties of optical fibers*

To define the fiber more precisely, we define some parameters:

Consider n_1 and n_2, the respective indexes of the core and the cladding, a new parameter Δ is defined:

$$\Delta = \frac{n_1^2 - n_2^2}{2n_1^2} \cong \frac{n_1 - n_2}{n_1} \qquad [5.1]$$

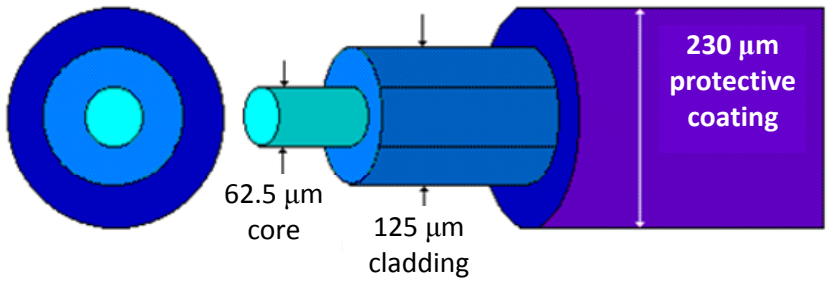


Figure 5.4. *Representation of the optical fiber's core and cladding*

Δ is the relative difference between n_1 and n_2, for the light wave guides $\Delta << 1$, typically $\Delta = 0.002$ for a single-mode fiber.

A second term V is then defined:

$$V = \frac{2\pi}{\lambda}\sqrt{\left(n_1^2 - n_2^2\right)} = \frac{2\pi a}{\lambda}\sqrt{2\Delta} \qquad [5.2]$$

where 2a is the core's diameter, λ the wave length of the direct beam from the light source and V the fiber's normalized frequency.

If we borrow a term frequently used in optical geometry, the numerical aperture (NA), we have [GHA 12]:

$$V = \frac{2\pi a}{\lambda} NA$$

$$V = \frac{2\pi a}{\lambda} NA \qquad [5.3]$$

The equations [5.2] and [5.3] define V, the fiber's key parameter, according to the value of V. We can define the type of fiber core, and it also enables us to class the fibers precisely; for $V < 2.405$, the fiber is single-mode.

The magic number 2.405 is the first zero of the Bessel function ($J_o(X) = 0$ to $X = 2.405$).

The single-mode property is created by decreasing the diameter of the core and the difference Δ for $V < 2.405$.

To design the single-mode optical fiber, it is vital to know the cut-off wavelength $\lambda_c = \frac{\lambda V}{2.405}$ of the highest proper mode and to operate at $\leq_c$ in the optical fiber. The core's diameter λ_c c is directly proportional to the wavelength, if λ increases, ϕ_c increases.

5.2.2. *Birefringence in optical fibers*

An important parameter characterizing optical fibers is the refraction index. The propagation of light in the medium should have propagation constants which vary in different directions. If n_x and n_y are refraction indexes in directions x and y respectively, then the propagation constants in directions x and y are β_x and β_y, the difference $\beta_x - \beta_y$ is a measurement of the medium's birefringence.

5.2.3. *Dispersion in optical fibers*

In communications systems, dispersion is classed in two categories: intermodal dispersion and intramodal dispersion. We will limit ourselves to the latter when discussing dispersion in single-mode fibers.

5.2.3.1. *Intramodal dispersion*

It consists of two dispersions, one specific to the material and the other relating to the wave guide.

5.2.3.1.1. Material dispersion

If the refraction index of the fiber's material varies with the wavelength, involving a variation in the group's speed, it is classed as dispersion of the material; the question we ask ourselves is how the refraction index in the fiber becomes dependent on the wavelength?

The interaction of resonances from the electromagnetic wave field with the electrons at the material's surface contributes to a loss of absorption in the fiber, as the particles' elasticity at their limits tends to oscillate at typical frequencies, the interaction between the light wave and the surface electrons becomes dependent on the frequency, which in turn makes the material refraction index a mirror, and by the same material dispersion, dependent on the frequency [GHA 12].

5.2.3.1.2. Waveguide dispersion

The dispersion of the waveguide is the result of dependence on the propagation characteristic β, obtained by resolving the eigenvalue equation of the particular

mode propagating in the fiber. The exact solution is very difficult to obtain, however introducing the new expression β in an approximate fashion makes it possible to calculate the parameter.

5.2.3.2. *Zero dispersion point*

The zero dispersion point occurs when:

$$\frac{d^2n}{d\lambda^2} = 0$$

For a pure silica glass fiber this point reaches 1.27 μm, since V is given by the expression:

$$V = \frac{2.405\lambda_c}{\lambda}$$

For a single-mode fiber made from pure silica at λ = 1.18 μm, the point where the dispersion is null corresponds to V = 2.2.

In general, from experimental observations [GHA 12] it appears that for the mode LP11 beyond λ > 1.2 μm, the dispersions of the material and the waveguide possess opposing signs and consequently, it is possible for this purpose that they cancel one another out and create a zero chromatic dispersion in the fiber within a certain range of wavelengths.

5.2.3.3. *Measuring dispersions*

There are two methods for measuring the dispersion characteristic in the optical fibers.

5.2.3.3.1. Measurements in the time domain

Optical pulses are emitted at the fiber's transmitting end and the output is connected at the receiving end, where the delay or spread of a short pulse is observed and the data are used to calculate the dispersion properties.

5.2.3.3.2. Measurements in the frequency domain

A light source's output is modulated in size by a sinusoidal sweep signal and sent to the very end of the fiber's transmission; at the very end of the receiver, the baseband frequency response, which is the response in terms of frequency modulation, is connected; the dispersion is therefore expressed in terms of the size of the fiber's band.

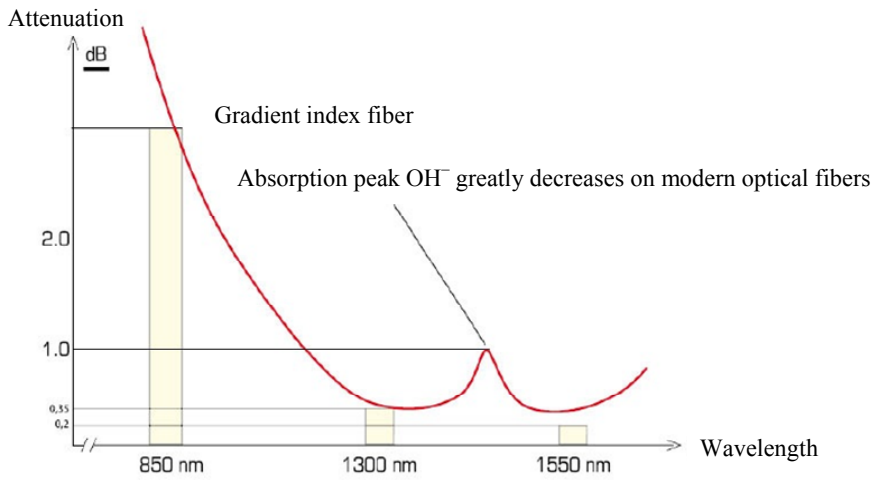


Figure 5.5. *Representation of attenuation in a fiber*

5.3. Soliton solutions for differential equations

5.3.1. *Introduction*

The soliton is a relatively recent discovery in theoretical physics and it has now become much more of an intuitive concept than a strictly mathematical idea. It would be sensible to introduce the concept of the soliton by examining the non-linear Schrödinger equation known to possess soliton solutions.

The latter is often present in problems in nonlinear optics. It can be used in general to describe the weakly nonlinear, almost monochromatic wave propagation (i.e. the wave packet) in a dispersive medium [ABL 11]. This equation's fundamental characteristic is that its solutions are wave packets, i.e. the envelope of a rapidly varying signal variant is the solitary wave; this is in contrast to the previous equations, which are low bandwidth signals (they contain a non-null component).

The latter equation is a generalization of the first two; this combines a weak nonlinearity with an arbitrary dispersion relation [ABL 91]. Note that in an appropriate limit, this equation can be reduced to the nonlinear Schrodinger equation, which leads to the possibility of a soliton envelope.

5.3.2. *Nonlinear Schrodinger equation*

The non-linear Schrodinger equation (NLSE) is defined as follows:

$$i\Psi t + i\varpi '0\psi x + \frac{1}{2}\varpi_0^{"}\psi_{xx} + q\left|\psi^2\right|\psi = 0 \qquad [5.4]$$

The name NLSE comes from the similarity of the linear part of the equation [5.4] to the standard Schrodinger equation, dependent on the time of the quantum mechanics.

In this context, ψ (x,t) can be interpreted as the envelope of a rapidly variable sinusoidal wave:

$$\phi(x,t) = \psi(x,t)e^{i(k_0 x - \omega_0 t)}$$

This is the typical equation for the propagation of a wave packet in a weakly non-linear dispersive system [ABL 04]. The dispersion relation takes the shape:

$$\Omega = \omega_0^{'} X + \frac{1}{2}\omega_0^{"} X - qa^2$$

Note that it is obtained by a direct substitution of a sinusoidal solution of shape $\Psi \to ae^{i(kx-\Omega t)}$.

In equation [5.4], the solution of this last equation is obtained by assuming that: $x \to x - \omega_0^{'} t$

$\Psi(x,t) = \varphi(x,t)e^{\,i\sigma(x,t)}$ where φ(x,t) and σ(x,t) are real functions.

For ←(x, t) this produces the two following equations: the real and imaginary parts of equation [5.4]:

$$\varphi\sigma_t - \frac{1}{2}W_0^{"}\sigma_{xx} + \frac{1}{2}W_0^{"}\varphi\left(\sigma_x\right)^2 - q\varphi^3 = 0 \qquad [5.4a]$$

$$\sigma_t - W_0^{"}\sigma_x + \frac{1}{2}W_0^{"}\varphi\sigma_{xx} \qquad [5.4b]$$

The solution consists of supposing progressive waves of the form

$\varphi = \varphi(x - v_e t)$ and $\sigma = \sigma(x - v_c t)$

The equation [5.4b] becomes:

$$\left[\varphi^2\left(W_0''\sigma_x - \nu_e\right)\right] = 0$$

which can be integrated to produce:

$$\sigma_x = \frac{\nu e}{w_e''} \qquad [5.4c]$$

By substituting the equation [5.4c] in [5.4a] and multiplying by 4 ρ_x this gives:

$$w_0''\left(\varphi_x\right)^2{}_x = \frac{1}{w_0''}\left(\nu_e^2 - 2\nu_e\nu_c\right)\left(\left(\varphi\right)^2{}_x - q^4\right)_x$$

which, on integration, gives:

$$\frac{1}{\varphi}\frac{w_0'' d\varphi}{\sqrt{\left(\nu_e^2 - 2\nu_e\nu_c\right) - qw_0''\varphi^2}} = \pm dx$$

This expression can be integrated and resolved for φ, the form of the solution depends on the sign of the term qwo"; for qwo" > 0 the solution is given by equation [5.4d], and for qwo"< 0 the solution is given by equation [5.4e].

$$\psi(x,t) = \left[\frac{v_e^2 - 2v_e v_c}{\left|qw_0''\right|}\right]\operatorname{sec h}\left\{\frac{\sqrt{v_0^2 - 2v_e v_c}}{w_0''}(x + x_0 - v_e t)\right\} e^{t\frac{Vs}{w_0''}(x - v_e t)} \qquad [5.4d]$$

Using the relation [5.4c] and $V_c = \frac{\Omega}{X}$, equation [5.4d] is written in the form: $Ve = \mathrm{X}W_0''$.

$$\psi(x,t) = a\operatorname{sec h}\left\{a\sqrt{\frac{|q|}{|w_0''|}}(x + x_0 - v_e t)\right\} e^{i(Xx - \Omega t))}$$

where:

$$\Omega = \frac{V_e X}{2} + \frac{a^2 q w_0'' X}{2V_e} = \frac{1}{2} W_0'' X^2 + \frac{1}{2} a^2 q.$$

$$\Psi = a \tan h\left\{a\sqrt{\left|q/w_0''\right|}(x + x0 - v_e t)\right\} e^{i(kx - \Omega t)} \qquad [5.4e]$$

The solution to the original problem is a rapidly varying sinusoidal wave, whose frequency and wave vector have been changed by Ω and X, and whose envelope is a solitary wave exponentially attenuating to zero for a large X.

Note that the NLSE has a very important property called its modulation instability [DEH 10, ZIO 14]. This refers to the fact that for a suitable choice of parameters, a small disturbance will grow exponentially with time.

5.3.3. *Focusing soliton oscillations*

Consider a soliton propagating along x in the plane x,y and assume that its size varies according to y (see Figure 5.6: the hatched regions correspond to greater sizes).

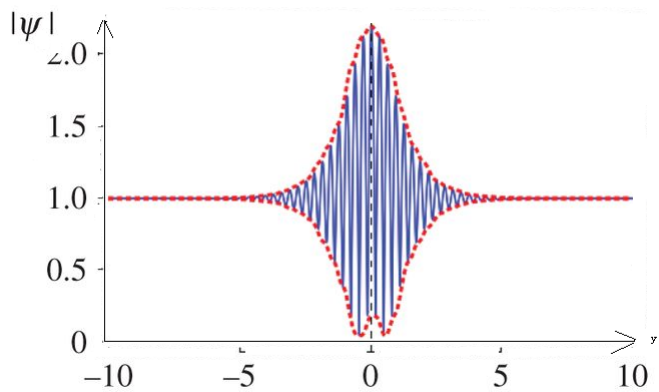


Figure 5.6. *Representation of attenuation in a fiber*

In a negative dispersion medium, the regions of large size move more quickly and the soliton curves (Figure 5.7); it is easy to find the size of this curving.

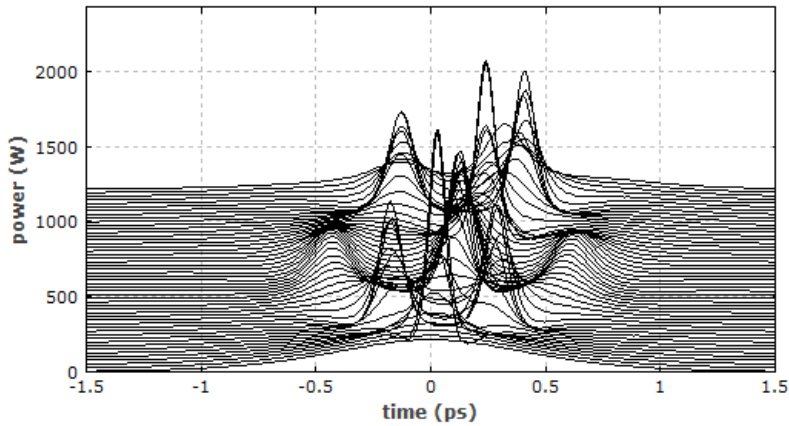


Figure 5.7. *Soliton subject to a modulation*

If the soliton is subject to a modulation in size, it curves. Because of this curving, a focalization effect is shown and the size of the central part of the portion of the soliton, shown in Figure 5.8 begins to grow; because of this, after a certain time, the central part will trap the peripheral regions and the wave's form will re-establish itself.

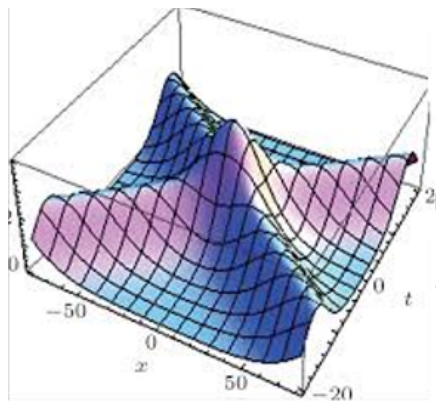


Figure 5.8. *Soliton focusing. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

On the contrary, in the case of GVD > 0, the situation changes: the soliton's size is negative, and leads to an increase in small oscillations. The sections of larger size are a little delayed and after the curvation, new portions of the disturbance rush

toward these regions. Because of this, the disturbance increases and the soliton dissociates in isolated clusters along the y-axis. It is not impossible for these clusters to then amortize, through disturbance radiation at large wavelengths (Figure 5.9).

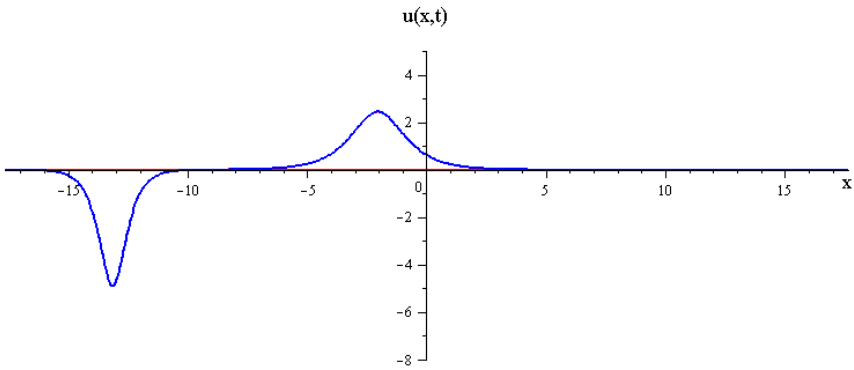


Figure 5.9. *Dissociation of the soliton. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

5.3.4. *Wave packet autostriction (modulation instability)*

Compression of the nonlinear wave is seen not only in the transverse direction, but also in the longitudinal direction relative to the wave's direction of propagation.

We assume a wave of a not particularly large size, so that it differs only very little from the sinusoidal wave, otherwise known as higher harmonics, and is weak when in equilibrium with the fundamental therefore allowing the wave to be characterized by the wave number k, and the frequency ω of the fundamental wave. For this wave, the main average, nonlinear effect is the dependence of the phase velocity or the frequency on the amplitude, so that for a small amplitude, when it can be limited to only the first correction that does not disappear, we have:

$$\omega = \omega_k + \alpha a^2 \qquad [5.5]$$

ω_k : Frequency of the linear wave

αa^2 : Nonlinear correction

If k and a vary with x, that is to say $\omega = \omega(x)$, then $k = -\frac{\delta\phi}{\phi x}$ will vary with time.

$$\frac{\delta k}{\delta t} = -\frac{\delta \omega}{\delta x} = -v_g \frac{\delta k}{\delta x} + \alpha \frac{\delta a^2}{\delta x} \quad [5.6]$$

with:

$$v^g = \frac{\delta \omega_k}{\delta k} \quad [5.7]$$

It appears that under well-determined conditions, the plane wave becomes unstable relative to the dissociation into isolated wave packets, so it is determined that the phase velocity depends on a correction term [ABL 03].

$$v = v_g x \pm \sqrt{\alpha a^2{}_0 v'_g x} \quad [5.8]$$

$$v'g = \frac{\delta v_g}{\delta k} \quad [5.9]$$

When $\alpha v'_g < 0$, there is instability in the form of fragmentation of the wave into packets and the autostriction of the wave packets. The physical direction of this instability is illustrated in Figure 5.10.

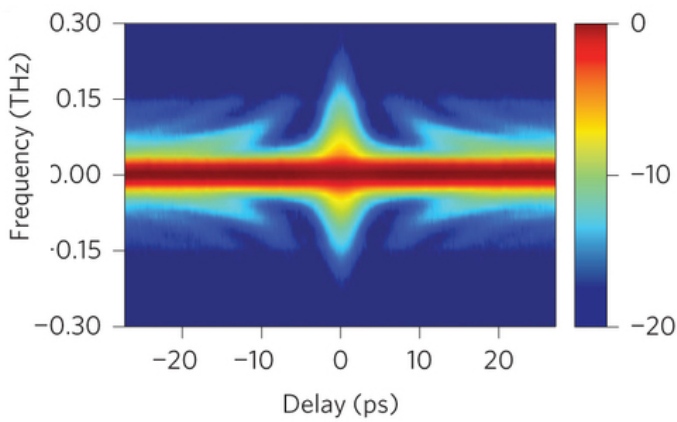


Figure 5.10. *Autostriction of the wave packet. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

If $\alpha < 0$ then at points A,A' the velocity is greater than at point B and on section P, the number of waves, which is proportional to the number of nodes per unit of length, will increase, whereas on section Q, it will decrease with time. Then, for $v'_g < 0$, the wave packet will be delayed in region P increasing the order at point A, whereas in region Q, it will be ahead and will increase the wave at point A'. The conclusion that autostriction takes place with $\alpha v'_g < 0$ is only valid for small enough values of x, in the opposite instance; the instability relative to the autostriction is then stabilized by the wave packet's diffraction spreading.

In conclusion, it is indeed possible for the wave to acquire periodic waves, and for it to form localized, soliton-type packets (see Figure 5.11).

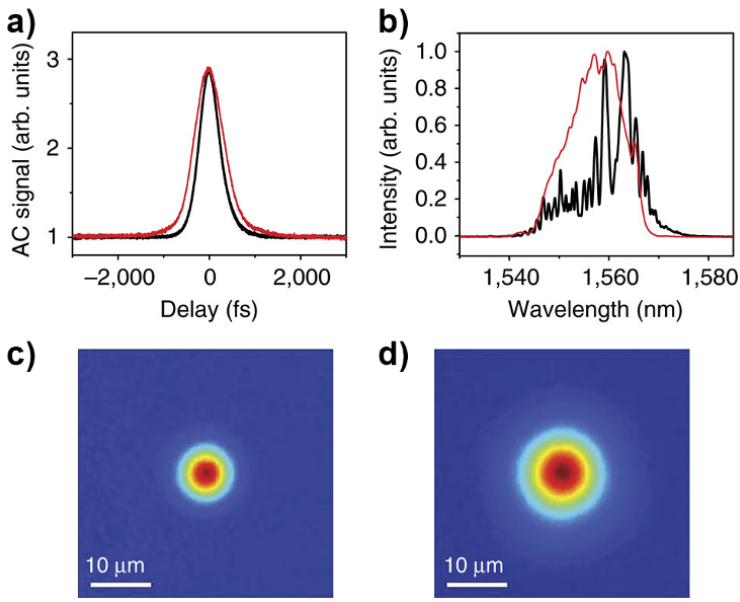


Figure 5.11. *Soliton characteristics: a) size, b) pulse phase, c) frequency chirp. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

Kerr nonlinearity in the optical fiber means that a fairly intense pulse alters the fiber's refraction index (a), the changed index in turn modulates the phase of the propagating pulse, so the index grows most at peak intensity where the phase delay

is, as can be seen, highest, and decreases in size at the front and back of the pulse (b). This is called phase modulation and in turn, it "chirps" the pulse's spectrum so that the low frequencies are placed in the first half, and the high frequencies in the other (c).

From this analysis, it appears that the frequency in the first half of the pulse decreases when the second shows an increase, in the same way as the sech pulse (soliton) [ABL 91].

Now consider what happens when the group velocity dispersion (GVD) and the nonlinear (NL) Kerr effect are both present at the same time; the envelope changes with the distance, producing an acceleration of the low frequencies and a slowing down of the high frequencies. The accelerated low frequencies travel far and the profile is attenuated more quickly.

The situation thus changes radically when the Kerr nonlinearity is paired with the GVD < 0 (negative as it is in the anomalous dispersion region).

The parasitic frequencies produced by the Kerr effect are compensated by these produced by GVD < 0, so the second half of the pulse containing the high frequencies is ahead, whereas the first, containing the low frequencies, is delayed [MOH 14].

On this figure, the dispersion of the fiber is given in picoseconds per kilometer-nanometer, which means that a 1 nm pulse (measured in terms of wavelength) spreads to a few picoseconds per 1 km; the dispersion of a conventional single-mode fiber is positive for wavelengths lower than 1.3 μm, and negative for greater wavelengths. In the positive dispersion, the low frequencies propagate more quickly than the high frequencies; in the negative dispersion, the opposite happens.

The pulse becomes quicker and flows into itself. A narrowing pulse is then obtained that does not change shape or speed along its propagation in the optical fiber. The dispersion is therefore kept in equilibrium by the nonlinearity and vice versa.

Note that the soliton's phase velocity in the negative dispersion medium is positive: that is to say, it moves more quickly than sound. In the soliton there is produced, so to speak, an equilibration of the nonlinearity and the dispersion; remember that nonlinearity tends to switch the pulse, whereas the dispersion causes a delay in the higher harmonics compared to the fundamental, which enables the solitary wave to maintain its profile in time.

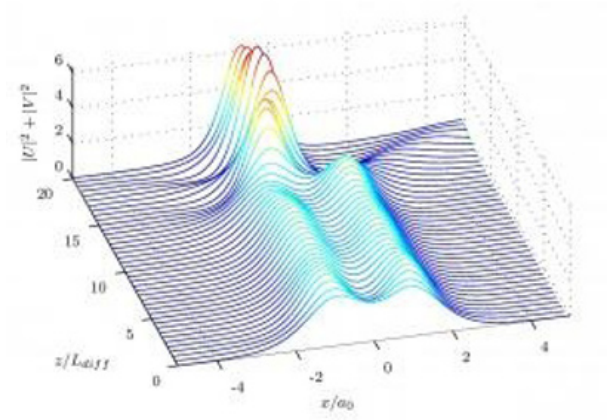


Figure 5.12. *Propagation of a soliton pulse in an optical fiber (dispersion-non linearity compromise). For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

5.3.5. *Evolution of the initial disturbance*

Let us now discuss the evolution in time of the oscillations created by a concentrated initial disturbance of finite size.

Suppose that at the initial instant, t = 0, a disturbance in the speed of amplitude u_0 is created. If $u_0 << c_0$ (c_0: speed of sound) the disturbance can be considered as being of weak non-linearity. In this case, the disturbance is broken down quite quickly before the nonlinearity can be manifested, into two waves propagating in different directions with the speed approximately equal to c_0 and constituting simple waves. It is therefore sufficient to follow the slow evolution of a single simple wave. The qualitative situation of these waves' evolution is revealed by the following reasoning:

First, suppose that the initial disturbance coincides exactly in shape with the soliton, which is to say that:

$$u(t,x)_{t=0} = \frac{u_0}{\text{sech}\left(\frac{x}{\Delta}\right)} \qquad [5.10]$$

where Δ is the typical size of the solitary wave. This disturbance could then propagate in the same way as a solitary wave.

Now consider the term which is a non-linearity parameter of the wave; its magnitude is proportional to the amplitude:

$$\sigma = \frac{u_0 k_0^2 \Delta^2}{\sigma c_0} \qquad [5.11]$$

For $\sigma << 1$, the amplitude of the disturbance is very small and, therefore, can be considered as linear.

For σ very close to 1, the beginning of a soliton is shown on Figure 5.13, and as it begins to take shape, when it reaches the value = 1, it is a fundamental soliton that appears, as shown in Figure 5.14.

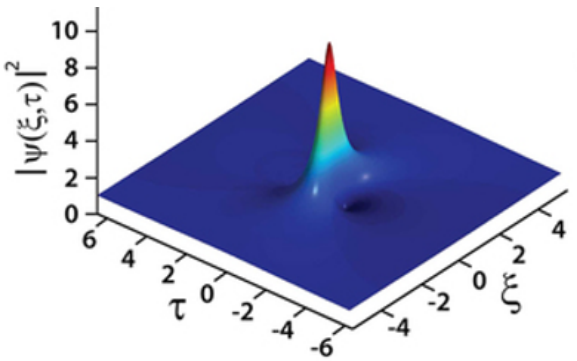


Figure 5.13. *Beginning of the soliton. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

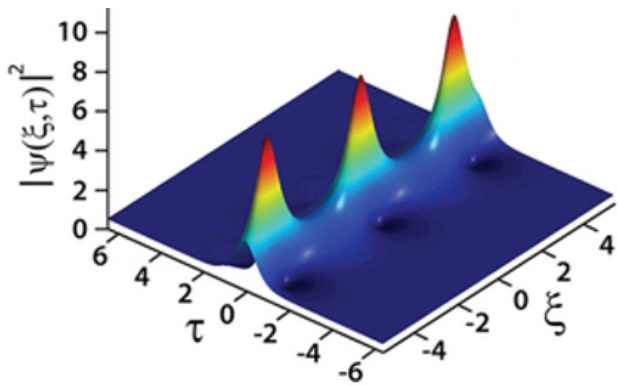


Figure 5.14. *A fundamental soliton appearing. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

Solitons, which are solitary waves that maintain their pulse length and their spectrum for thousands of kilometers, are very robust. The input pulse can be a square wave; all the unwanted parts will be removed, and the result is a soliton that propagates along the fiber. The dispersion is maintained in equilibrium by the non-linear and *vice versa*.

However, for $\sigma > 1$, the amplitude is so great that as a general rule there is no solution to the progressive stationary wave.

If the initial disturbance does not coincide in its profile with the solitary wave and shows the aspect of a pulse of size ∇ and amplitude μ_0, the size σ can be adopted as a parameter of nonlinearity.

For $\sigma << 1$, we have a linear disturbance. The part of the disturbance's spectral development with large wavelengths moves at a speed close to c_0, whereas the components with short waves are delayed on the fundamental pulse. The pulse, in its entirety, spreads due to the dispersion and its amplitude drops, as can be seen in Figure 5.15.

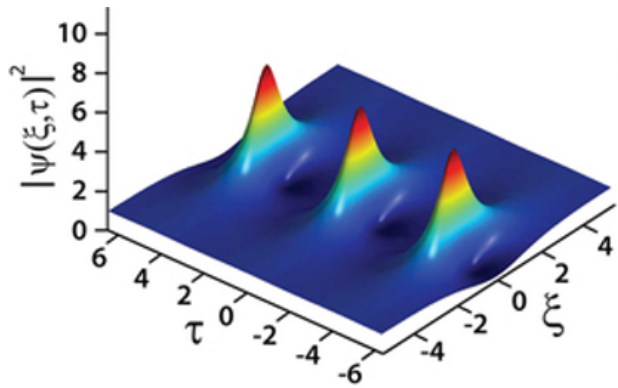


Figure 5.15. *The pulse spreading. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

It follows that at the stage where the nonlinear packet spreads, the parameter σ increases and the disturbance becomes more and more nonlinear.

One interesting case is an instance where a strongly nonlinear disturbance $\sigma >> 1$, when ∇ is large at the first stage of this disturbance's evolution: the dispersion does not become involved and the behavior of the disturbance of the leading edge tends to switch. However, with the appearance of the higher harmonics, the dispersion comes

into play. Its role amounts to "ramifying" the disturbances of different wavelengths. Additionally, after a large enough lapse of time, the disturbance disassociates into separate groups analogous to the wave packets in the linear instance. Each of these groups can more or less be considered to move at a constant speed. Indeed, all the solutions corresponding to progressive waves are already known: these are periodic waves at $\sigma < 1$ and solitons at $\sigma = 1$; no other solution is possible. Therefore, the initial pulse with $\sigma >> 1$ should break down into solitons and into a packet with weak nonlinearity.

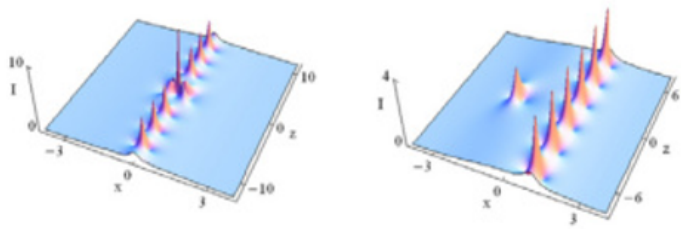


Figure 5.16. *A soliton propagating from a pulse disturbance with $\sigma < 1$. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

All solitons move at a supersonic speed $c_0 + c$, which is even greater than the amplitude of the solitary wave, whereas the packets, while spreading in time and decreasing in amplitude, are delayed in relation to point $x = c_0 t$.

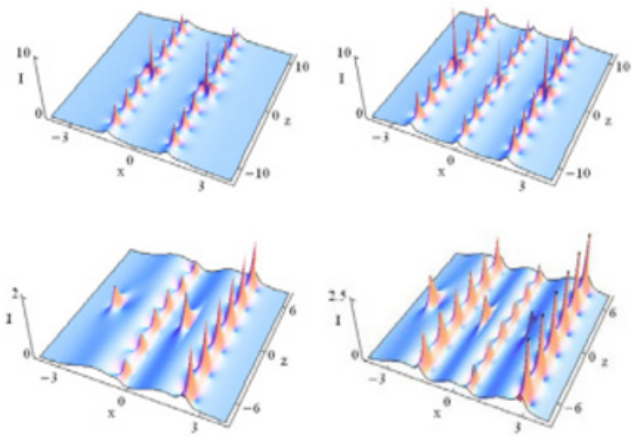


Figure 5.17. *A soliton propagating from a pulse disturbance with $\sigma >> 1$. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

Digital calculations have revealed the interesting nature of the nonlinear interaction of solitary waves with one another. If the solitary waves differ enough in amplitude, so that their relative speed is sufficiently large, one of the solitary waves passes in some way through the other.

However, during the solitons' mutual overlap, there is no superposition of disturbance: the total amplitude of two solitons that have fused proves to be a little less than the sum of their amplitudes. In a sense, in this case, we can speak of a double soliton state. This disturbance in the later evolution breaks down into two solitons coinciding exactly with the initial waves. After such a decomposition, it seems that we have solitons that have passed through one another. In a case where the difference in the solitary waves' speed is small and their amplitudes are similar, fusion does not occur. The solitons then meet at a short distance and the quickest wave through the "channel" links them, some of the disturbance passes to the slow soliton that is ahead; because of this the slow soliton is accelerated, whereas the faster soliton is halted.

Throughout this analysis, it is necessary to take account of the fact that solitons can only form where the initial disturbance has a positive amplitude (within a negative dispersion medium). If the initial disturbance has a negative amplitude throughout, it can only create solitary waves. In this case, it evolves into a "tail" of a nonlinear wave, which then spreads to a small amplitude and becomes linear.

The above will also apply to positive dispersion mediums, to modification corresponding not to the "barrels" but to the "hollows," and these all move at a speed lower than c_0, whereas the wave, the "tail" with slight amplitude moves at a speed greater than c_0. In negative dispersion mediums, the solitons only form for negative amplitudes.

5.4. Conclusion

In this study, it is clear that if we carefully manipulate the parameters of the optical fiber that characterize nonlinearity and dispersion, we can create an optimal regime for propagating pulses in the anomalous dispersion region (GVD < 0) in which the enlargement of the pulse due to the group velocity is balanced by the nonlinear compression of the pulse, leading to a pulse propagation without distortion, or a "soliton propagation."

6

Photonic Crystals

6.1. General introduction

For some decades, a community of researchers including specialists in optics, physicists and chemists has set itself the ambitious goal of creating a material that would, for photons, be what a crystal semi-conductor is for electrons. This new type of material has excited a lively interest in the world of research and in many branches of physics and chemistry. It is formed of the periodic, dielectric or metallic structures that come under the heading "photonic crystals (PCs)" or "Photonic Band Gap PBG", which show photonic states structured in forbidden bandwidths [YAB 87, JOH 87, YAB 91a].

Photonic crystals are new materials whose optical properties permit light to be manipulated on the scale of a wavelength. These crystals are structures whose dielectrical index varies greatly on the scale of a wavelength along one, two or three directions in space. This makes them effective, multidirectional, and compact reflectors, whose use makes it possible to create or envisage creating numerous components such as filters, guides, lasers with no thresholds, and microcavities [TAF 75a, TAL 02, QIU 03, AKA 03, KNI 00].

3D PCs have an omnidirectional forbidden bandwidth. However, the technological difficulties in creating them are great, given the dimensions required (in the order of a wavelength). Studies have therefore concentrated in the first

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

instance on 2D crystals, for developing planar integrated optical components of considerably reduced size (a few microns for optical applications).

The creation of two-dimensional periodic structures using different lithographic methods is now well-established for materials such as silicon and semi-conductors III-V [SCH 98[SMI 99, POT 99, REE 01a, REE 01b].

During the last decade, photonic crystals (PC), also known as structures with forbidden photonic band gaps (PBGs) have been the subject of many research studies.

PCs are very promising systems for applications in the domain of electromagnetic waves, for real achievements in the domain of micro-waves, optoelectronics and optical telecommunications. Many works have been published on semiconductors benefiting from technological advances in microelectronics.

The aim of this chapter is to present basic concepts relating to photonic crystals. First of all, the example of a photonic crystal with one dimension will be shown to introduce the main notions concerning periodic structures, emphasizing the notion of the forbidden photonic band gap, before entering further into the details of the structure that will mainly interest us: two dimensional crystals. We will end by presenting some examples of applications in which periodic structures are used. This enables us to highlight the use of materials at forbidden photonic band gaps in several domains such as optics, micro-wave circuits and antennae.

6.2. Photonic crystals

Photonic crystals [YAB 93, JOA 95] are artificial structures whose dielectric constant is modulated periodically in one, two or three directions with a period in the order of the wavelengths of optical photons (Figure 6.1). These structures can be obtained by a periodic arrangement of two different materials. Their simplest shape is a periodic structure with a dimension composed of a layer stack, also called a “Bragg mirror”. Photonic crystals have the capacity to inhibit the propagation of light in some directions for a frequency range called the forbidden photonic band gap (BIP). This optical peculiarity comes into play when the length of the crystal mesh is of the same order of magnitude as the wavelength of the light in the medium. This phenomenon is to some extent similar to that of the opening of forbidden electronic band gaps in atomic crystals of semiconductor materials.

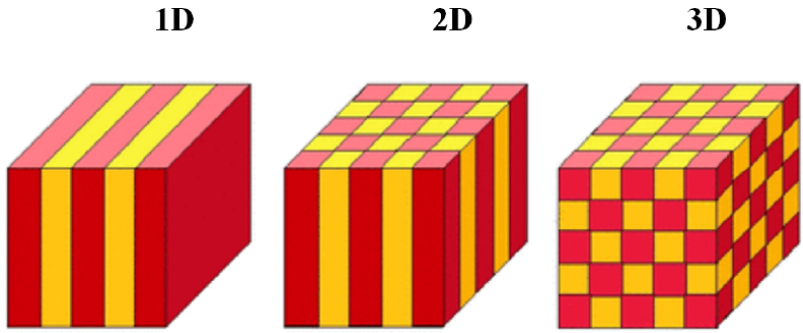


Figure 6.1. *Schematic illustration of unidimensional 1D, two-dimensional 2D and three-dimensional photonic crystals 3D*

The property of a "gap" or "forbidden band" was initially demonstrated by Lord Rayleigh in 1887 in Bragg mirror-type structures. The concept's generalization to two or three dimensions was initiated in 1987 by Zengerle [ZEN 87], Yablonovitch [YAB 87] and John [JOH 87] with the aim of controlling the spontaneous emission of light.

Photonic crystals exist in nature in mineral and biological states. For example, opals are minerals made up of arrangements of spheres of hydrated silica. Their fires result from the diffraction of light by their structure in a three-dimensional photonic crystal. The origin of the coloring of many animal and vegetable species also comes from periodic motifs. The blue coloring of the wings of morpho butterflies and the leaves of some types of the Selaginella are examples of this coloring [VUK 03]. The blue, green, yellow and brown colors of peacock feathers come from diffraction by 2D photonic crystals of varying number and mesh length (Figure 6.2) [ZI 03].

6.2.1. *Photonic crystals with one dimension (Bragg network)*

A unidimensional (1D) photonic crystal is made up of periodic alternation in a single direction of space of two dielectric mediums with the respective dielectric constants ε_1 and ε_2. The Bragg mirror made up of a successive stack of layers with two different refraction indexes forms a photonic crystal with one dimension. A diagram of this structure is shown on Figure 6.3. This structure's forbidden band gaps, also called a Bragg mirror, are sensitive to the wave's angle of incidence. Therefore, in order to obtain control over the forbidden band gaps whatever the angle of incidence, it is necessary to extend the structure's periodicity to two or

three dimensions. The 1D structure is linear. They have already been studied at length and used as dielectrical mirrors or optical fibers.

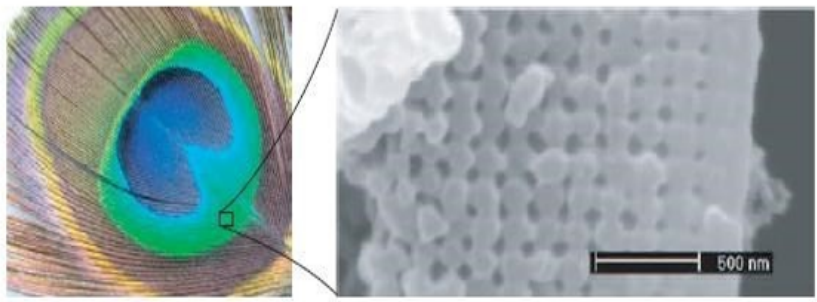


Figure 6.2. *Peacock feather. The box on the right is an image taken under a scanning electron microscope (SEM) of a slice of a green feather strand. The structure of 2D photonic crystal is made up of pillars of melamine linked by keratin as well as pockets of air*

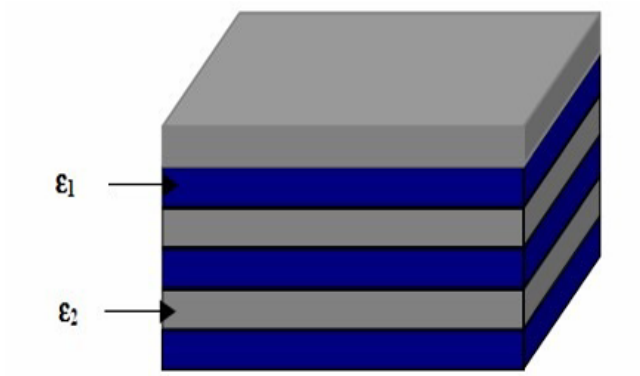


Figure 6.3. *Diagram of a Bragg mirror made of a finite periodic, dielectric medium*

6.2.1.1. *Forbidden photonic band gap 1D*

We will now try to give some specifics on the key notion of photonic crystals: the forbidden photonic band gap. To do this, we will study the simplest case: that of a unidimensional stacking of layers with different indexes. A similar development can be found in [SAK 01] or indeed in [LOU 03]. We are only interested in the case with normal incidence where the electric field is parallel to the Oz axis (Figure 6.4).

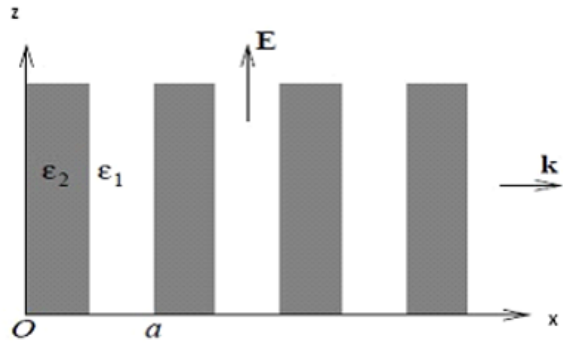


Figure 6.4. *Geometry of a 1D photonic crystal*

This is the interval that is called a forbidden photonic band gap. Note that this is even larger than the modulation of the dielectric constant A_1 is significant and that it is cancelled when the material is homogenous ($A_1 = 0$). We can interpret these results in the following fashion:

Close to the zone's edges, the modes of the wave vector $k \approx \pi/a$ a and $k \approx -\pi/a$ begin to combine under the effect of the dielectric constant's modulation. This mixing causes degeneracy to appear and causes the appearance of the forbidden band (Figure 6.5). Inside the forbidden band, no mode can propagate and the medium is therefore a perfect reflector.

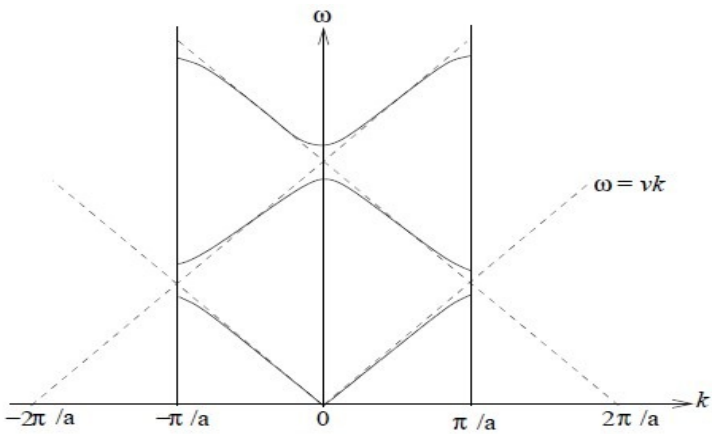


Figure 6.5. *Dispersion relation for a unidimensional photonic crystal. The boundaries of the first Brillouin zone are indicated by the two vertical lines, and the dispersion lines of a uniform material are in dotted lines [JOA 95]*

6.2.1.2. *Width of the forbidden photonic band gap*

The width of the forbidden photonic band gap depends on the contrast between the two mediums' indexes: when this contrast is slight, the width of the gap is slight (Figure 6.6(a)) and when it is large, it increases considerably (Figure 6.6(b)).

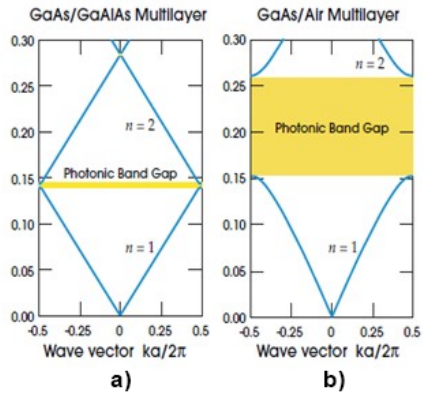


Figure 6.6. *Structures of photonic bands for Bragg networks with period a with a) permittivity layers ε = 13 and 12 and b) permittivity ε = 13 and 1 [JOA 95]*

6.2.2. *Band diagram*

In the case of a triangular network of pockets of air in a dielectric matrix (ε = 12) and for a ratio of r/a = 0.4 with r representing the pockets' radius and a the network's period, the band diagram is represented in the following way (Figure 6.7):

The band diagram represents the variations in frequency permitted in the network depending on the projection of the wave vector in its high-symmetry directions. The diagram is shown in reduced units. In fact, the law of scale enables the photonic crystals' properties to be transposed to all the frequency domains provided that the period and the wavelength are modified in the same proportions.

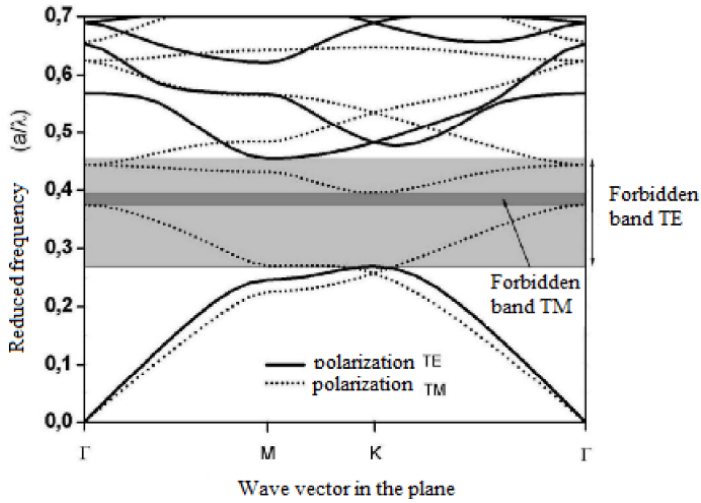


Figure 6.7. *Band diagram of a two-dimensional photonic crystal*

To interpret the band diagram, it is first sensible to take account of the influence of the polarization of light, in fact, of whether it is considered to be electric transverse (ET) polarization or magnetic transverse (MT). The permitted and forbidden energy bands are different. It can be shown, for example, that a structure made of a triangular network of cylinders with high permittivity immersed in a weaker permittivity matrix leads to the appearance of a broad forbidden photonic band gap for the MT polarization. When the forbidden photonic band gaps for the ET and MT polarizations overlap they are therefore called complete forbidden bands. A photonic crystal can also show a forbidden band in one of the network's directions but not in the others.

In most cases, the usefulness of a photonic crystal comes from its ability to prevent the propagation of light. It is, therefore, highly desirable to work with a crystal that shows the most complete forbidden band possible.

6.2.3. *Maps of forbidden bands*

Maps of forbidden bands show the edges of forbidden bands for a given network according to the fill factor f (Figure 6.8). They give an overview of the possibilities of confining light. For the square network, the forbidden bands in ET and MT polarization open, respectively, for f = 35% and f = 50% [SAK 01]. For the triangular network, they open respectively for f = 11% and f = 63% [SAK 01]. The area of the complete forbidden band corresponds to the intersection of forbidden

bands ET and MT and is situated in the energy window u = 0.37–0.56. The triangular network is generally used more than the square network: the forbidden ET bands are broader and open for filling factors.

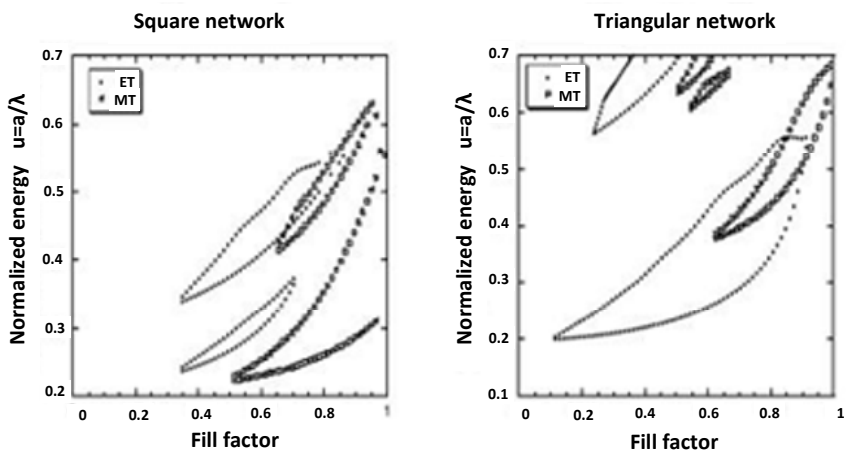


Figure 6.8. *Maps of forbidden bands of a network of air pockets in a dielectric matrix ε = 11.4, for a) a square network and for b) a triangular network*

6.3. Three-dimensional photonic crystals

3D photonic crystals have attracted and still attract numerous research efforts. They are the only structure that makes it possible to obtain a forbidden energy band in all space directions. We have seen that CP 3D have existed in nature for a long time (Figure 6.1), but the first 3D photonic crystal was made in 1990 by K.M. Ho *et al.* [HO 90]. It was made of spheres of silicon arranged in a diamond structure. But history generally remembers the famous Yablonovitch 3D structure for microwaves made in 1993 by E. Yablonovitch [YAB 91b], by piercing holes in plexiglas from three azimuthal angles separated at 120° and making an angle of 35° compared to the normal.

6.4. Filters and multiplexors

An important function that can be created with photonic crystals is wavelength division multiplexing (WDM). The aim is to insert or extract very precise wavelengths. Several experiments have illustrated the possibility of coupling a cavity with a guide [SMI 99, CHU 01]. For example, the experiment in [CHU 01] enables extraction or insertion of a very precise wavelength in a waveguide.

6.5. Add-drop filters

Space–frequency filtering is one of the specifics of photonic crystal filters. As such, Figure 6.9 shows a diagram of an add-drop filter, which has a strategic role in optical telecommunications. Unlike telephone communications where the electrical signals are transported through copper wires, the transmission of optical signals is carried out by optical fibers along which several channels of independent wavelengths can coexist (more than 1,000 in the next generation of fibers). Each wavelength channel is meant to occupy a spectral domain $\Delta\lambda$ around 0.3 nm in the region of $\lambda = 1{,}500$ nm (which is around 40 GHz in frequency); this gives the optical fibers previously unprecedented overall flow capacities, of several terabits per second. This being the case, to use the signal corresponding to precise information transmitted along the fiber; it is necessary to drop the wavelength channel where this information is located in the receiving end. In the same way, if we would like to be able to add information on a given wavelength channel, it is then necessary to insert the signal into the set of information channels. This double filtering (Add-Drop) function is therefore essential in optical telecommunications networks.

In the case on Figure 6.9, the filter shown is designed from a 2D photonic crystal with hexagonal symmetry where two wave guides coupled to one another by a central cavity, also hexagonally shaped, have been introduced. Optical fibers (not shown) are placed at the wave guides' entrances and exits. One of the wave guides (the one at the bottom) is used to propagate a set of signals at different wave lengths λ_i, among which there is a signal at wave length λ_1 that we wish to select. The central cavity is chosen in order to present a resonance at this wave length; the circle shown on the figure indicates the location of the electromagnetic field linked to the resonant mode. If the guides are perfectly coupled to the cavity, the optical beam at wave length λ_1 will therefore be able to pass entirely from one guide to another, since the optical cavity presents a transmission unit for the field mode adapted to it. The subtraction function has therefore been created. It is possible, on the other hand, to create the addition function by injecting a signal with the wavelength λ_1 through the higher guide's left entrance.

Various photonic crystal based versions of the Add-Drop filter have already been created (see, for example [NOD 07]). However, selectivity is required to select one wavelength channel from the others. Such selectivity requires quality factors in the order of 10,000 for the cavity acting as coupling (Figure 6.9) as well as an excellent coupling between the guides and the cavity. The best quality factors obtained lie at around 3,000 for the smallest cavities with a single pocket missing in a 2D crystal [YOS 01]. This value increases to more than 40,000 for three or four missing pockets. Furthermore, work is underway to optimize the coupling between the guide and the microcavity.

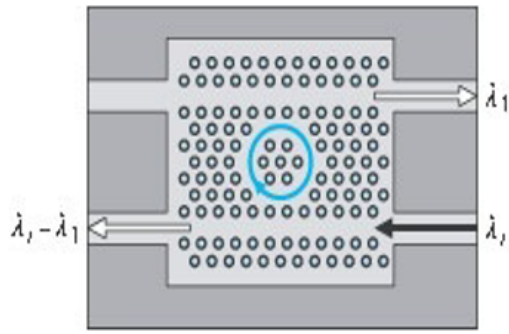


Figure 6.9. *Add-Drop filter: the entrance signal, below right, is made of a large number of signals of different wavelengths λ_i. The filter, created in a two-dimensional crystal of hexagonal symmetry, enables one of the crystals to be extracted (here, the one at wavelength λ_1) by shifting it in another direction [NOD 07]*

6.6. Digital methods for photonic crystal analysis

6.6.1. *Introduction*

Generating periodic structures in optical materials and microwaves is a currently expanding technique, as a result, in particular, of their very many potential applications. Research on this type of material has also changed considerably in the course of recent years, as much at the basic as at the applied level. Creations from these periodic materials are structures with finite dimensions. However, digital modeling, which enables these materials' characteristics to be determined, generally considers these structures to have infinite dimensions. In light of the increasing interest in periodic structures, digital methods for modeling them have not stopped developing. They are many and varied and can be classed according to the domain in which they operate: frequency or time. For the first category, we can cite as examples: the plane wave method (PWM), the method of moments and the finite element method. As for the second category, the most usual and widespread is the finite difference time domain (FDTD) method. The results of the simulations that will be shown in this work will tackle plane-wave calculations and FDTD, created thanks to RSoft's " BandSOLVE" and "FullWAVE" software.

6.6.2. *Modeling periodic dielectric structures*

Periodic dielectric structures are essentially materials with forbidden photonic bands formed from dielectric networks. These structures' main characteristic is their ability to function as mirrors by partially or totally reflecting electromagnetic waves in a particular band of frequency, for particular incidences depending on the type of material used [LOU 03]. These structures reflect waves thanks to the phenomenon of constructive interference between the different layers that form the material. As a result of the periodic stratification, the waves then interfere in a constructive or destructive way depending on the value of the phase shift, which depends on, among other things, the wavelength and the angle of incidence [GUO 03]. Two approaches can be used to study these structures: modeling in the frequency domain and in the time domain. Frequency methods are generally the most appropriate for studying this type of material. They make it possible to obtain simultaneously (almost instantaneously in two-dimensional instances) the band structures and state of the modes. Time methods are better adapted to carrying out simulations that involve a change in time, such as transmission calculations and calculating the time from relaxation to resonance. But they can also be used to calculate band structures and to find resonance modes.

6.6.3. *FDTD method*

The digital FDTD method was developed by Yee [YEE 66] in 1966 and it was only in 1975 that a series of articles advocating its future applications appeared [TAF 75a, TAF 75b]. Thanks to its advantages and to IT skills becoming more and more effective, FDTD has not ceased to gain users for more and more varied applications.

The FDTD method can simulate the behavior of an electromagnetic wave in any kind of medium (dielectric, metal, plasma), while still taking account of the most complex geometric shapes of the objects that can form that system. No matrix inversion is involved. Its extremely simple theoretical formulation [TAF 05] provides predictions with great precision for a broad range of problems in the electromagnetic domain. It has a broad band; an impulse excitation in the time domain is enough to give a system's response on a wide band of frequencies via a Fourier transform.

In this section, we show the principles of the FDTD method and we explain the points necessary for modeling photonic crystals.

6.6.4. *Available digital tools*

6.6.4.1. *Bandsolve*

All the band diagrams in our study have been computed using "Bandsolve" software, from the same software series as "Fullwave", i.e. RSoft.

"Bandsolve" is a simulation software that makes it possible to generate and analyze photonic band diagrams. Computation of these diagrams is based on a method using the decomposition of electromagnetic fields into plane waves for periodic structures. The structures whose band diagrams we wish to compute are all structures that repeat periodically [NEE 06].

At two dimensions, it is necessary to consider two different propagation directions: ET (with the E field perpendicular to the pockets' axis) and MT (where E is parallel with the pockets' axis). These two polarizations are decoupled and give rise to two independent band diagrams. There is not necessarily a forbidden band in these two cases. Moreover, it can be applied to structures such as photonic crystal fibers, which are complex for other simulation techniques. Band Solve is particularly useful for optimizing the properties of photonic crystal structures, which are simulated using the FDTD method implemented in the software, Full Wave, to examine the time-dependent properties such as losses, and to calculate field distributions in structures with finite dimensions [PWM].

We have validated our calculations in the instance of a triangular network. To do this, we have taken the example used by [NEE 06]. The structure is a triangular mesh made of air pockets (n = 1) of periodic cylindrical shape immersed in a dielectric medium (Si) with the refraction index (n = 3.42). The cylinders' radius is r = 0.43a. In Figure 6.10(a) and (b), we respectively show the band structure calculated by [NEE 06] and the one we have simulated. There is a concordance between our PWM results and those produced by silicon with $\varepsilon = 11.6$ and $r/a = 0.43$ for the ET polarization (in red) and TM (in blue). The hatched zones mark each of the polarization' BIPs. Only the frequencies between 0.385 and 0.406 permit the opening of a forbidden band.

6.6.4.2. *Full Wave*

The digital simulations have been carried out with the Full Wave software, which is an electromagnetic simulation software based on the FDTD method [FDT]. The FDTD method is based on the solving of Maxwell equations in a spatially and temporally discretized domain. It enables the evolution of the EM field to be followed over a course of time at any point in the structure. We can thus obtain EM field maps at any place or moment, knowing that the field's evolution according to time also enables us to obtain information on the structure's spectral response.

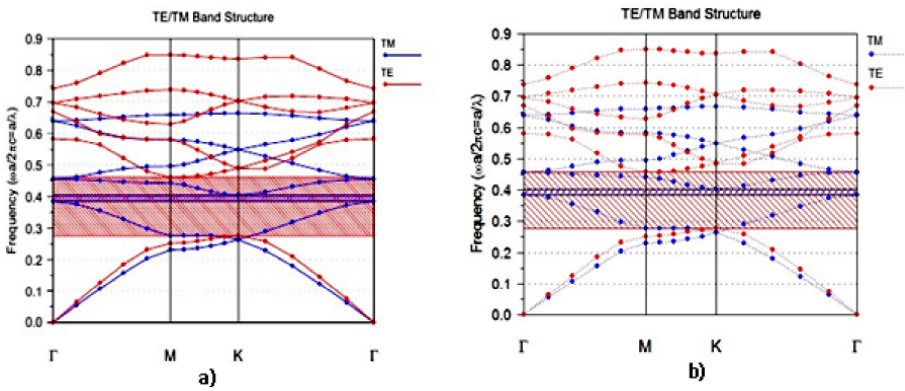


Figure 6.10. *Dispersion diagram of a triangular network a) results obtained by [NEE 06] and b) results obtained by the Band Solve simulator. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

This software can simulate structures (limited, infinite or periodic), formed of different materials that can be metallic or dielectric. Using Full Wave requires us to define the materials that the structure is made of, with the help of electric permittivity. It is also necessary to define the structure's environment and therefore the boundary conditions. To do this, it is necessary to have absorbent conditions at the edges of the discretization (calculation) domain that enable us to avoid the parasitic reflections caused at the edges of the FDTD calculation window in order to simulate an open medium. In our work, we consider the absorbing layer model discovered by J.P. Béranger [BER 96] and designed by perfectly matched layer (PML) [MEK 99], which is perfectly adapted to modeling absorbing boundaries in electro-magnetics.

This software enables us to calculate the field diffracted by any structure, periodic or not. We have used it to study the materials with dielectric forbidden photonic band gap.

Given the lively interest excited by materials with forbidden photonic band gaps, studies have been directed toward modeling this type of periodic structure. The plane-wave method was the first to be used to calculate the energy band structures of dielectric structures. This technique for resolution in the frequency domain consists of developing the electromagnetic field on a plane-wave basis. Writing Maxwell equations in this base then leads to an eigenvalue equation whose solution enables us to obtain dispersion relations linking the frequency to the wave vector. The FDTD method has been widely used for modeling this type of material thanks to its ease of implementation. However, it is more often used to calculate transmission and

reflection diagrams than diagrams of band structures due to the enormous calculation time and memory storage capacity that it requires.

6.7. Conclusion

This chapter focuses on the digital study of photonic crystal cavities, formed from air pockets on InP, with low volume (the omission of one of more motifs) with a minimum number of losses, with the aim of increasing the quality factors while still retaining the weakest possible modal volume. These cavities are based on a mode engineering technique that consists of using defects: removing holes by moving them or locally changing their radius. By locally varying the holes' radius (that is to say the fill factor) or their position, we thus obtain a gradient index that enables us to obtain a less sudden transition between the photonic crystal and the cavity's edge. This enables us to limit the losses outside the plane and so to increase the quality factor. For the same structure, we have studied the optical properties of forbidden photonic bands and cavities according to the variation in the air pockets' refraction index. This research has been pursued using a digital study of two types of filter: the first filter comprises two guide sections and is therefore very well-adapted to a coupling with guides of similar widths. Most of the wavelengths guided will be reflected at the end of the guide, except for some, which will be coupled to the cavity. In this filter, the length of the wave guide can be optimized to reach high values of the transmission and the quality factor simultaneously. The number of holes between the cavity and the wave guide is chosen to be equal to 2, 3, 4 and 5. For values of N, we have obtained a very high quality factor with a very weak transmission. In order to increase the transmission and keep the high-quality factor simultaneously, while reducing the losses from propagation, we have changed the size of the holes at the end of the cavity and studied the effect of these modified holes on the position, transmission rate and quality factor of the cavity's resonant mode. The second drop filter juxtaposes the cavity in parallel to the guide to create a lateral interaction of the cavity's modes with the guide's modes. This coupling enables us to extract one or more frequencies propagating in the guide. These frequencies can eventually be redirected in a directive way, towards a second guide also juxtaposed to the cavity. Wavelength router applications are, therefore, possible.

7

ROADM

7.1. Technological advances

Technological *advances* in the domain of optics and photonics have resulted in decisive development in quantum routers. Photonic technology is fairly similar to quantum technology. On this, we will cite the work of [CHE 85, CHI 03, CHO 04, CHO 11, CHO 12]. Researchers from the Weizmann Institute have developed the first quantum router [ISR 14].

In parallel, researchers from the University of Tsinghau in China have found another version of a quantum router [MOR 12].

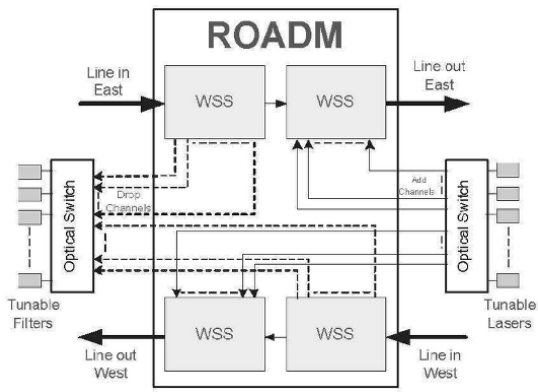


Figure 7.1. *Example of a router incorporated into a device*

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

7.2. "Router"-type filter

The photonic filters under study have the capacity to provide an information routing function. Thus, selected frequencies are allowed in the transmission process, and those that are rejected are removed from the circuit. The routing function that we propose could be a means of routing information from one access point to another.

An initial, theoretical proposition was provided by Fan and coauthors [FAN 99] in 1999. Since then, several experiments have shown the possibility of coupling a cavity with a guide, for example, an experiment by Chutinan and co-authors [CHU 99], of which a diagram is shown on Figure 7.2, enables a precise wavelength (WDM mono-channel) to be extracted from the plane or inserted into a wave guide.

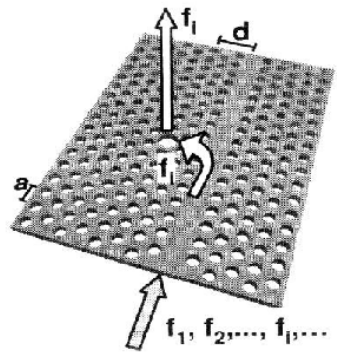


Figure 7.2. *Diagram of the principle behind a multiplexing device (insertion or extraction of a particular wavelength) [QIU 03]*

Figure 7.2 shows a diagram of the basic structure of drop (router) filter devices, which is based on 2D photonic crystals made of a triangular network of air pockets. Our approach is to design a (WDM: Wavelength Division Demultiplexing) demultiplexer of greatly reduced size, versatile and compact at the wavelength $\lambda = 1.55$ µm which can be adapted to optical telecommunications networks. This demultiplexer is based on using photonic crystals that are linear and pointed by default.

The router filter is a wavelength selective optical device including a network for modifying the complex amplitude of the electromagnetic field of a wave of light, using a filtering function. It can also function as a fiber optic wavelength multiplexer and demultiplexer.

The basic photonic crystal is the same as the one studied previously: it is a hexagonal crystal of the period a = 0.44 μm with the same air fill.

The structure on which this study is based is shown on Figure 7.2. It is a W_1 guide corresponding to the omission of a row of pores of 0.36a radius, linked to a linear cavity. The latter is also formed by the omission of two adjacent holes in the direction ΓK of the photonic crystal. The cavity and the guide will be separated by 3 rows of holes. We now have a cavity, produced from the same sample, which therefore shows parameters very similar to those of the coupled system. The light will consequently be generated at the entrance to the guide.

Quantum algorithmics for adaptive networks in WDM (Wavelength Division Multiplexing) routers for voice, data and multimedia applications have led to a new domain in the maintenance of projected, guaranteed communication networks. These days, multimedia communication for the reliable exchange of data requires the communication to meet strict norms where information can easily be transmitted and received by commentators with ease and comfort. High network demand has led to a rapid increase in bandwidth for communication, unfortunately, this has occurred at the expense of communication traffic and the loss of security in data circulation. In order to solve this problem, quantum cryptography is put forward as an alternative solution and quantum key distribution (QKD) uses quantum mechanics to guarantee secure data communication.

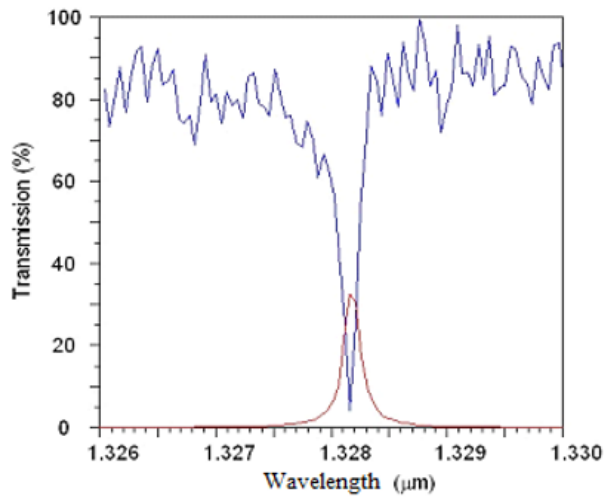


Figure 7.3. *Transmission spectrums of the filter inside the cavity (red line), at the guide's exit (blue line). The cavity and guide are separated by 3 rows of holes. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

On Figure 6.14, we have shown the transmission spectrums linked to the system, coupled with the generation of light occurring at the entrance to the guide. In this case, the cavity and the guide are separated by 3 rows of holes. We notice the existence of a mode of cavity 1.3281 μm, characterized by a Q factor close to 8595. The appearance of this mode of cavity can only arise from the transfer of a particle of light guided towards the cavity. At the same time, spectral analysis of the signal transmitted through the guide makes a drop in transmission occur, which coincides spectrally with the cavity mode.

To describe the effects of coupling, it is however easier to consider the guide as a disturbance of the cavity. By approaching a guide of a cavity with quality factor Q, we enable the evanescent particles of the guide's fields and the cavity to couple with one another. The cavity's quality factor Q is therefore reduced by the losses resulting from the coupling in the guide. When the guide is "far" from the cavity, the mode propagated in the guide does not "see" it. The cavity acts as a single cavity, and the signal propagated in the guide does not feel its influence. In the opposite case, where the guide is infinitely close to the cavity, its influence on the cavity is very significant and completely breaks down the structure's Q factor. Transmission through the guide is still total and occurs at once as the cavity is not able to trap light. Between these two extremes, the coupling between the guide and the cavity leads to a decrease in the filter's transmission. In this filter, the distance between the cavity and the guide can be optimized in order to acquire the highest quality factor and filter transmission. The number of rows between the guide and the cavity (d) is chosen to be equal to 3, 4, 5 and 6. Figure 7. 4 shows the influence of the number of rows between the cavity and the guide (d) on the wavelength and the resonant mode's transmission at the guide's exit. The hollow present in this figure's transmission spectrum represents the selective extraction of the guided light ("drop" filtering).

We have demonstrated a coupling effect of the guide towards the cavity. In particular, in cases where a mode is injected at the entrance to the wave guide, a light particle is extracted into a mode with losses from the cavity, then radiated into the air.

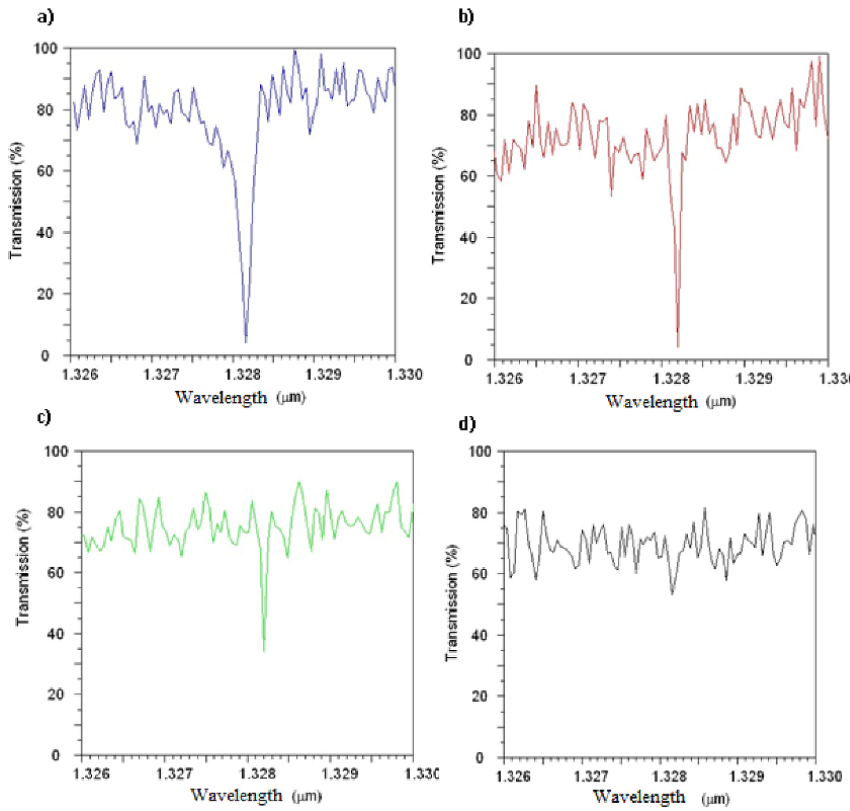


Figure 7.4. *Transmission spectrum for the filter at the guide's exit. The cavity and the guide are separated by: a) 3 rows of holes (the blue line), b) 4 rows of holes (the red line), c) 5 rows (the green line) and d) 6 rows of holes (the black line). For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

8

WDM

Whereas transmission systems based on optical fibers only relied on the use of time multiplexing (or time division multiplexing (TDM)), a new generation of systems appeared at the beginning of the beginning of the 1990s, implementing wavelength division multiplexing (WDM).

8.1. Operating principle

WDM technology was born out of the idea of injecting several streams of digital signals simultaneously into the same optic fiber at the same modulation speed, but each at a distinct wavelength.

At transmission, n channels at a nominal flow, D, are multiplexed at the receiver; the overall signal n × D is demultiplexed into n nominal channels. The principle of a linkage comprising a multiplexer and a demultiplexer is shown in Figure 8.1. It should be noted that the fibers' design and manufacture follows norms G651 to G655, and that the WDM's design and manufacture follows the norm G692. In particular, the spacing between the two wavelengths is defined by international norm ITU-T G 692 (optical interfaces for multi-channel systems with optical amplifiers). It defines a wavelength comb authorized in the single transmission window 1,530–1,565 nm. This spacing in nanometers (nm) or in Gigahertz (GHz) between two wavelengths has been fixed at 200 GHz or 1.6 nm and 100 GHz or 0.8 nm.

WDM technology is termed dense (DWDM) when the spacing used is equal to or less than 100 GHz. Systems with 50 GHz (0.4 nm) and 25 GHz (0.2 nm) have already been tested.

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

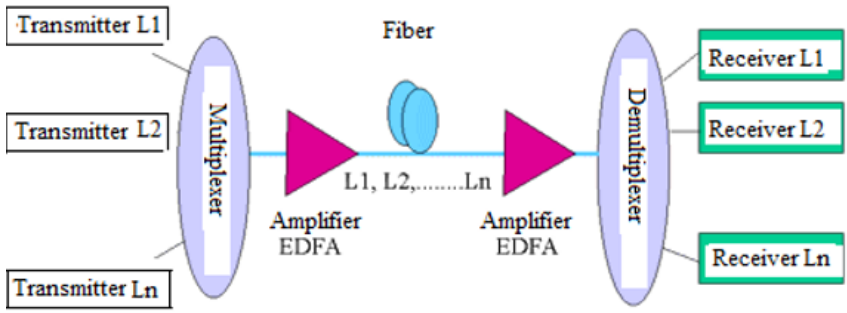


Figure 8.1. *Principle behind a WDM/DWDM link*

One of the key components of WDM/DWDM is the erbium-doped fiber amplifier (EDFA), which enables insertion losses resulting from multiplexing/ demultiplexing the wavelengths to be compensated.

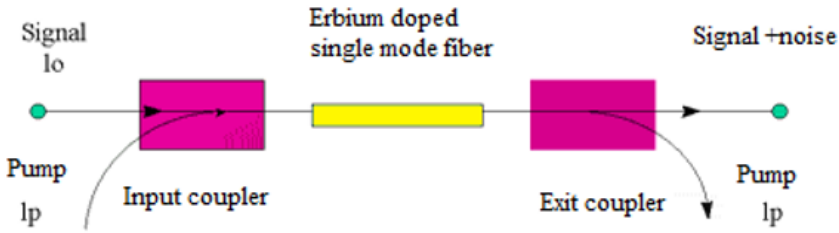


Figure 8.2. *Principle behind the optical amplifier*

Nevertheless, the DWDM introduces nonlinear phenomena that result, in particular, in limiting the distance between amplifiers to between 50 and 100 km in practice.

8.2. Using WDM systems

WDM/DWDM systems marketed today carry 4, 8, 16, 32, or 80 optical channels, which enables capacities of 10, 20, 40, 80, or 200 Gb/s, respectively be reached, allowing for a nominal flow of 2.5 Gb/s per channel, a flow for which the transmission/reception components are widespread.

To give a concrete idea of this, a system with 16 2.5 Gb/s channels will allow 500,000 telephone conversations to be transmitted along a fiber simultaneously.

Taking account of the numerous advantages that DWDM brings, integrating this new technology into operating networks requires us to rethink its architecture with the double aim of moving the investments already made while preparing for the near future, where simplicity, reliability and low cost will be the keys to success.

The approach taken by new operators in the US today, of building their network directly with the Internet protocol (IP) on SDH, or indeed the IP on DWDM, is a revealing indication of this tendency, which should appear in Europe in the coming years.

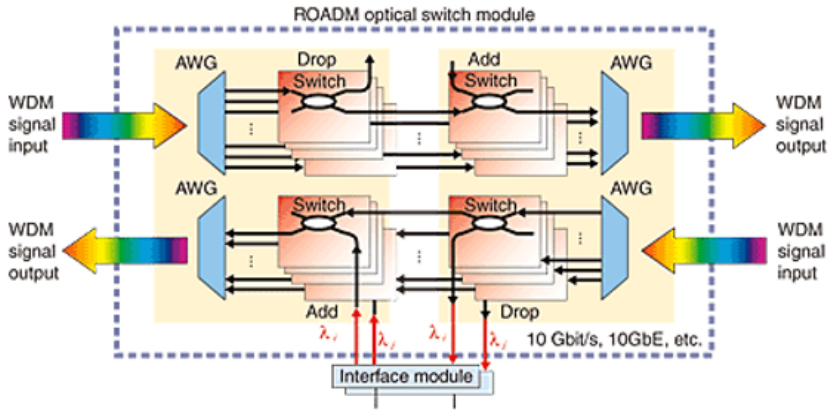


Figure 8.3. *WDM/ROADM device. For a color version of the figure, see www.iste.co.uk/benslama/quantum.zip*

It thus seems certain that tomorrow the optical wavelength will become an integral part of the network and that DWDM technology has not yet reached its limits.

New techniques currently being developed enable optical systems' capacities to be multiplied further:

– soliton transmission, enabling very narrow pulses to be transported over thousands of kilometers without being distorted, while still maintaining a very large bandwidth;

– pulse modulation or duo-binary transmission, enabling the electronic flow to be increased two- or threefold, using pulses with two or three binary levels.

8.3. DWDM networks

The quantum algorithm for adaptive networks in WDM (Wavelength Division Multiplexing) routers for voice, data and multimedia applications has created a new domain in sustaining foreseeable and guaranteed communication networks. Currently, multimedia communications for the exchange of reliable data require the communications to respond to rigorous norms where the information can easily be transmitted and received between users [VAZ02]. High demand on the network has led to a rapid increase in communication bandwidth, unfortunately, this has happened at the expense of the communication traffic and compromises the security of data circulation [CHE10, CHO04]. To solve this problem, quantum cryptography is proposed as an alternative solution and quantum key distribution (QKD) uses quantum mechanics to ensure secure communication data [KHA04].

The switching network (WDM) is formed of switching nodes with a communication that links these nodes. Each linking channel contains a number of wavelengths and each wavelength is also divided into a number of time slots to control the transfer of each packet. Node architecture for sub-wavelengths demands a multicast data transfer mode supporting three links with the congestion and free links. The link's wavelength packet and the three time intervals for all the channels is the node for determining sessions using the bandwidth's time slot.

9

Quantum Algorithms

Quantum computers are known for being qualitatively more powerful than classic computers, but until now, only a small number of algorithms that use this potential effectively have been discovered. It is therefore highly desirable to develop other types of quantum algorithms that broaden the range of possible applications [COE 09]. Here, we propose an effective and precise quantum algorithm for finding the square-free part of a whole number – a problem for which no effective classic algorithm exists. The algorithm relies on Gauss sum properties, and it uses the quantum Fourier transform [CLE 98]. We give an explicit quantum network for the algorithm. Our algorithm introduces new concepts and methods that are not currently used in quantum information processing and can be applicable to a broader category of problems. The fundamental principle of classic IT is based on the Church–Turing argument, which states that any calculation device that it is possible to create on a practical level can be simulated by a universal computer known as a Turing machine.

However, this hypothesis relies implicitly on the laws of classical physics and was contested by Feynman and others, who suggested that calculation devices that function using quantum mechanics could be qualitatively more powerful than classic computers. It has been shown that the quantum Turing machine [TUR 50] is capable of simulating other quantum mechanical systems, with an exponential improvement in calculation in polynomial time over the classic Turing machine. Testing them did not give a real, rapid quantum algorithm, but in the following year Peter Shor arrived with his famous factorization algorithm [SHO 99] in response.

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

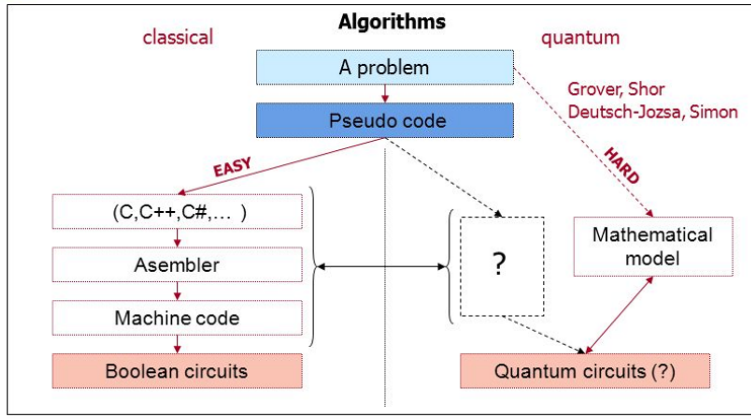


Figure 9.1. *An example of a quantum algorithm*

10

Applications

10.1. Laser satellites

Lasers are a promising means of ensuring quantum communications links. In the domain of telecommunications, we can glimpse possible applications for use in the space domain. In order to ensure propagation between satellites in the least possible time, a broadband service articulated around constellations of satellites with inter-satellite laser links (ISL) is considered. This technology makes it possible to satisfy the increasing demand for data traffic.

Because of the relative speed between two satellites, a significant Doppler effect can be observed on the inter-satellite links by the terminals on board the satellites. This chapter describes an analytical method for determining the shift in wavelength, measured by the terminal onboard a satellite, of the signal transmitted by the inter-satellite links.

The fine pointing mechanism in optical ISLs is considered in the analytical expression of a Doppler wave's change in length. Then, depending on the ISL characteristics of the satellite constellations, the expression of the Doppler shift is deduced in two phases. First of all, for the whole ISL access time, it changes according to the constellation's parameters. LEO satellite constellations' inter-satellite laser links are considered in our research; we aim to reduce inter-satellite propagation delays. To do this, we use laser beams to reduce the delays. Because of the relative velocity of very high satellites and in line with the increase in data traffic, a significant Doppler effect is observed at the edges of the terminal mounted on the inter-satellite links.

Through this work, we seek to establish effective inter-satellite links to increase the performances of the laser beams that reduce propagation delays, and to filter communication to avoid any form of interference.

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

10.1.1. *The Doppler effect in inter-satellite laser communications*

We show the frequency detected by the detection satellite as follows, when the detection satellite and the source satellite are both in motion:

$$f_d = f_s \frac{1 - \left(\frac{u_d}{c}\right) cos\theta_d}{1 - \left(\frac{u_{ds}}{c}\right) cos\theta_s} \quad [10.1]$$

with f_s being the source frequency delivered by the source satellite, $\boldsymbol{u_d}$ *et* $\boldsymbol{u_s}$ the velocities of the detection satellite and of the source satellite respectively, $\boldsymbol{\theta_d}$ the angle between the waves' propagation directions and the motion of the detection satellite, $\boldsymbol{\theta_s}$ the angle between the waves' propagation directions and the motion of the source satellite and c the velocity of the light wave.

As for transmissions via inter-satellite laser links, it is difficult to obtain the angles between the waves' propagation directions and the satellites' motion at first hand, and since the light wave propagates along a straight line between the two satellites, the two angles are formed between the relative position vector and the velocity vectors of the two satellites.

The relative position vector $\boldsymbol{r(t)}$, of the source satellite to the destination satellite is obtained by:

$$r(t) = r_d(t) - r_s(t) \quad [10.2]$$

$\boldsymbol{r_s(t)}$ $\boldsymbol{et}$ $\boldsymbol{r_d(t)}$ are the position vectors of the source satellite and the destination satellite. Taking into account equation [10.1.2], we can rewrite equation [10.1.1] in the following form:

$$f_d = f_s \frac{c - \dot{r}_d(t)\left[\frac{r(t)}{|r(t)|}\right]}{c - \dot{r}_s(t)\left[\frac{r(t)}{|r(t)|}\right]} \quad [10.3]$$

$\boldsymbol{\dot{r}_s(t)}$ and $\boldsymbol{\dot{r}_d(t)}$ are the velocity vectors of the source satellite and the destination satellite respectively. Converting the frequency into a wavelength, the normalized Doppler shift is given by:

$$\frac{\Delta\lambda}{\lambda_s} = \frac{\frac{dr(t)}{dt}}{c - r(t)\left[\frac{\dot{r}(t)}{|r(t)|}\right]} \quad [10.4]$$

$d|r(t)|/dt$ is the relative velocity of the destination satellite compared to the source satellite.

During the pointing, acquisition and tracking process, the source satellite is activated after the acquisition of the destination satellite's tags. Then, the source satellite should direct its beam ahead following a certain angle along the destination satellite's path, because the destination satellite has moved from its original location by an additional distance during the light wave's propagation. The propagation delay is calculated by:

$$\tau = \frac{|r(t)|+|r(t,\tau)|}{c} + t_d \qquad [10.5]$$

Where:

$$\boldsymbol{r(t,\tau) = r_d(t+\tau) + r_s(t);}$$

$\boldsymbol{t_d}$: processing delay in the source satellite.

Because of the small change in the relative distance between the two ISL satellites during the de time delay, equation [10.1.5] can be approximated by:

$$\tau = 2\frac{|r(t)|}{c} + t_d \qquad [10.6]$$

We substitute $\boldsymbol{r(t,\tau)}$ in equation [10.1.4], the normalized Doppler shift in the inter-satellite laser communication has the following form:

$$\frac{\Delta\lambda}{\lambda_s} = \frac{d|r(t)|}{cdt} \qquad [10.7]$$

Hence the term $\boldsymbol{c - \dot{r}(t+\tau).[r(t,\tau)/|r(t,\tau)|]}$ is ignored because of $\boldsymbol{c - c \gg \dot{r}(t+\tau).[r(t,\tau)/|r(t,\tau)|]}$ Thus, using equation [10.1.7], the Doppler shift received at any point of the destination satellite's orbit during the ISL's establishment can be estimated.

10.1.2. *Modeling the Doppler effect in inter-satellite laser communications*

We are interested in low earth orbit (LEO) constellations; there are two types of inter-satellite link (ISL) connections: intra-orbit inter-satellite links (ISL) and inter-orbit inter-satellite links (ISL).

The first type of connection connects satellites that belong to the same orbital plane, so the relative distance of the two communicating satellites is fixed, following equation [10.1.7], no Doppler effect can be detected, while the second type of connection connects satellites belonging to different orbital planes. However, the

relative distance of the two communicating satellites varies from one moment to another, which triggers the appearance of the Doppler shift.

We will adopt the Delta-Walker notation: N is the total number of satellites in the constellation that contains P orbital planes, each orbital plane contains S satellites, F is the constellation phasing factor. The phase offset between the satellites in the adjacent orbits is determined by: $2\pi F/N$. Where F can take the values : 0…P-1. Depending on the geometric relationship of the geography, the position vector (x_{ik}, y_{ik}, z_{ik}) of satellite number k in orbit number i, can be expressed by the constellation parameters:

$$x_{ik} = -Rcos\theta \sin\left(\frac{2\pi i}{P}\right) sin\left[\omega t + 2\pi\left(\frac{k}{S}\right) + \frac{iF}{PS}\right] + R cos\left(\frac{2\pi i}{P}\right) cos\left[\omega t + 2\pi\left(\frac{k}{S}\right) + \frac{iF}{PS}\right]$$

$$y_{ik} = Rcos\theta \cos\left(\frac{2\pi i}{P}\right) sin\left[\omega t + 2\pi\left(\frac{k}{S}\right) + \frac{iF}{PS}\right] + R sin\left(\frac{2\pi i}{P}\right) cos\left[\omega t + 2\pi\left(\frac{k}{S}\right) + \frac{iF}{PS}\right]$$

$$Z_{ik} = Rsin\theta sin\left[\omega t + 2\pi\left(\frac{k}{S}\right) + \frac{iF}{PS}\right] \quad [10.8]$$

$\boldsymbol{R}$: distance between the satellite and the earth's center, is equal to the orbital altitude of satellite H plus the earth's radius, r_E.

$\boldsymbol{\omega}$: satellite's angular velocity.

$\boldsymbol{\theta}$: the orbital plane's inclination.

$\boldsymbol{k}$: varies from 0…S-1.

$\boldsymbol{i}$: varies from 0…P-1.

Figure 10.1 shows the logical connections of incessant inter-satellite laser links for a constellation of 2π, with considerations on the limitation and distance permission of the inter-satellite links (ISLs) to link with the nodes that belong to the same group of nodes (i.e. the two communicating satellites are ascending satellites or indeed descending satellites).

There are only two types of incessant ISL inter-orbital links: (a) the k to k connection, which connects the $\boldsymbol{k}$th satellite in the ith orbital plane with the $(k - 1)$th satellite in the (i + 1)th orbital plane:

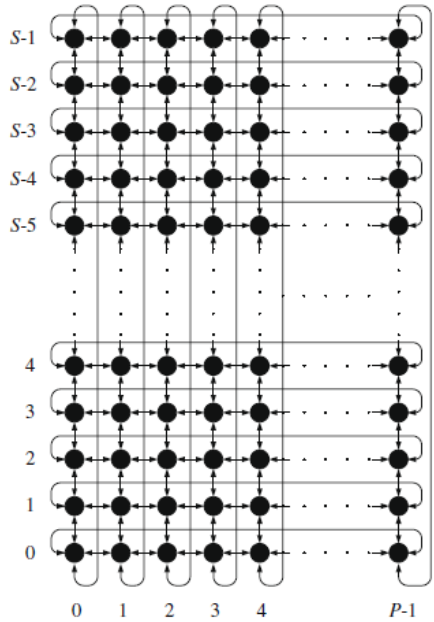


Figure 10.1(a). *The K to K connection*

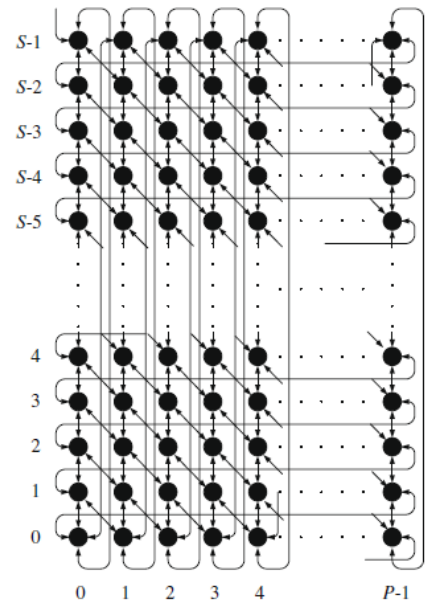


Figure 10.1(b). *The K to K – 1 connection.*

Using equation [10.1.8], the relative distance for the two types of inter-orbital connection for the incessant inter-satellite links is given by:

$$|r(t,\tau| = R\sqrt{\text{acos}(2\omega t + 2\pi m) + b} \qquad [10.9]$$

Where:

$$a = sin^2\theta \left[1 - cos\left(\frac{2\pi}{P}\right)\right] \qquad [10.10]$$

$$b = 2cos\theta \sin\left(\frac{2\pi}{P}\right)\sin(2\pi m) - 2\cos(2\pi m)\left[sin^2\theta - sin^2\theta \cos\left(\frac{2\pi}{P}\right) + 2cos\left(\frac{2\pi}{P}\right)\right] + 2 \qquad [10.11]$$

Parameter $\boldsymbol{m}$ is given by:

$$m = \begin{cases} \dfrac{F}{PS} + \left(\dfrac{\omega\tau}{\pi}\right) & \text{K to K link} \\ \dfrac{S-1}{S} + \dfrac{F}{PS} + \left(\dfrac{\omega\tau}{\pi}\right) & \text{K to K } - \text{ 1 link} \end{cases} \qquad [10.12]$$

We substitute equation [10.1.9] in equation [10.1.7], the determination of the Doppler shift depending on the constellation's parameters is given by:

$$\frac{\Delta\lambda}{\lambda_s} = -\frac{\omega R}{c}\frac{\text{asin}\,(2\omega t + 2\pi m)}{\sqrt{\text{acos}(2\omega t + 2\pi m) + b}} \qquad [10.13]$$

We consider the delay $\boldsymbol{\tau}$ to be constant as the rate of its variation is very small, in the order of 10^{-5}.

From equation [10.1.13], we see that the Doppler shift in the incessant inter-satellite links depends on the constellation's parameters.

To illustrate this chapter, we carry out a simulation with the following data: H = 1000 km; λ_s = 1550 nm, θ = 55°; P = 11; S = 12 and F = 1.

Figure 10.2a shows the variation of the relative distance between the two communicating satellites, connection k to k, we see that the relative distance varies between [500 km, 4500 km].

Figure 10.2 b shows us that the relative distance of the two communicating satellites in k to k – 1 connection mode varies between [3300 km, 5400 km].

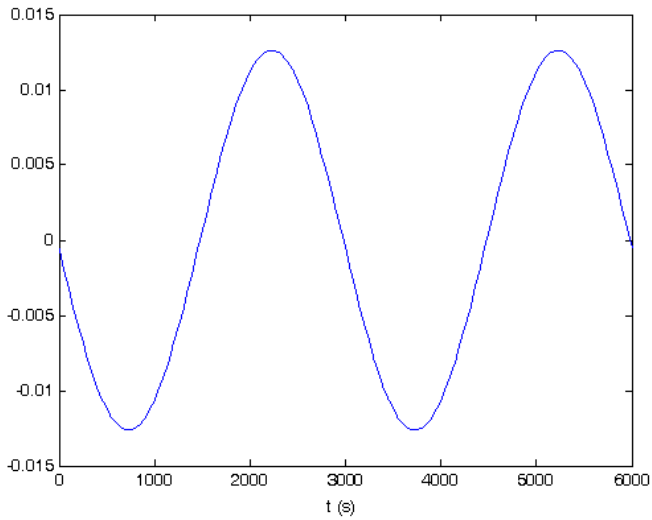


Figure 10.2(a). *The K to K connection.*

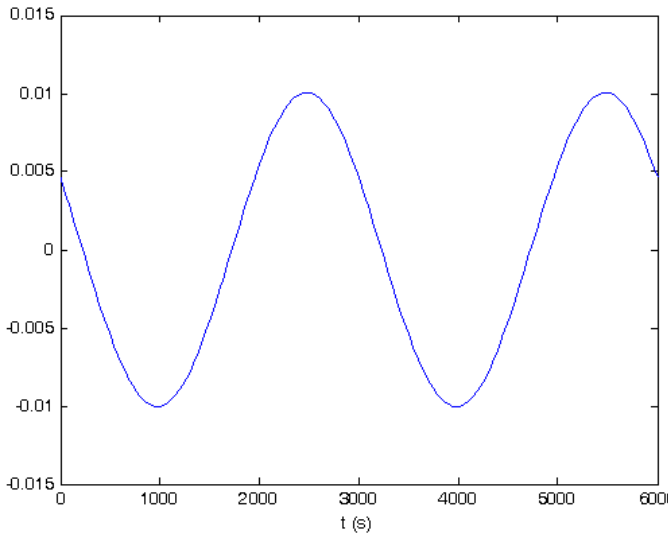


Figure 10.2(b). *The K to K – 1 connection.*

Figures 10.2a and 10.2b show the variations in the Doppler shift depending on the time in a constellation period, for the k to k connection and the k to k – 1

connection, the Doppler shift varies periodically with a half period as much as the constellation period. It reaches its peak value twice above each of the earth's hemispheres. The peak value above the northern hemisphere is produced when the two ISL satellites rise or descend.

The Doppler shift in the incessant inter-satellite links depends on the constellation parameters.

10.1.3. *Calculation software*

A calculation software using the main formulae obtained by the following authors [ARN97, ARN98a, ARN98b, ARN98c, ARN99, FUY10, LAM95, BAR85, SPI68, WEI12, LAM95] and which makes it possible to calculate the optimization of the opening of the telescope, the amplitudes of the vibrations depending on the SNR, the bit error rate BER depending on the S and the gain factor, are discussed in this chapter. Readers interested in further information should consult these references.

10.1.4. *Calculation software*

10.1.4.1. *Illustration and general structure of the software*

10.1.4.1.1. Password

When running the satlaser software, the first window to open is the password window, where the exact password must be entered in order for the software to be used.

Figure 10.3. *Password*

This window contains two buttons:

OK (*Valider*): if the password is correct, you simply need to click the OK button to run the software.

CANCEL (*Quitter*): if you wish to exit, you simply need to click on “exit”.

10.1.4.1.2. Main menu

This is the main window that includes the different menus needed to use the software. The latter is broken down into three parts:

Figure 10.4. *Main menu*

A: Description and generalities on laser satellites. This part contains two buttons:

1) INTRODUCTION : a click on the first button displays a window containing a general introduction on the subject.

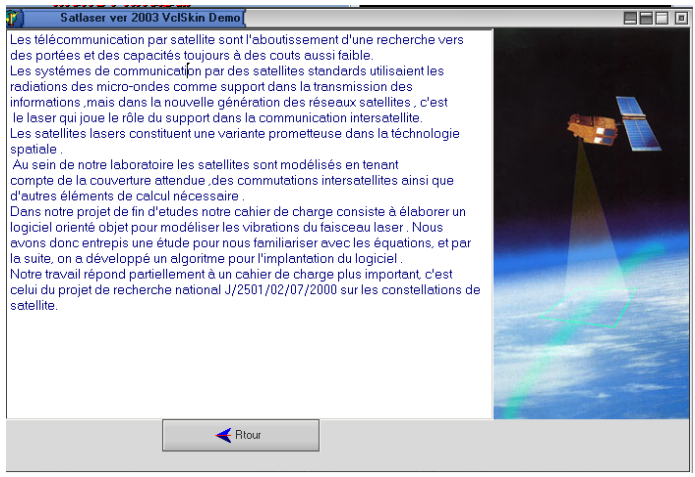


Figure 10.5. *Introduction*

2) Généralité sur les satellites lasers (General remarks on Satellite Lasers): a click on the second button displays a window containing the architecture of an optical link as well as its different blocks.

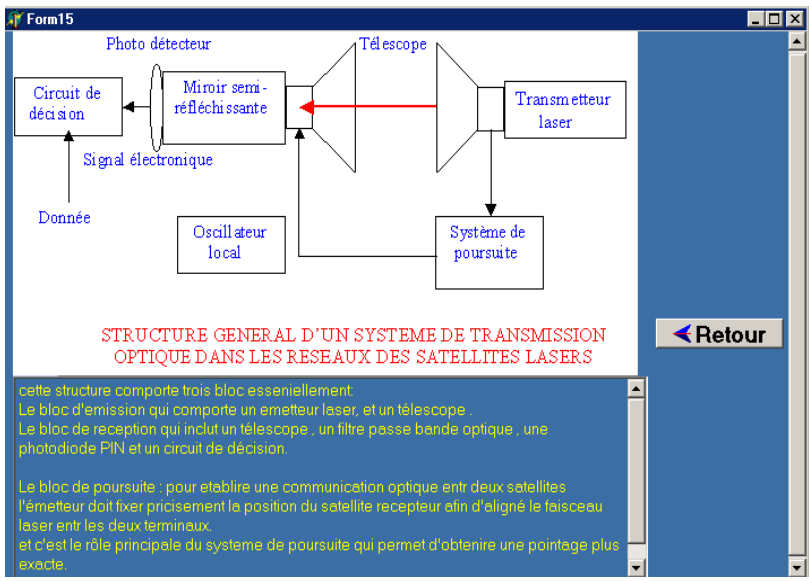


Figure 10.6. *General remarks on satellite lasers*

The return (*Retour*) button takes the user back to the home page (main menu).

10.1.4.1.3. Graph study of the solutions suggested: in this part there are six buttons

3) L'optimisation de l'ouverture du télescope émetteur (Optimization of the telescope opening): When you click on this button; the window that will appear contains a developed structure of an optical transmission system in order to decrease the effects of the vibrations.

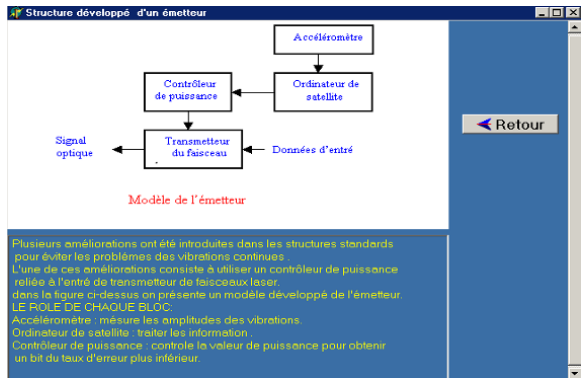


Figure 10.7. *Developed structure of an optical transmission system*

4) Isolateur de vibration (vibration isolator): A simple click on this button displays a window containing another solution.

Figure 10.8. *Vibration isolator*

5) Canal de diversité (diversity channel): This displays the window below:

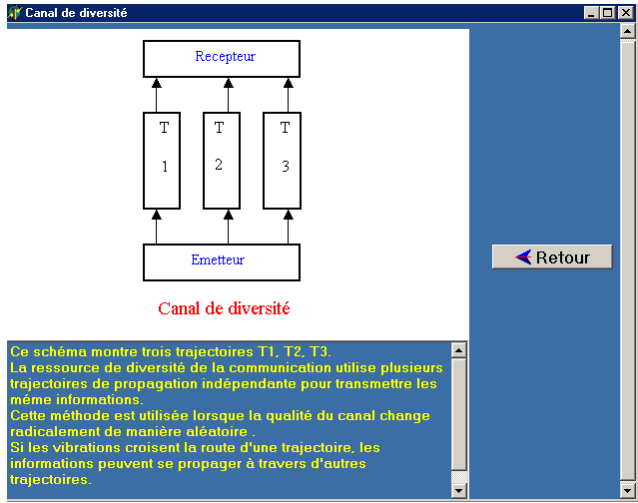


Figure 10.9. *Diversity channel*

6) alimentation auto accordée directe (Self-generated supply): When activated, it displays the following window, with a small explanation on this solution.

Figure 10.10. *Self-generated supply*

7) Adaptation de la bande passante (bandwidth adaptation): Activating this button displays a window containing two curves:

– The first, for asynchronous detection (FSK)

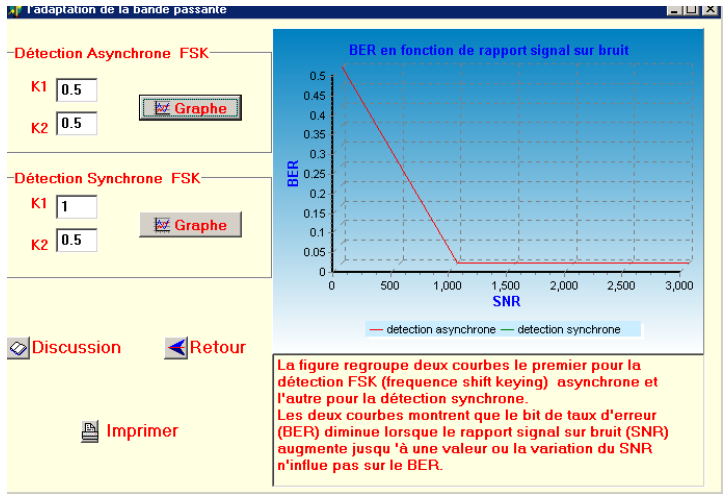


Figure 10.11. *Bandwidth adaptation*

Graphe: Clicking on the Graph button leads to the following graph:

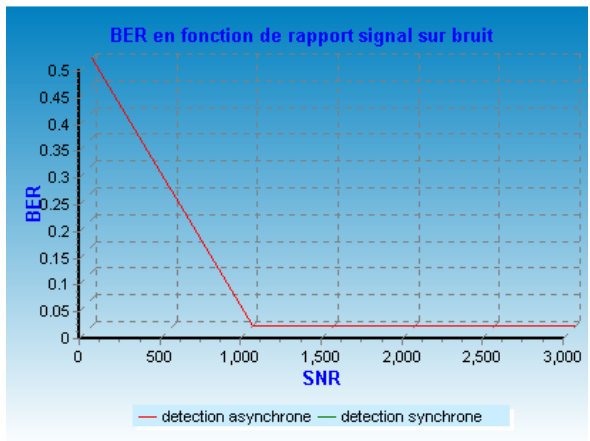


Figure 10.12. *The bit error rate (BER) depending on the signal to noise ratio (SNR)*

– The second for synchronous detection (FSK):

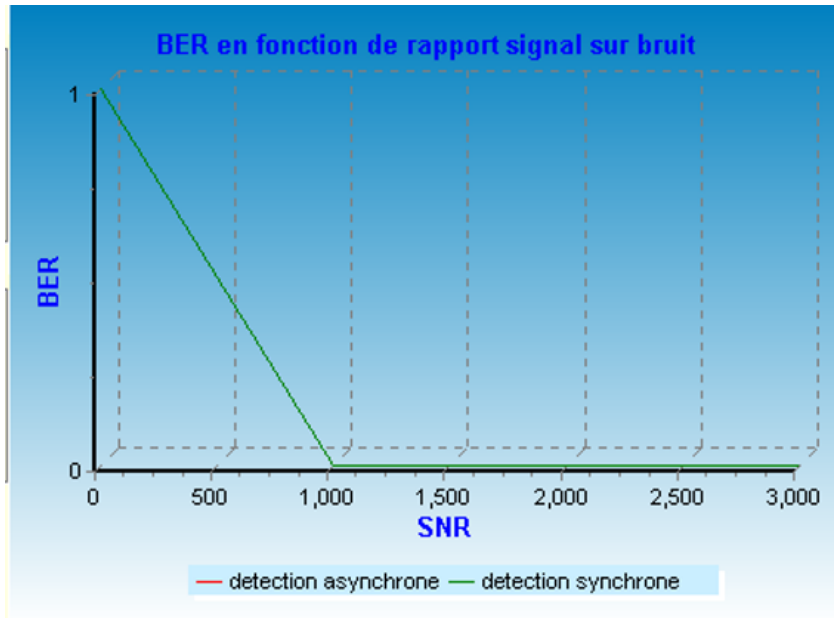


Figure 10.13. *The bit error rate (BER) depending on the signal to noise ratio (SNR)*

Clicking on the discussions button leads us to all the commentaries that can be developed from the two curves:

The two curves show that the bit error rate (BER) decreases when the signal to noise ratio (SNR) increases, up to a precise value at which the variation of the SNR does not influence l.

Activating this button gives us a window containing the essential part of our software, as it shows a graph study of different solutions proposed to improve the optical communication.

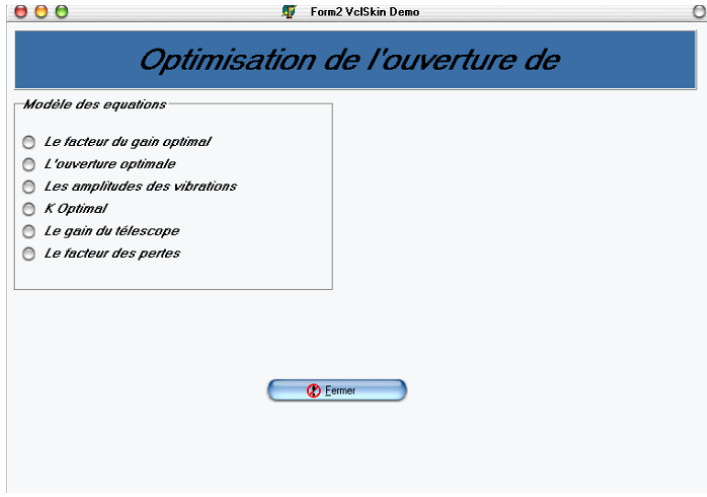


Figure 10.14. *Optimization of the telescope opening*

This window is itself broken down into six parts. Activating each button adds a new window just next to it which captures the data essential for obtaining the curves.

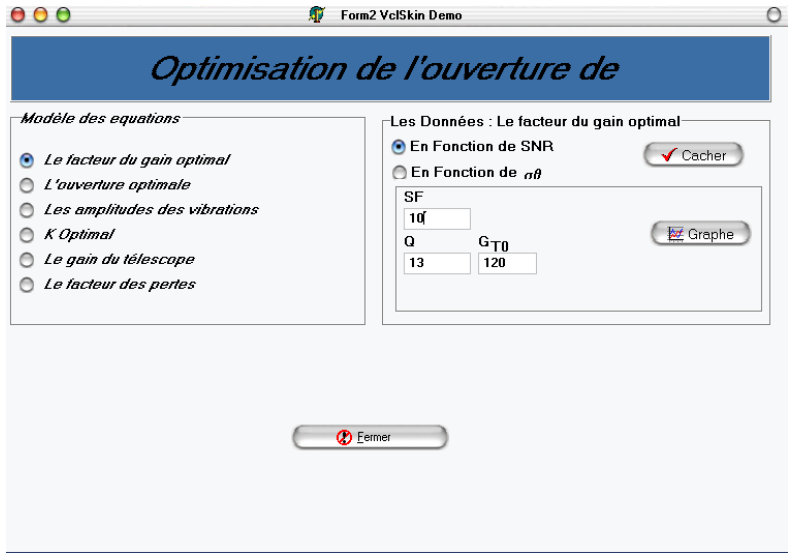


Figure 10.15. *The data*

The optimal gain factor

– Depending on the SNR:

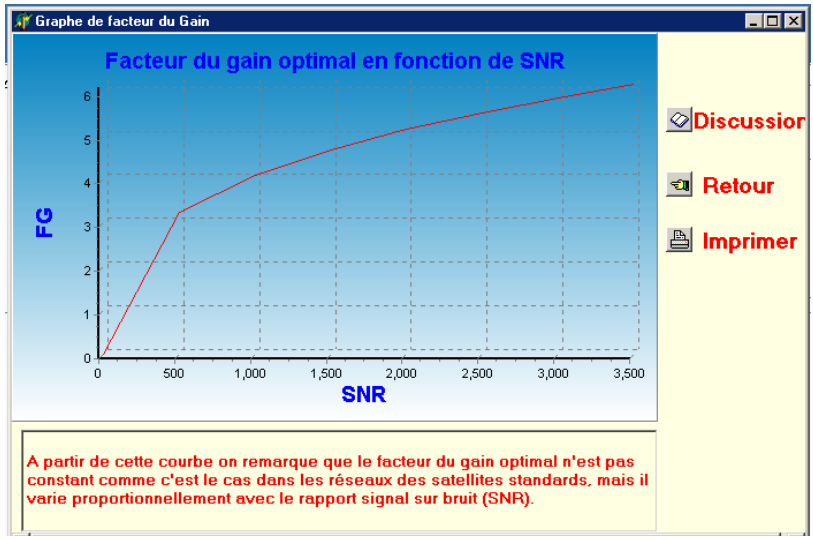


Figure 10.16. *Optimal gain factor depending on the SNR*

– Depending on the vibrations' amplitudes:

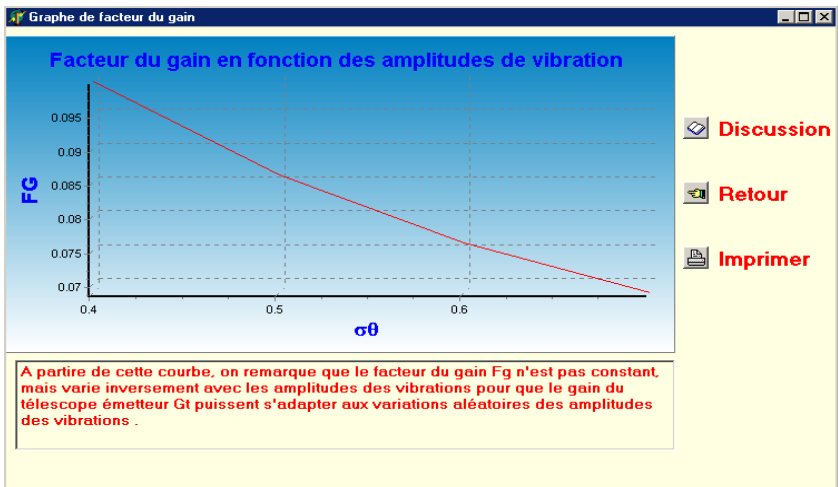


Figure 10.17. *Gain factor depending on the vibrations' amplitudes*

Optimal opening

After entering the data, we should click on the Graph button, and the following figure can be seen.

The optimal opening depending on the SNR:

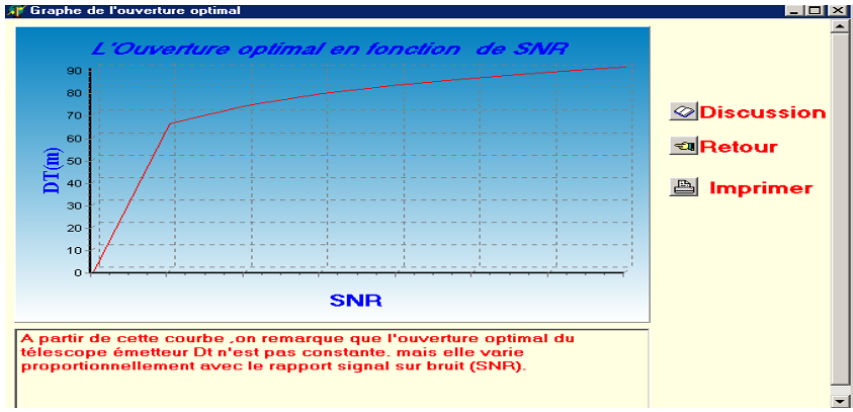


Figure 10.18. *The optimal opening depending on the SNR*

Depending on the σ_θ:*

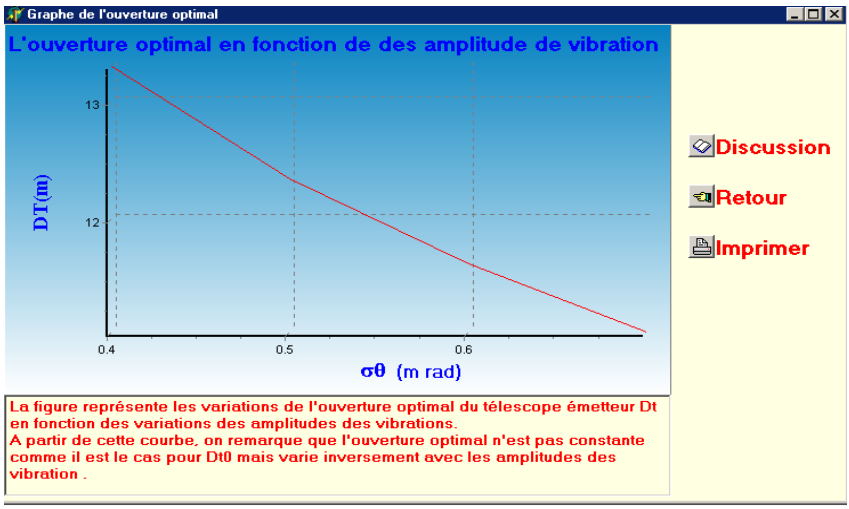


Figure 10.19. *The optimal opening depending on the* σ_θ

The vibrations' amplitudes

– Depending on the SNR:

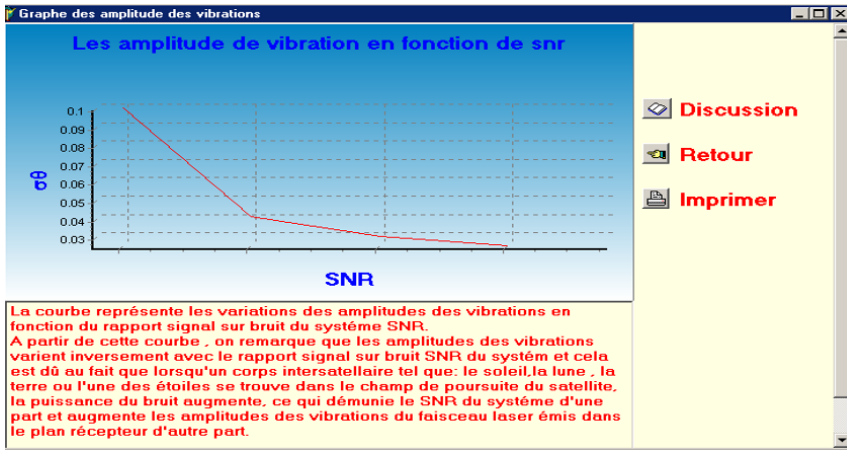


Figure 10.20. *The amplitudes depending on the SNR*

Optimal K depending on S:

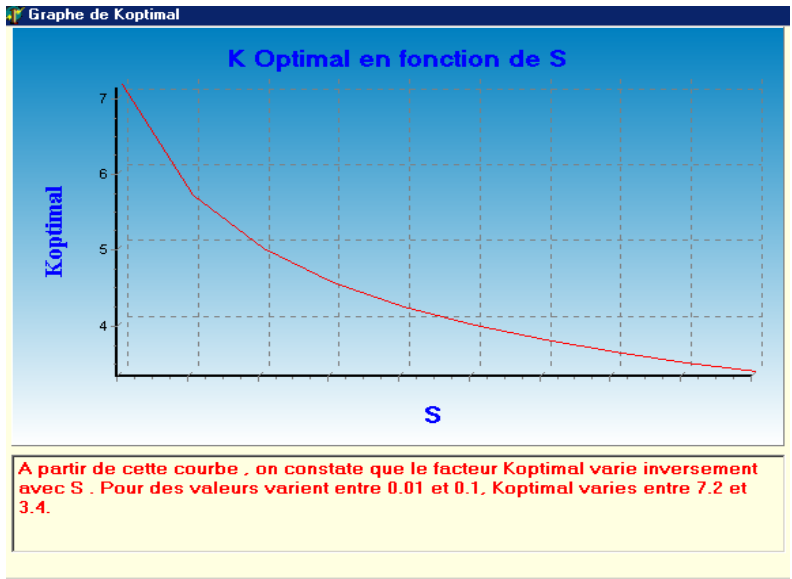


Figure 10.21. *Optimal K depending on the SNR*

The telescope's gain depending on the SNR

If we click on the graph button, the following window will be displayed.

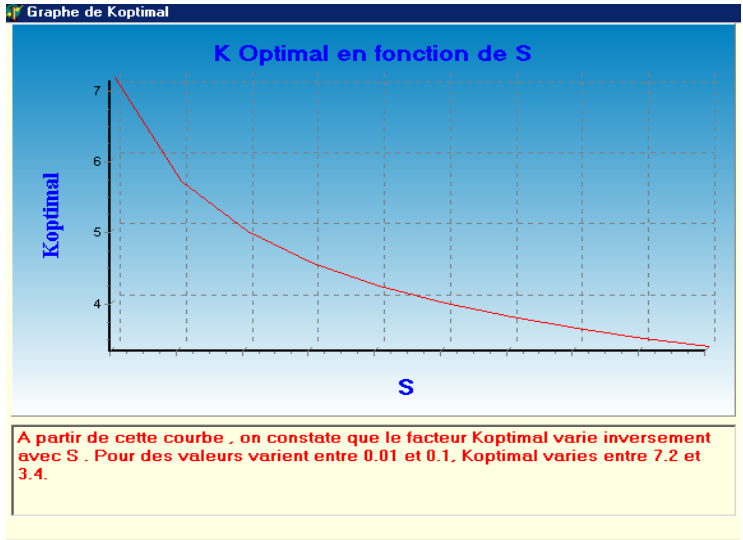


Figure 10.22. *The telescope's gain from the transmitter depending on the SNR*

The loss factor

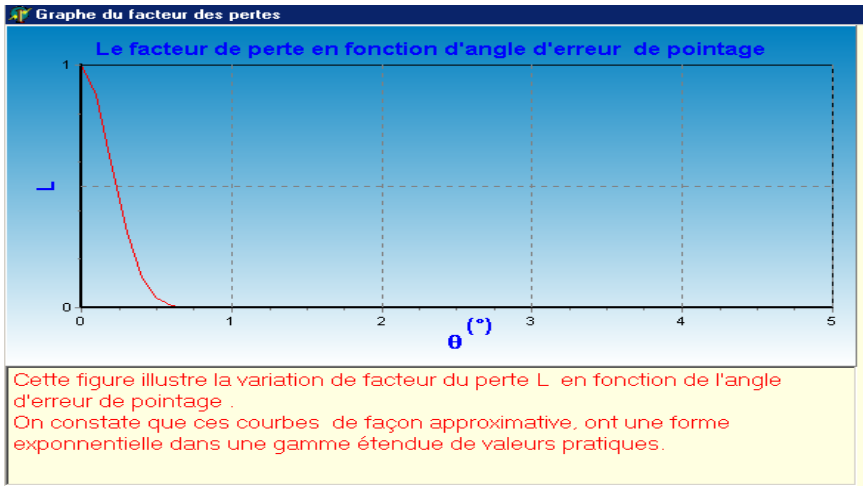


Figure 10.23. *The loss factor (L) depending on the pointing angle error*

Activating this enables a window to be displayed, containing all the explanations on the symbols that have been used when running the software, as well as some directions for imaginary use of the different options.

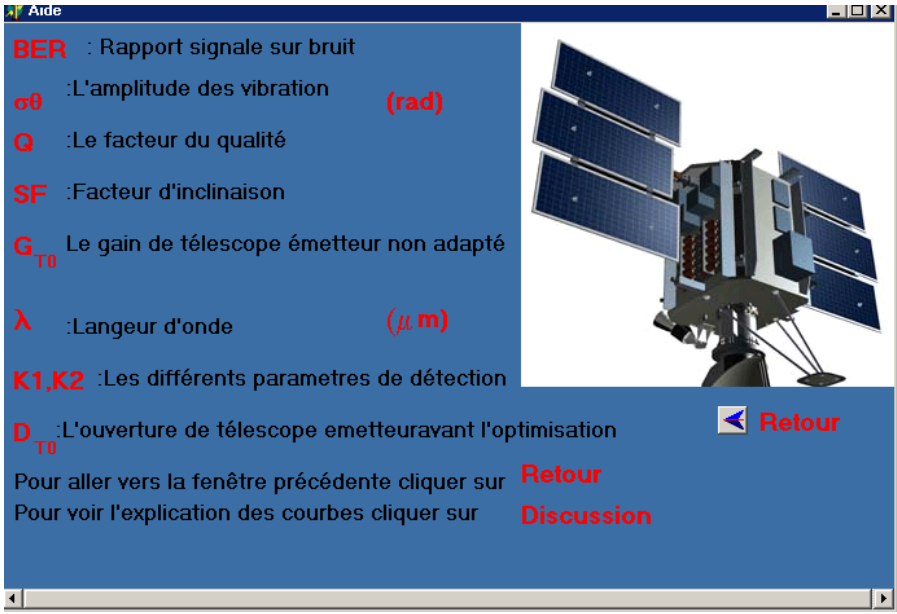


Figure 10.24. *Summary*

The software is enhanced by images – synoptic diagrams and photos – that give a general overview of laser satellites.

11

Quantum Cryptography

Quantum cryptography is not in itself a new cryptography procedure. In fact, it does not directly enable intelligible messages to be communicated, but it does (mainly) enable the distribution of quantum keys, which often leads to quantum key distribution being known by the more general term of quantum cryptography. It therefore appears as a component of classical cryptography, as it meets its requirement for private key distribution.

The security of this method relies on the laws of quantum mechanics and is considered to be unconditionally safe.

Anton Zeilinger's team (at the Institute for Quantum Optics and Quantum Information at the University of Vienna, Austria) recently presented a study stating that they have demonstrated a "quantum teleportation" over a distance of 143 km in the Canary Isles. If this is confirmed, this distance record establishes a new tier in the world of quantum teleportation and also opens the way for a future global quantum network dedicated to secure communications by satellite.

Researchers from the University of Sciences and Technology of China, in Shanghai, stated that they had demonstrated quantum teleportation over a distance of 97 km across a lake in China. Quantum teleportation does not involve matter; it is rather the process of transferring the exact information about a particle, from one area to another, using quantum entanglement. The particle does not travel through the intermediary space. The Chinese demonstration of quantum teleportation confirmed that 1,171 photons have been teleported in 4 h, registering a loss of 35–53 dB over a distance of 97 km. The Austrian demonstration has confirmed that 605 photons have been teleported in around 6.5 h, registering a loss of 28–39 dB over a distance of 143 km. The DARPA requires the researchers to demonstrate a sustained transmission of secure quantum keys at the rate of 1–10 Gb per second, at distances of 1,000–10,000 km, *a real quantum leap* (…).

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

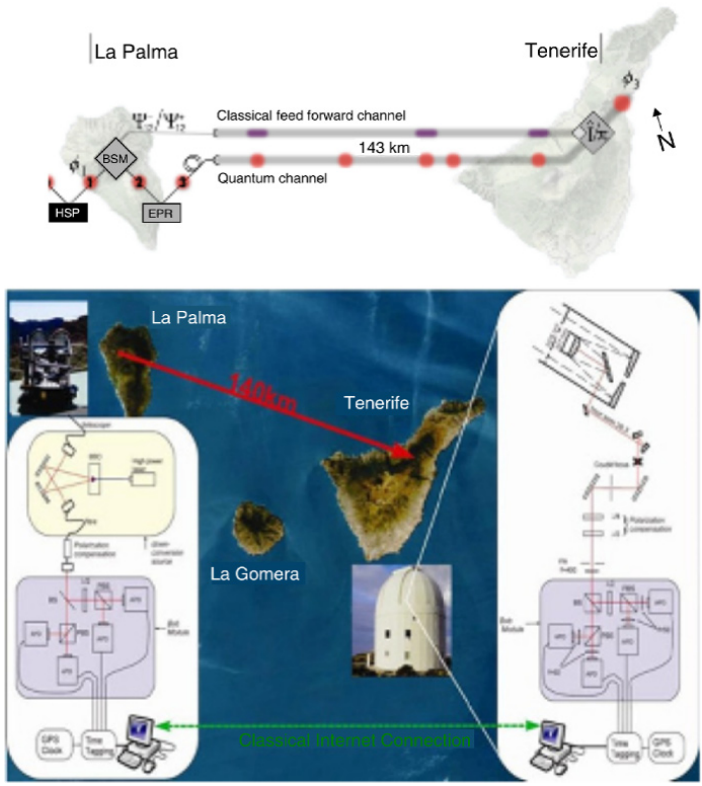


Figure 11.1. *Diagram of teleportation*

It also requires that the communications should not sustain any loss in the face of the environmental decoherence (quantum decoherence) that a contaminated atmosphere presents for any experiment. According to DARPA: "Current quantum communication technologies are very sensitive to loss, with an increase in the loss leading to a drop corresponding to the bit rates (for example, 10 dB of loss results in a decrease factor of 10 in secure flow). The programmers selected are meant to present a method for decoupling secure flow from loss".

The programmer has two secondary goals: to demonstrate, conclusively, that the security of quantum communications can be extended to new domains, even under water and in a vitiated atmosphere, and to extend entirely macroscopic quantum communications to new domains.

11.1. Cloning photons

In 1982, W. K. Wooters and W. H. Zurek demonstrated that it was impossible to clone an arbitrary and unknown quantum state [WOO 82].

As evidence, suppose that Eve were to have a quantum photocopier. By definition, the photocopier carries out the operation

$$|white> |\psi> = |\psi> |\psi> \quad [11.1]$$

With $|white\rangle$ the initial state of the photon that will serve as a "blank page". If $|\psi\rangle$ represents a horizontal polarization written $|H\rangle$, then

$$|white> |H> = |H> |H> \quad [11.2]$$

If $|\psi\rangle$ represents a vertical polarization written $|V\rangle$, then

$$|white> |V> = |V> |V> \quad [11.3]$$

If $|\psi\rangle$ is a linear combination of states $|H\rangle$ and $|V\rangle$, then the initial state of the photocopier is also written

$$|white> (\alpha|H> + \beta|V>) = \alpha|H> |H> + \beta|V> |V> \quad [11.4]$$

11.2. Quantum cryptography

11.2.1. *Introduction*

In general, a communication model is formed of a system, and involves an input data source on a routing support, and a receiver where the modulation and demodulation are produced [TAM 14]. The information is obtained from the source carriers. This is the initial information that uses symbols from the finite data set (alphabet, figures or equivalent) and the mode of transmission can occur either in a single stroke or transmissions at regular intervals [NIE 00].

In this case, each piece of data of a transmitted symbol does not depend on the previous ones [MAR 10]. The discreet channels transmit symbols from a specific set (input alphabet), and in their exit they generate another set of symbols (output alphabet) [GIS 07]. As the input alphabet and the output alphabet can be different, it is necessary to use a coding that maximizes the transmission's efficiency [MIG 09].

Fundamentally, the coding consists of allocating a specific word to each of the symbols in the input (built with elements of the output alphabet) [ARR 14].

This should be carried out by finding a mean length for the code to be reduced to a minimum, as well as a decoding unique to the receiver. Additionally, the channel is not generally ideal, the information received differs from the information sent, and this difference results in a probability of error in the behavior of the receiver; whose mission is simply to recover the original information, with the maximal fidelity possible [GIS 10].

In the quantum communication approach, the concepts mentioned above are still used, but with some profound changes. In the first instance, a quantum datum relates to the symbol generated by the input source. The meaning of the data through the channel is a Hilbert space (dimensions in qubits). Generally, it is also necessary that the source coding attributes a representation in the form of qubits to each state-symbol [SIN 03].

Secondly, any process linked to the data transmission that alters the data's state, is characterized by a super-operator [ZHU 03]. But in this case, the usual response is to include the behavior of the channel's noise, because of the interaction between the system and the (more or less active) environment in the input data. In channels without error, the pure state is associated with each symbol [NAT 15], whereas in noisy channels a mixed state is used. They are closed in quantum systems, formed of sub-systems linked to the information (open system) and the noisy environment [KHA 04].

11.2.2. *Methodology*

A quantum communication network is formed of the input source, a communication channel and the output, like the classical mode, and the data's security depends on all three stages of the communication. Current research shows that the data transmission mode depends on the channel's integrity and capacity [GLI97]. From classical information theory, we have bits that can be 0 or 1. In quantum information theory the equivalent is quantum bits or qubits [GIS 10]. These are two dimensional quantum states.

We can code the bits as qubits using orthogonal states, with the notation 0 and 1 [NAT 15]. According to classical information theory, we have bits that can be 0 or 1. In quantum information theory, the equivalent is quantum bits or qubit [GIS 10]. These are two dimensional quantum states. We can code the bits as qubits using orthogonal states, with the notation 0 and 1 [NAT 15].

The advantage of qubits is that they can be in superposition and through the channel during the transmission of data; the combiner combines the orthogonal polarization data by directing them through the correct channel [SIN 03]. However,

the combiner and the divider can differentiate the polarizations only by a finite value, by introducing cross-talk [GLI 97]. This means that a small part of the pulse addressed can still inject, and vice versa.

In a balanced interferometer, this would cause interference, since a small part would then be modulated, that should not have been and vice versa. In this configuration where the interference is unbalanced, the optical path length difference creates pulses that leave the transmitter and arrive at the receiver with a time lag [GLI 97]. This directs the cross-talk to arrive in the coupling channel at different moments to identify the data signal required. The converted wave network or a wavelength converter is a device that enables a wavelength's signal to be converted to another wavelength.

In optical networks, that do not have wavelength converters, each message can only be activated from a certain wavelength to an input port with the same wavelength on an output port [NAT 15]. Although wavelength converters improve the network's performances, it is well known that all optical wavelength converters are costly [GLI 97].

$$\text{Function } [Px, Py] = \rho xy\text{NonUPhase}(1, 2, N) \qquad [11.5]$$

Equation [11.5] shows the representation of non-uniform data transfer along a channel

$$\text{Function } [Px, Py] = \rho xy\text{UPhase}(1, 2, N) \qquad [11.6]$$

Equation [11.6] shows the representation of uniform data transfer along a channel where Px is the data path probability at axis X, Py the data path probability at axis Y and ρ represents the concentration of data.

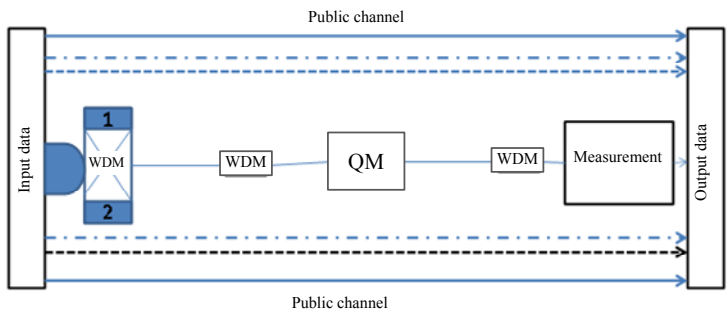


Figure 11.2. *Schematic of network supporting QKD and WDM channels.*

11.2.3. *Results and discussion*

A system and a process for a quantum distribution of keys on a network (WDM) are represented in Figure 11.2. The quantum bit error (QBER) depending on the propagation distance in km, the channels are varied between -10 and -30 dBm. The transmitter can select a receiver among the receivers with which to communicate, and transmits quantum signals to the receiver selected on the WDM network. The primary results have been obtained by Djeffal and Benslama in [DJE 16].

Quantum signals have a wavelength equal to a reception wavelength, from the receiver. Consequently, the WDM network enables quantum signals to communicate between the transmitter and receivers with a wavelength routing. A communication network contains a plurality of nodes interconnected by an optical transmission medium. The transmission support is capable of supporting a plurality of wavelengths organized in bands. A filter at each node to pass a band linked to it, and passively transmits other bands via the transmission support [KHA 04].

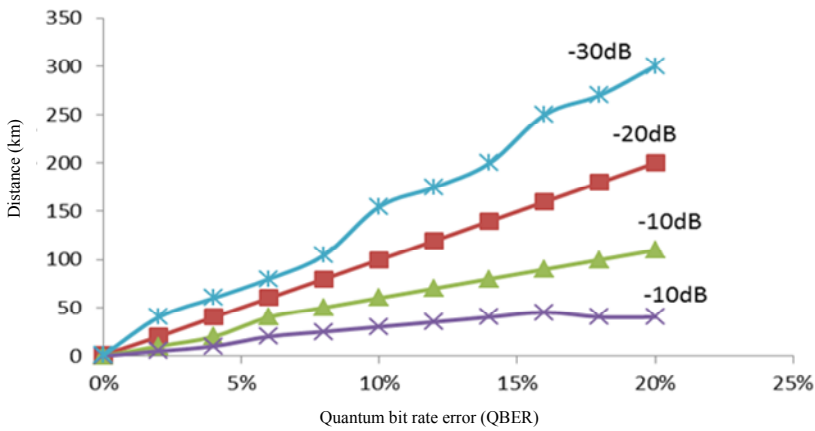


Figure 11.3. *QBER response as a function of the propagation distance. For a color version of this figure, see www.iste.co.uk/benslama/quantum.zip.*

A device is provided at each node to add a band to the transmission support. Communication can be established directly between a pair of nodes in the network that share a common band without the active intervention of an intermediary node. This enables the network to be independent of the protocol. Additionally, the low losses sustained by the passive filters enable there to be a relatively long path without optical amplification.

Figure 11.4, shows the key generation rate, which is the quantum bit rate depending on the straight-line distance with the transmission parameters and before reduction of the transmission distance. The maximum transmission is around 6 km which is expected, the rate is of stable amplitude, whereas the minimum is obtained for the exchange of random or fluctuating data.

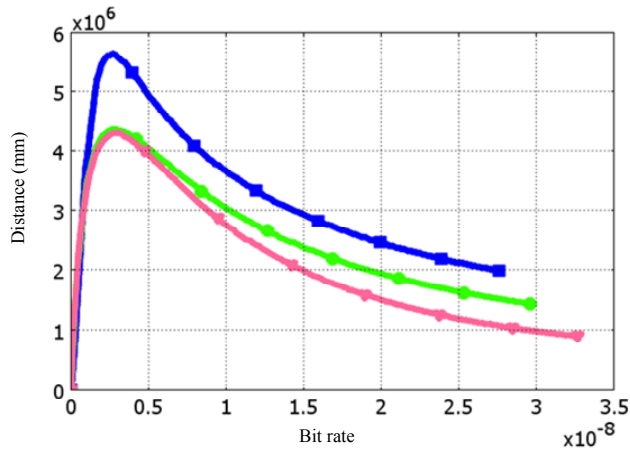


Figure 11.4. *The bit rate as a function of distance. For a color version of this figure, see www.iste.co.uk/benslama/quantum.zip.*

The difference between the random and uniform phase is entirely evident so although the two are traced, only the uniform data phase is visible and reaches a long distance. As mentioned above, the maximum transmission distance is reached at a rate of around 6 km, with a lower bit rate around 2.5×10^{-7}. This is in agreement with the general principle of congested and decongested phenomena; if the channel is entirely occupied by the random data, the channel will certainly be weak, also because the data are entirely limited to distance travel [SIN 03, NAT 15]. To find the maximum transmission key generation rate, the bit flow for each distance has been calculated for all the models found and it can be seen that the stable amplitude gives the best key generation rate [KHA 04].

For a variable amplitude, the non-random fluctuations seem the best adapted. For the same maximum transmission distance, they give a rate of around 2.5×10^{-7}. The reason for this could be that at least one of these values is the optimal value. Consequently, the many pulses will be of non-optimal amplitudes, which have the lowest rate. The random fluctuation gives a lower rate for all the distances, and a shorter maximum distance. In the presence of random fluctuations, the model has no prior knowledge of the amplitude.

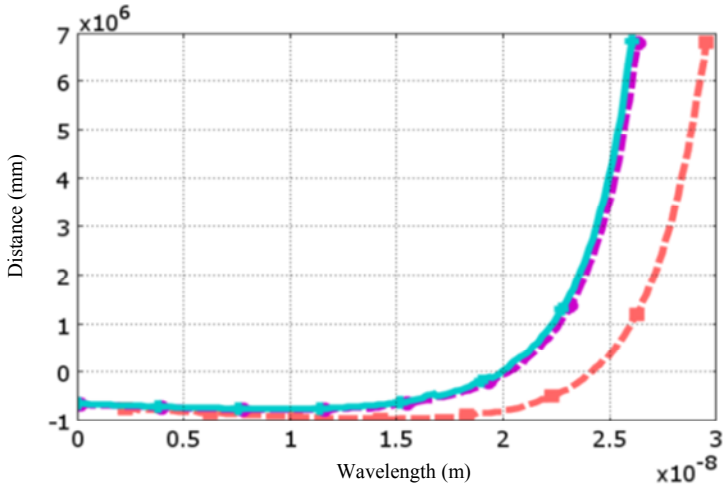


Figure 11.5. *Wavelength dynamic. The distance coverage increases with the decrease in wavelength. For a color version of this figure, see www.iste.co.uk/benslama/quantum.zip.*

The different quantum key distribution wavelengths (QKD) are measured depending on distance in kilometers, as illustrated in Figure 11.5. The quantum bit rate error depends largely on the channel's integrity and the operating system on the same medium as the conventional, between 200 and 250 nm of the channel's wavelength, fast distance coverage has been noted for three models and a single model exceeds the operating system in the same band close to 250 nm and of course, when the wavelength increases. It is foreseeable that the distance coverage should increase, although for all the models with the best performances from the furthest distance, it is from the classical signal as the wavelength increases [KHA 04]. It can be inferred that the main wavelengths with optimum quantum distribution function are found in the region above 250 nm.

Figure 11.6 shows a communication system for quantum key distribution with a relatively simple structure and great efficiency in communication for 4 different users with a different transmission flow. The system provides a quantum key distribution between a transmitter and several receivers on a network (WDM) with the wavelength routing it comprises. It has been identified by attributing a receiver with different wavelength for each of the receivers, or selecting one of the receivers to communicate with the transmitter and the transmission of quantum key signals from the transmitter to the receiver selected on the WDM network. The four receivers are situated at 300 km in which the quantum key signals are on a wavelength identical to the reception of the receiver's wavelength on Figure 11.6.

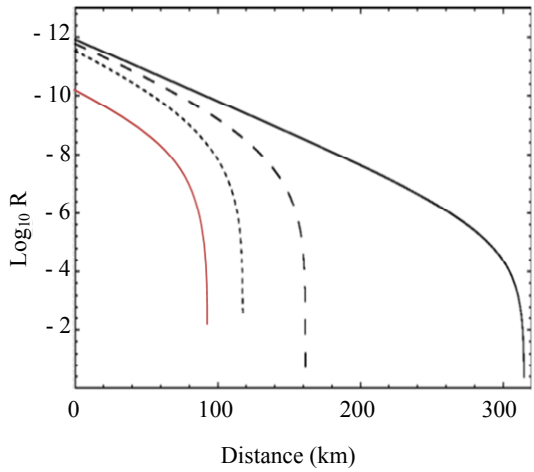


Figure 11.6. *The $Log_{10}R$ function of transmission rates depending on distance*

The communication system is formed of a transmitter and several receivers, each receiver having a distinct wavelength; and a WDM network linking the transmitter to the receiver, the transmitter selects in the receiver, one of the receivers with which to communicate, and transmits quantum signals from the selected receiver on the WDM network. The quantum signals are transmitted on a wavelength equal to the reception, from the receiver and this distance can be covered by the channel's precision.

According to Figure 11.6, a wavelength routing technology is used to implement the quantum key distribution for a plurality of receivers and can be identified in secure data communication. Wavelength routing can be carried out by a division of wavelength, which can be in the form of a waveguide network (AWG). Additionally, the system can be used, alternatively, linked by a means, which is adapted to the network's user. Again from Figure 11.2.5, continuous-wave light is used in the system, which can improve the system's security. Additionally, differential phase detection is also used and is one of the most important aspects in overcoming the influence of a change in parameter and phase shift in the system, which can also make the system simple and stable.

11.2.4. *Conclusion*

In general, the present study shows a communication system for a quantum key distribution network, the random and uniform phase-mode transmission has been studied for a stable amplitude. The results of the random phase have shown a

minimal distance coverage on the non-random phase. For the fluctuation in amplitude, random events show a change in the improved system's performances. Consequently, it is concluded that the rare fluctuations should not significantly degrade the system's performances, but the data transmission mode has a significant effect on the channel's integrity. Although the study has not emphasized the aspect of the chain's security, it can however be concluded that the non-random fluctuations should give a better performance than the random fluctuations.

It seems that it is better for mode 1 to share its information on the amplitude with a third mode, in which a transmitter can communicate via a classical quantum communication network with several receivers, by using a different secret key sent at a different wavelength for each different receiver.

11.3. Solutions to the practical limits of quantum cryptography

11.3.1. *Introduction*

Noise in quantum communications is basically asymmetrical: phase error is much more probable. Despite considerable progress in quantum encryption, many questions remain to be answered and many problems can only be solved using current technologies (quantum noise). In order for quantum cryptography to become an effective method on a large scale, we should introduce some coding techniques into protocol BB84.

This very point is the aim of our work. We will try to develop a method of quantum error correction based on error correcting codes in order to pair them with purely quantum theories to create a quantum error correcting code so as not to lose information, or to ensure that communication is maintained between Alice and Bob.

11.3.2. *Theoretical considerations*

Security requirements in quantum transmission depend strongly on its nature. It is clear that quantum distribution requires security mechanisms to be implemented in order to restrict access to cryptographically distributed content only to the application's legitimate clients for a set amount of time. We suggest analyzing specific needs for large-scale commercial applications in the belief that the solutions provided for these applications can be used for applications whose security needs are more flexible.

The main needs of quantum communications in terms of security can be summarized in three points:

– Authentication: The source should be able to provide a mechanism to check the origin of the packets sent for the possible risk of identity theft. This need is vital above all for applications where the data is quantum (photon). The receiver should also be able to ensure that the data received have not been altered during transmission (this is described as integrity).

– Confidentiality: Only authorized clients should have access to data content and this access is only authorized for a length of time agreed beforehand.

– Protection against denial of service: Denial of service attacks aim to prevent legitimate clients from accessing the service. The service provider should therefore be able to minimize the impact of this type of attack on legitimate clients.

These three security requirements are not new and several solutions have already been proposed and are used in the context of quantum communications. However, the current solutions cannot be applied directly in the context of quantum communications for satellite networks for reasons described in the following section.

11.3.3. *Practical considerations*

When creating a quantum system, certain practical considerations complicate the use of protocol BB84.

– Light pulses containing exactly one photon are technically difficult to produce.

– Photo-detectors are not 100% efficient and can be disrupted by quantum noise.

– During reception, we need to consider the problem that creates incoherences between Alice and Bob: the choices of basis (H/V) which rely on Heisenberg's uncertainty principle.

– Spying: The protocol demands that Alice and Bob delete their data as soon as they identify an error (the "resetting" from protocol BB84).

– The security of a quantum key distribution system is assessed by calculating its quantum error rate. It is necessary for an error rate to be less than 11% in order to guarantee the confidentiality of a key transmission. The error rate depends on the characteristics on the components used and is a function of the length of the quantum channel.

11.3.4. *Quantum noise*

11.3.4.1. *Noise from quantum uncertainty*

In quantum mechanics, Heisenberg's uncertainty principle relies on it being impossible to observe two non-commutations at once (a certain value at the same time). For example, in a state of the electromagnetic field in which energy is well-defined, the amplitude field cannot take a certain value. This is true, in particular, in the electromagnetic vacuum (that is to say, in the total absence of light) when the measurable energy is strictly equal to zero.

Because of the uncertainty principle, however, the amplitude domain cannot also take the value zero, but must fluctuate at random. These fluctuations in the void are very important for optical telecommunications, as they are a fundamental source of noise, which contaminates an optical signal at each stage of its life, its creation, propagation and distribution. As the subject of the quantum noise is the limit of quantum communications, here we will very briefly study an example of quantum fluctuations in different features of quantum telecommunications [KNI 01].

11.3.4.2. *Quantum noise in signal generation*

Fluctuations are visible in spontaneous transmissions in the amplifiers and lasers used in optical communications, through which the energy stored in the laser's active medium is emitted as light through the emission of photons. The transmission should be triggered by the fluctuations; this phenomenon, which is the first photon that triggers the stimulated transmission, characterizes the laser output power, which is coherent and directional. However, the light transmitted is incoherent and directional, therefore, with the exception of triggering the emission it stimulates, it represents a mechanism for energy loss and a source of excess phase and amplitude noise for optical amplifiers and lasers.

An ideal laser transmits a coherent light which is a wave with relatively well-defined amplitude and phase, while a photodiode detects the energy.

The process of detecting light is faced with two different variables (the amplitude and the number of photons), which, according to quantum mechanics, are not compatible. Thus, one of the consequences of noise is to fix a minimum amount of energy for detection errors. Furthermore the static Poisson demands the detection of tens of photons to obtain a signal acceptable to the noise.

11.3.4.3. *Spying*

To obtain information on the secret key that Alice and Bob are attempting to exchange, Eve must intercept the photons sent by Alice, then, for each of the photons intercepted, measure its polarization according to one of the two bases,

rectilinear or diagonal, and finally send a new polarized photon to Bob for each photon intercepted. This attack is practically impossible to carry out with any success, and the calculation power available to Eve is therefore of little importance.

In fact, just like Bob, Eve must decide, for each photon intercepted, to measure its polarization according to one of the two bases, and just like Bob, Eve ignores the basis chosen by Alice. Thus, because of Heisenberg's uncertainty principle and because the two bases form a pair of complementary properties, any spy making this attack runs the risk of introducing incoherences in Alice and Bob's data. If any eavesdropping has taken place, Alice and Bob should then restart the initial protocol.

11.3.5. *The QBER in quantum transmissions*

The performance (detectability, confidentiality, etc.) of a quantum key distribution is evaluated by calculating the QBER. This rate is defined as the ratio between the number of erroneous bits detected by Bob, written $N_{erroneous}$, and the total number of bits detected by Bob, written N_{total}. The total number of bits detected is the number of bits used by the key, written N_{key}, and the number of erroneous bits [LAW 97].

$$QBER = \frac{N_{erroneous}}{N_{total}} = \frac{N_{erroneous}}{N_{erroneous} + N_{key}} \qquad [11.7]$$

The number of erroneous bits and the total number detected can be expressed in terms of the transmission flow.

$$QBER = \frac{R_{erroneous}}{R_{erroneous} + R_{key}} \qquad [11.8]$$

11.3.5.1. *Losses in the quantum channel*

The probability that a photon transmitted by Alice is detected by Bob depends on the losses in the quantum transmission channel and the optical losses from Bob's module. The greater these losses are the greater the probability that the photon is absorbed before arriving at the photon detectors. If the losses in the fiber between Alice and Bob are expressed in dB, then the probability of the photon being absorbed by the fiber is:

$$\eta_{fiber} = 10^{\frac{l.\alpha}{10}} \qquad [11.9]$$

with (l) the length of the fiber forming the quantum channel and (*fiber*) its loss coefficient per unit of length.

Bob's module unites several optical components that have insertion losses and each of them increases the probability that the photon will be absorbed before arriving at the detectors. However, only Bob's modulator shows enough loss to be taken into account. η_{Bob} is the probability of Bob's module absorbing the photon.

$$\eta_{Bob} = 10^{\frac{l.\alpha_{Bob}}{10}} \qquad [11.10]$$

Thus, the flow of photons detected by Bob before basis reconciliation is expressed:

$$R_{raw.key} = f_{pulse}.\mu\eta_{fiber}.\eta_{Bob}.\eta_{\det ector} \qquad [11.11]$$

where f_{pulse} corresponds to the frequency with which the optical pulses containing an average of μ photons are generated, and $\eta_{detector}$ is the detector's quantum efficiency.

By definition, the key's stream of formation after reconciliation corresponds to half the flow of formation of the raw key.

$$R_{recon.key} = \frac{1}{2}.R_{raw.key} \qquad [11.12]$$

11.3.5.2. *Contributing factors to QBER*

Three error factors contribute to QBER:

a) the detectors' dark count;

b) the interferometer's contrast;

c) the detectors' afterpulsing.

a) The first contribution comes from the photon counter, which can be triggered without a photon being present. This phenomenon is called a *dark count* and characterizes the quality of a photodetector, formed of an avalanche photodiode. The error generation rate resulting from the *dark count* is expressed as:

$$R_{dark} = \frac{1}{2}.f_{pulse}.P_{dark}.n\ .\mathrm{n} \qquad [11.13]$$

with n the detector number, P_{dark} the probability that there will be a *dark count* from the detectors during the observation time. The first factor ½ expresses the fact that a *dark count* can occur when there is an anticoincidence of the bases (the bit is therefore eliminated during the reconciliation of the bases). The second factor ½ expresses the fact that a detector can be triggered by the effect of a *dark count*, and not by the arrival of a photon, when there is a coincidence of the bases (the bit is made countable to form the refined key).

b) The second contribution reflects the fact that a photon with a given phase value may not be detected by the detector with the corresponding eigenvalue. When there is a coincidence of the bases, the interferences' phase values do not coincide exactly with the detection system's eigenvalues, thus causing errors. The flow of this contribution is:

$$\begin{aligned} R_{contrast} &= R_{key}.P_{constrast} \\ &= \frac{1}{2}.f_{pulse}.\mu.\eta_{fiber}.\eta_{Bob}.\eta_{\det ector}.\frac{1-C}{2} \end{aligned} \qquad [11.14]$$

where C represents the interferometer's contrast.

c) The phenomenon of *afterpulsing* is an accidental triggering of an avalanche during the avalanche photodiode's reloading phase. However, if the photodiode's avalanche recharging time is long enough, the probability of this phenomenon appearing is negligible. A compromise therefore exists with the detection frequency.

11.3.5.3. *Expression of the QBER*

From equations [11.13] and [11.14], the error flow is expressed as:

$$\begin{aligned} R_{erroneous} &= R_{contrast} + R_{dark} \\ &= \frac{1}{2}.f_{pulse}.\mu.\eta_{fiber}.\eta_{Bob}.\eta_{\det ector}.\frac{1-C}{2} + + \frac{1}{2}.f_{pulse}.P_{dark}.n \end{aligned} \qquad [11.15]$$

The QBER in a quantum channel transmission can be deduced from equations [11.7], [11.8] and [11.11],

$$QBER = \frac{\mu.\eta_{fibre}.\eta_{Bob}.\eta_{\det ecteur}.\left(\frac{1-C}{2}\right) + \frac{1}{2}.P_{darck}.n}{\mu.\eta_{fibre}.\eta_{Bob}.\eta_{\det ecteur}.\left(\frac{3-C}{2}\right) + \frac{1}{2}.P_{darck}.n} \qquad [11.16]$$

11.3.5.3.1. Evaluating the QBER

According to expression [11.16], the quantum error rate is a function of the average number (μ) of photons in a pulse and the contrast *C* of the interferometer. We will evaluate the expression of the *QBER* for different values of μ.

a. D.1/QBER (μ = 0.1)

Figure 11.7 and 11.8 show, for different values of the contrast *C* of the interferometer, an estimation of the channel's error rate depending on its length, in the absence of any eavesdropper. In fact, the detection device consisting entirely of fiber, it is difficult to control the phase fluctuations in the optical fibers linking each detector. The direct consequence of these fluctuations is a variation in the interferometer's contrast.

Several measurements have been carried out and give a value for the contrast oscillating between [0.7] and [0.9].

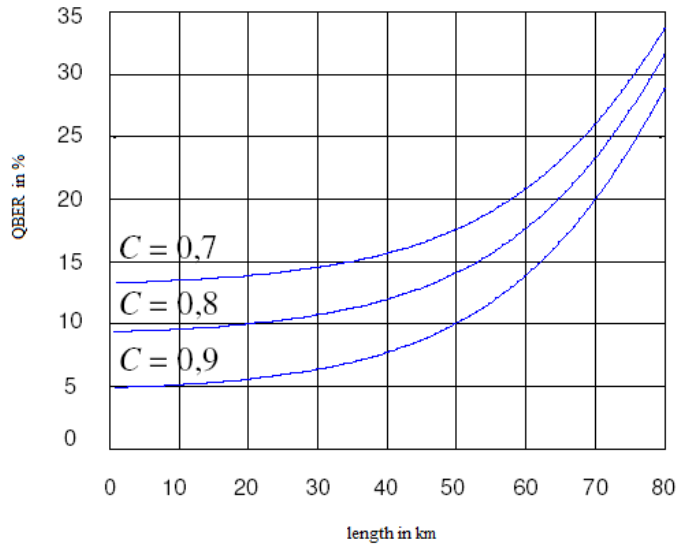


Figure 11.7. *Error rate as a function of contrast C*

In the worst case, the value of the contrast is 0.7. In this case, the error rate is higher than 13% whatever the channel's length, which does not guarantee unconditional security.

The average value of our detection system's contrast is 0.8. Figure 11.7 shows an evaluation of the error rate in this instance.

A transmission's confidentiality is therefore guaranteed, since the error rate is less than 11% when the channel's length does not exceed more than 30 km. In the best cases, the contrast's value is 0.9. The goal of a transmission is to form an encryption key that can be considered to be confidential so long as the channel's length does not exceed 50 km.

By modifying the interferometric equipment in order to refine its contrast with the help of a phase-lock loop, it is possible to approach a quantum key distribution system's usual values. These contrast values are higher than 0.95.

Figure 11.8 shows an estimation of the quantum error rate for the contrast values for {0.95, 0.96, 0.97, 0.98, 0.99}.

A transmission's confidentiality is therefore guaranteed for a channel with a maximal length of 60 km.

b. D.2/QBER ($\mu = 0.5$).

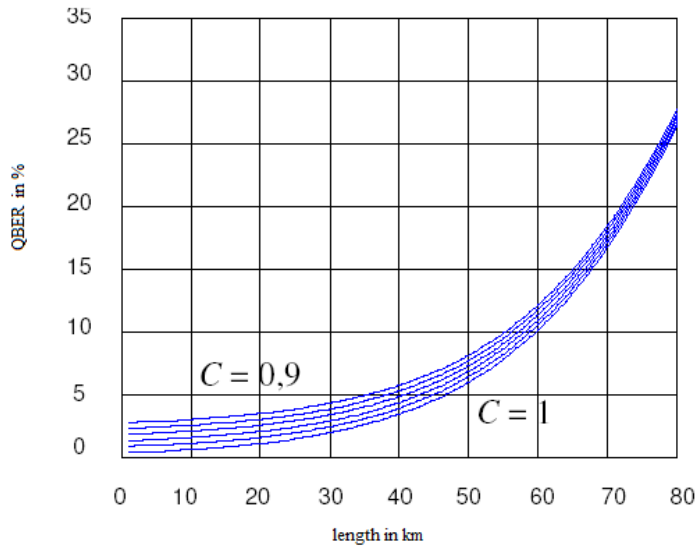


Figure 11.8. *Error rate (contrast between 0.95 and 1)*

By increasing the average number of photons per pulse, the photons' arrival rate on the detectors increases. The number of empty photon windows being lower, the *dark count* decreases. The consequence is an improvement in the error rate.

Figure 11.9 shows the estimation of the quantum error rate for different contrast values between 0.95 and 1.

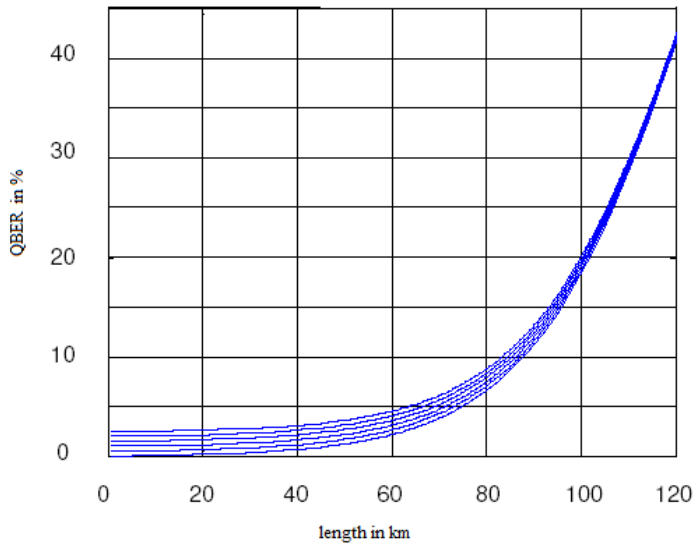


Figure 11.9. *Error rate (contrast between 0.95 and 1)*

Unconditional security is guaranteed when our device's quantum channel length does not exceed 83 km.

11.3.6. *Error correction methods in quantum cryptography*

The principle of quantum photo-detection (quantum detection) is extremely simple: it consists, with the help of a photon, of channeling the electron between a basis level, where it does not conduct electricity, and an excited level where it will. The pure semiconductor can for example act as a quantum photo-detector (Figure 11.10): in the basis state, it does not conduct the current, but a photon can create, via a photoelectric effect, an electron-hole pairing and place an electron in the conduction band, enabling the current to be transported [DE 97].

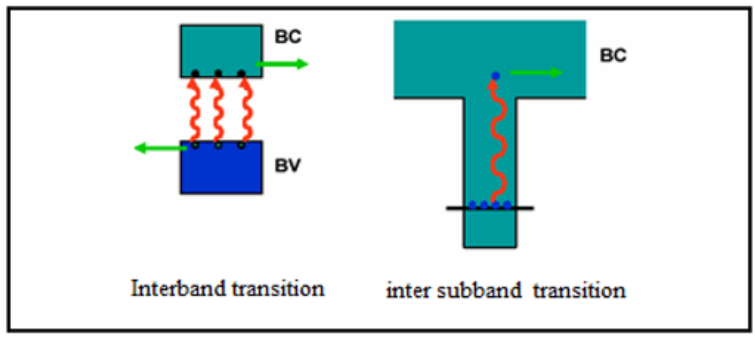


Figure 11.10. *Two quantum detection mechanisms. On the left, we use the band structure of a semiconductor. On the right, a quantum well*

A quantum well can also carry out this function, the electrons are trapped in the quantum well, as the AlGaAs barrier prevents them from leaving, but by absorbing a photon, the electrons will have energy to leave the trap and therefore to conduct the current.

11.3.6.1. *Single-photon transmission*

Light pulses of very weak intensity are needed in order to produce light pulses containing exactly one photon. These light pulses are very easy to obtain using a laser. Even if no interception has occurred on the quantum channels, the problem of these imprecisions necessarily involves incoherences in Bob's data. To resolve this problem, a single-photon source is needed [PEL 02].

The single-photon source is a key element in many potential uses for quantum mechanics. For example, a set of such sources, linked to linear optical elements (beam splitters) and photo-detectors, could be used to create a quantum computer. The simplest physical idea for creating a photon-emitting source "on demand" is to use an impulse excitation for a two-level quantum system. For each impulse excitation, the system transmits one and only one photon. Ideally, the single-photon source should have the following characteristics:

– A high repetition rate, and therefore a short life span for the dipole transmitter.

– A high quantum efficiency, all the impulse excitations are therefore transformed into single photons.

– Photon transmission in a single space mode with a defined polarization.

– A spectral width equal to Fourier transform of the impulsion duration.

– And of course, one photon at a time.

For quantum cryptography, the condition on the spectral width is not vital. Nevertheless, a fine spectrum enables us to isolate the light coming from the quantum system better from the surrounding noise. The transmission wavelength should be adapted to the propagation medium. For applications, the system is also required to be stable in time, simple to use, and ideally not expensive.

11.3.6.2. *Different sources*

Currently, essentially four types of single-photon sources can be identified that are used or sought in scientific laboratories:

– Quantum transmitters (molecule, atom, colored center, semiconductors), components capable of transmitting light pulses containing a single photon.

– Very much attenuated laser sources, so much so that on average, only one photon remains per pulse. These sources form an approximation; this is linked to the photons' arrival statistics in a standard laser source: it has been possible to reduce the average number of photons per pulse, but there will always be some pulses containing two photons or more. Because of the inevitable occurrence of pulses containing more than one photon, absolute security in a quantum link is only obtained in a very limited space domain (range).

– Twin photon sources, in which one of the two photons serves only to trigger the detector that will receive the second photon. Otherwise, the detection of a photon can be used to assess the presence of the complementary photon. In this type of protocol, a single photon is essentially used for quantum communication, but the twin photon only enables the detector to be opened when is necessary, and thus decreases incidence of noise in the detector.

– Twin photon sources in which polarization-entangled or energy-time pairs are used are at the very heart of the quantum communication protocol.

11.3.7. *The correcting code for error correction in BB84*

During reception, it is necessary to consider the problem that the incoherences between Alice and Bob cause: the choice of basis (H/V) which relies on Heisenberg's uncertainty principle.

To solve this problem, it is necessary to add an additional stage to the protocol that enables Alice and Bob to correct their errors under the same conditions, the elaborate correcting code is a method developed from the *Vernam Cipher*.

11.3.7.1. *Vernam cipher*

The *Vernam cipher*, also called the *Vernam one-time-pad* uses shift encryption but with modulo 2 in place of modulo 26. Binary arithmetic or the exclusive OR (XOR) is defined as [VER 26]:

⊕	0	1
0	0	1
1	1	0

Gilbert Vernam invented this encryption in 1926 to encrypt and decrypt telegraph messages. So that this system can be unconditionally secure, three requirements are placed on the key.

– The key should be as long as the message. A secret bit is therefore necessary to encrypt each bit in the message.

– It should be entirely random.

– Each key should be usable once and only once, hence the name *onetime – pad*.

Here is the detail in the Vernam method: Alice wishes to communicate the message m to Bob. She has a key k, of the length m, which is secret and shared by Bob. Alice obtains the cryptogram $e_k(m) = c$ by bit by bit modulo 2 addition and the message and the key, which is $c = m \oplus k$.

As for Bob, after receiving the cryptogram, he obtains the message by performing the same operation, which is $c \oplus k = m \oplus k \oplus k = m$. As the key is completely random, each bit of the cryptogram is, too. This system confirms the Shannon theorem, which states that knowing a cryptogram does not provide any information on the message.

Of course, we cannot use the same key twice in case of the following attack:

– Eve (spy) generates a message m and asks Alice (sender) to encrypt it.

– Eve receives $c = m \oplus k$ *from* Alice.

– Eve can now calculate the key $k = c \oplus m$.

– Then Eve can decrypt all the messages encrypted with the key k.

The main drawback and the essential difficulty to be resolved, for this encryption method to be in practice, lies in the fact that the key cannot be reused and the process of generating it in secret can only be secured by conventional means such as a planned meeting between Alice and Bob, or indeed by using an trusted messenger. Consequently, implementation over a long distance and for a large number of participants requires too many resources and security would be difficult to guarantee. Up to the present, keys have been transported by means of a diplomatic bag, even though this channel is not totally foolproof. Until recently, this encryption found applications mainly in the military and diplomatic services. As will be seen in the next section, the difficulty of distributing secret keys can be removed by virtue of quantum key distribution.

An example of transmitting an encrypted message using Vernam encryption is shown below. The key is absolutely random and identical for encryption and decryption.

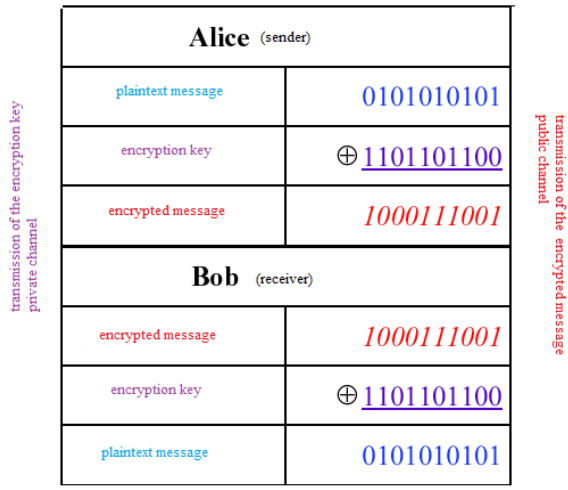


Figure 11.11. *Example of an application for Vernam one-time-pad encryption*

11.3.8. *Time coding for error correction in BB84*

We suggest protocols for quantum key distribution based on a time coding. They rely on single photon pulses limited by the Fourier transform. We use the product of the time–frequency uncertainty that results from it and which has a non-null value dependent on the pulse's shape. In the examples that we describe, we use coherent pulses whose time profile is rectangular and has the duration T. The coherence length is therefore equal to c_T.

The benefit of time coding lies mainly in the simplicity of using it in experiments. The amplitude modulators created in integrated optics have bandwidths able to reach 40 GHz. It is therefore possible to produce pulses with ascent and descent times lasting much less than a nanosecond.

The photon counters can have response times of less than a nanosecond (300 ps for silicon counters). Moreover, the time it takes the pulses to travel in a fiber is a robust parameter, which is not very sensitive to the fiber's defects. The effects of group velocity dispersions are not noticeable in the range of nanoseconds. The effects of depolarization do not directly influence the pulses' shape or their moment of arrival.

Alice and Bob share a synchronized clock that enables them to synchronize the sending and detection of the pulses. In the simplest case of the two-state protocol, Alice sends pulses by choosing at random and with identical probabilities a delay of 0 or a delay of T/2 in relation to the clock's signal (Figure 11.12).

These two delays code bit 0 and bit 1. In order to determine the bit sent, Bob measures the moment the photon is detected with the help of a rapid photon counter. Depending on the window in which the detection is made, the result is ambiguous or nonambiguous. A detection in windows 1 or 3 enables Bob to know the bit sent by Alice. A detection in window 2 gives no information on the bit sent by Alice. Half the results are also ambiguous for Eve. Having detected a photon in 2, she has a one in two chances of resending a pulse different to the one received and therefore of creating an error in the key exchanged between Alice and Bob.

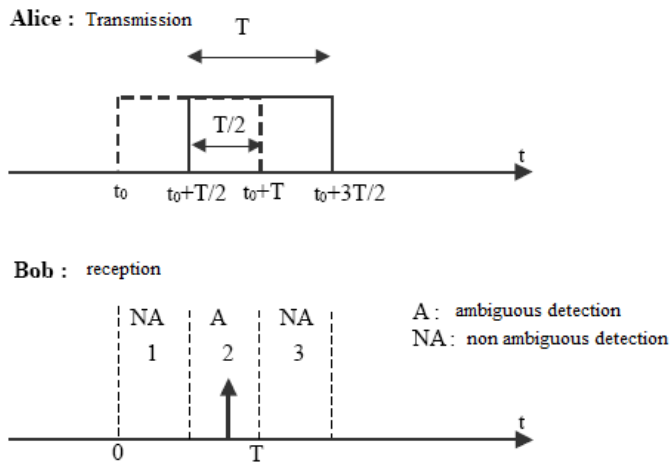


Figure 11.12. *Principle of the two-state protocol*

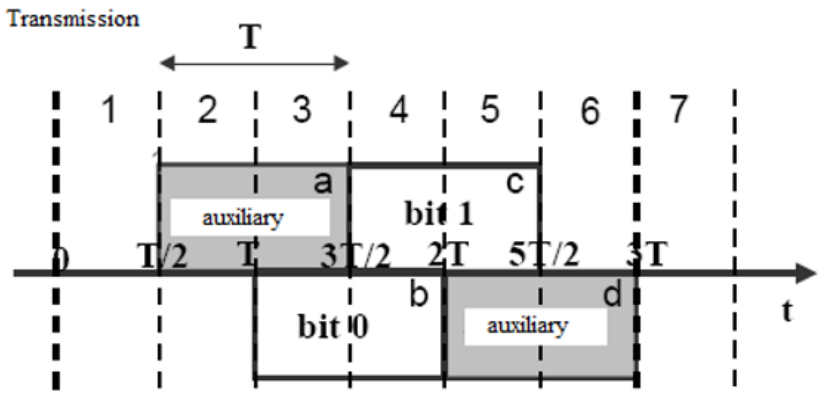


Figure 11.13. *Principle of the four-state protocol*

If the measurements are limited to the time domain, it is easy for Eve to make a perfect copy of the key without it being possible to detect her intervention. It is enough for her to resend a pulse of one photon of the duration T/2 centered on the time interval corresponding to its measurement result. All Bob's detections conform to the pulses sent by Alice and he is not able to detect the shortening of the pulses with a single measurement. Measurement of the average of the pulses received is carried out in the frequency space by means of an interferometer. Bob randomly send the pulses that he receives to a photon counter to establish the key or to the interferometer to measure the pulses' average duration. The two routes' propagation time differs by T/2 and their phase shifts by p. For perfect pulses, the probability of detection in one of the output channels is 0.75 and 0.25 in the other. The difference in the number of photons counted in each of the two channels normalized by their sum enables the contrast to be defined. The contrast's value depends directly on the pulses' average duration and thus makes it possible to trace it.

11.3.9. *Conclusion*

Protocol BB84 enables two partners, Alice and Bob, to communicate a secret cryptographic key to one another. But because of Heisenberg's uncertainty principle and the fact that the two bases form a pair of complementary properties, any spy carrying out this attack runs the risk of introducing incoherences in Alice and Bob's data.

To do this Alice and Bob use protocol BB84 with quantum key distribution using time coding or the quantum error correction method to exchange a secret key following this protocol with the same conditions.

Large-scale protection in quantum information is the aim of research efforts in our laboratory. We will therefore try to link this method with purely quantum theories for a long-distance quantum transmission.

11.4. Quantum error correcting codes

11.4.1. *Introduction*

Despite our need to be able to transmit and receive information on a perfect network, this network does not exist, whatever the diffusion by waves, or indeed wire. The data can therefore be altered slightly during a transmission, but a slight modification in a program can make it totally unusable, and a change in its data can corrupt it entirely. It is therefore necessary to find a means of detecting these errors as they occur, if they can be easily checked, or a means of correcting them, if data recovery is not easy. In Figure 11.14, there is a diagram of a transmission channel secured by an error correcting code.

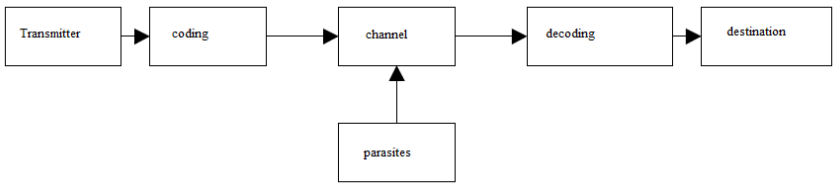


Figure 11.14. *Transmission of a message via a parasite channel*

A correcting code is a coding technique based on redundancy. It is meant to correct errors in the transmission of information (more often called a message) on an unreliable communication route, we will be interested mainly in the coding of digital signals, that is to say suites of 0 or 1, which are usually called bit suites. In the third chapter, I suggest integrating two elaborate coding methods to guarantee high security.

11.4.2. *Classical error correcting code*

In classical theory, the usual way of compensating the effects of noise on data storage or communication is to introduce redundancy in a sufficiently structured way. This is what is called error correction.

11.4.2.1. *The parity bit*

In the case of a DES key coded on 64 bits, 1 bit in 8 would not be used for coding, therefore leaving as many as 56 bits for coding the key. In fact, the eighth bit, which is called the parity bit, is the modulo 2, the sum of the seven others [HAM 50].

This system is extremely simple and only takes up a seventh of the space in the message that we wish to protect. However, its drawbacks outweigh its advantages [HAM 50]:

1) It only enables errors to be detected when there is an odd number of bits, (but it is true that more than one error in eight consecutive bits transmitted is fairly unlikely if a good quality channel is used).

2) If it detects an error, it is not possible to tell which bit it is located on, it is therefore necessary to recharge these eight bits (octet).

11.4.2.2. *Hamming code*

The Hamming code is an error correcting code based on the notion of the Hamming distance. Take an alphabet made up of four characters (00, 01, 10, 11). If an error occurs, then the character sent is transformed into another and there is no means of finding the original character. On the contrary, by adding information in such a way that the characters are very different from one another, this becomes possible [HAM 50].

11.4.2.3. *Repetition coding*

This coding consists simply of sending the same information several times in a row. If, for example, each bit is sent twice and an unequal pair is received, we know that an error has occurred, but cannot correct it. By contrast, if we send each bit three times and a single error appears, we will have a triplet formed of two identical bits and a different bit [HAM 50].

The advantages of this system are therefore the simplicity, as well as the possibility of error correction. But its main disadvantage is that it occupies several times the space of the message that is coded, which can be particularly awkward during the transfer of long files.

11.4.2.4. *Convolutional coding*

The principle of convolutional codes, invented by Peter Elias in 1955 [ELI 55], is not to cut the message into finite blocks, but to consider it as a semi-infinite

sequence $a_0a_1a_2\ldots$ of symbols that passes through a succession of shift registers, whose number is called a *code memory*.

To simplify, and also because it is the same for almost all the convolutional codes used, we will consider a case where the message is formed of bits.

In the example shown in Figure 11.15, it reaches the coder at instant t. The output bits will be $X = a_t + a_{t-1} + a_{t-2}$ and $Y = a_t + a_{t-2}$ (modulo 2 addition).

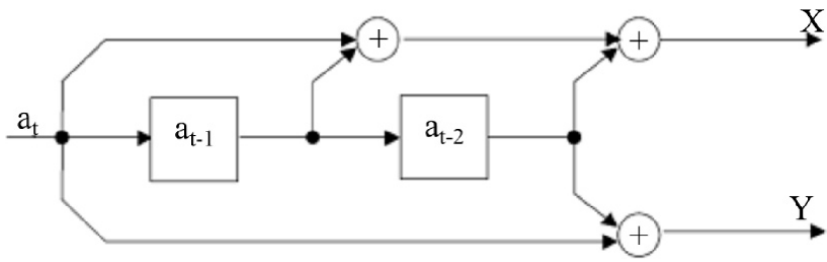


Figure 11.15. *Example of a convolutional coder*

11.4.2.4.1. Non-systematic convolutional codes (or NSC)

A convolutional code is called *systematic* if one of the output bits is identical to the input bit.

NSC codes, of which the one shown below is an example, have the advantage over systematic codes of providing more information: any of the coder's output bits gives information on several bits of the coded message. The decoder therefore has more elements in a NSC code, and therefore enables more errors to be corrected.

For this reason, it was NSC codes that were mainly studied and used until the beginning of the 1990s [MAS 71].

11.4.2.4.2. Recursive systematic convolutional codes(RSC)

A convolutional code is called "recursive" if the sequence passing through the shift registers is "powered" by the content of these registers. An example of a recursive coder is shown on Figure 11.16.

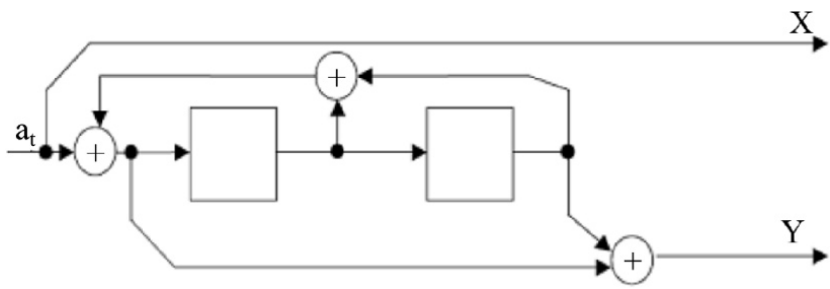


Figure 11.16. *Example of a RSC coder*

11.4.3. *Quantum error correcting code*

Just as in the classic case, a quantum code corrector uses a coding/imperfect transmission/decoding procedure in order to reduce error. But several particularities in the quantum instance make direct adaptation of classic strategies impossible, for example, first of all the qubit's structure is different from that of the classical bit [SHO 94].

11.4.3.1. *The Shor code*

Peter Shor's adaptation of the classical error correcting code by repetition (tripling each piece of data) begins by replacing each qubit |0> by the same qubit x 3 |000> and similarly each qubit |1> but the 3-qubits |111> [SHO 94].

If we have the qubit |x,y,z > we can for example know it. Shor's idea is to calculate the pair [y XOR z, x XOR z].

The calculation shows that if a single one of the components has flipped (0 become 1, or 1 become 0) in a 3-qubit made up of three times the same component, then the Shor pair gives the binary writing of the number of the bit that has changed: we can therefore make the correction.

EXAMPLE 11.2.– For (0,1,0) y XOR z represents 1, x XOR z represents 0 so the Shor pair is [1.0], which gives 10, the binary writing for 2, the number of the component to be corrected.

11.4.3.2. *Quantum error correcting codes developed in our laboratory*

In this section, we will focus on a quantum error correcting code developed in our laboratory. This gives us a broad approach with which to continue research based on quantum theory and applications for error correction.

11.4.3.2.1. XOR code

To make a transmission with total security in this coding section, we use changes on the key before Alice's basis choices appear, so before the transmission of photons through the quantum channel.

The transmission key developed by Alice is: (2^n)

1101001110010111……..

EXAMPLE 11.3.–

$2^n = 32$.

Section I-1:

11/01/00/11/10/01/01/11/……..

The key is cut into pairs of bits, there are 16 pairs.

Section I-2:

The XOR sum is calculated for the bits existing in the key's pairs to find an original Bit: (0), (1), (0), ……..

Section I-3:

A parity bit is used:

– If the number is even 0.

– If the number is odd 1.

A new key, which is a series of 00 or 11 with a technique for masking and encoding at the same time, is used so the least errors risk being detected when Bob receives the key.

(00), (11), (00), ……..

Section I-4:

There is a problem in this section: how do we know if the XOR = 1, if the bits are (01) or (10), and similarly for XOR =0 the bits are (00) or (11)? To solve this, we need additional bits, these are **XOR bits**:

For XOR = 0:

If the pair is 00 (0 for bit 0, 0 for the XOR). 00

If the pair is 11 (1 for 1, 0 or bit XOR). 10

For XOR = 1:

If the pair is 01 (0 for the pair 01, 1 for the XOR). 01

If the pair is 10 (1 for the pair 10, 1 for the XOR). 11

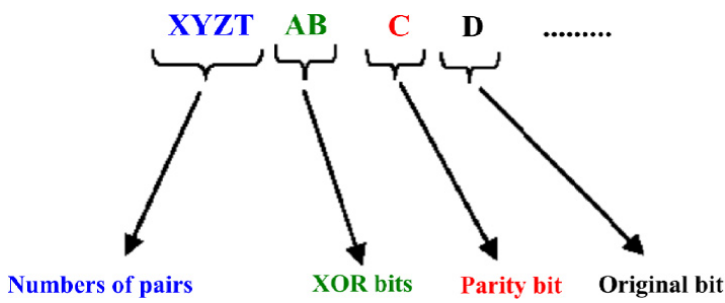
Then:

The key:

1000/ 0111/ 0000 ……...

Section I-5:

The numbers of pairs equals the number of bits (2^n = 32) then the numbers of pairs are coded by n/2 bites = in our example 4, for example the first pair *0001*(**10**00) so suites *0010*(**01**11), *0011*(**00**00),…….



The original bits and the parity bits and the XOR bits: When we make use of all the combinations that can by applying this method:

00 ------- **10**00, 11--------- **00**00.

01 ------- **01**11, 10 -------- **11**11.

The first three bits always have the same shape, which provides speed in the error detection.

The new key, before the basis choice by Alice is therefore:

*0001***10**0 *0010***01**1 *0011***00**0……

After a random choice of basis, the result is sent by the quantum channel, without forgetting that the message sent has information for no-one except Bob as no-one other than he is aware of the method.

11.4.3.2.2. Blind detection code

The process of mixing the key between the source and the polarizer is modeled by [WU 09]:

$$X(t) = A(S(t)) + B(t) \quad [11.17]$$

where X*(t)*, the vector of the observations measured by the receivers.

A, the mixing operator.

S*(t)*, the vector of the source signals that we seek to estimate.

B*(t)*, the noise vector that models the measuring errors.

Problems in blind source separation can be classed depending on the nature of the operator *A*.

– If this operator is linear, we speak of a linear mix.

The equation (1) is therefore written as:

$$X(t) = A(t) * S(t) + B(t) \quad [11.18]$$

where A(*t*) filter impulse response matrix

– is the continuous convolution operator.

– If the signals measured are in discreet time, which is necessarily the case for the digital signals recorded, the time variable *t* is replaced by an entire time index *n* and the continuous convolution operator is replaced by a discreet convolution.

The equation [11.18] therefore becomes:

$$X(n) = A(n). S(n) + B(n) \quad [11.19]$$

Among the linear mixes, two particular cases can be isolated:

– The mixes are linear and instantaneous, so A(n) is formed of sample units δ centered on 0.

The matrix A(n) is therefore written in the form:

$$A(n) = A\ \delta(n) \qquad [11.20]$$

where A is a matrix, and the convolution operator become a simple matrix multiplication.

$$X(n) = A\ S(n) + B(n) \qquad [11.21]$$

The mixes are linear at attenuations and delayed when the function A(n) is formed of sample units of different amplitudes and centered on different instants following the source-sensor pair considered.

The detection is based on the principle of block detection (parsimony principle) because of this, our algorithm consists of separately identifying the lines of the mix matrix.

The filter's response enables the line containing the useful information to be identified and therefore for matrix A to be generated. The following conditions are placed:

– The mix matrix S is a squared matrix in which the number of lines (columns) is odd (i = 2n + 1).

$$i = 0,1,2,3\ldots.n$$

$$S = \begin{bmatrix} S_{11} & S_{12} & . & . & S_{1i} \\ S_{21} & S_{22} & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ S_{i1} & . & . & . & S_{ii} \end{bmatrix}$$

– In the initial state, the matrix A_0 is a diagonal unitary matrix with the same lines and columns as S, in the case of a determined known detection.

$$A_0 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 0 & 1 & 0 & . & . & 0 \\ 0 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 \end{bmatrix}$$

The filter's response affects the lines of matrix A_0, through a change in the useful line, so that i = n + 1 (center line) the result will be in A_1

We return to the equation of the mixing process:

$$X_1 = A_1 S_0 \qquad [11.22]$$

The second phase consists of re-injecting the transpose of the matrix X_1 obtained in the filter that will again generate A_2, then recalculating the product to obtain X_2:

$$X_2 = A_2 S_1 \quad \text{with} \quad (S_1 = X_1^T) \qquad [11.23]$$

X_1^T, the matrix transposed from matrix X_1. and make the loop again.

The source to be identified is centrifuged at the center of matrix X_3 (the element n + 1 of the line n + 1). To make our algorithm more robust, we continue the calculations for X_5 and ensure that the result is identical for X_3, X_4 and X_5.

$$A_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$S_0 = \begin{bmatrix} A & B & C \\ D & E & F \\ G & H & I \end{bmatrix}$$

The symbol to be found is *C*.

The filter's response gives matrix A_1

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$X_1 = A_1 S_0 = \begin{bmatrix} D & E & F \\ A & B & C \\ G & H & I \end{bmatrix}$$

The filter's response on the transpose of X_1

$$X_1^T = \begin{bmatrix} D & A & G \\ E & B & H \\ F & C & I \end{bmatrix} = S_1$$

is matrix A_2:

$$A_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$X_2 = A_2 S_1 = \begin{bmatrix} D & A & G \\ F & C & I \\ E & B & H \end{bmatrix}$$

The filter's response on the transpose of X_2

$$X_2^T = \begin{bmatrix} D & F & E \\ A & C & B \\ G & I & H \end{bmatrix} = S_2$$

is matrix A_3:

$$A_3 = \begin{bmatrix} 1 & 0 & 0 \\ \boxed{0} & \boxed{1} & \boxed{0} \\ 0 & 0 & 1 \end{bmatrix}$$

$$X_3 = A_3 S_2 = \begin{bmatrix} D & F & E \\ \boxed{A} & \boxed{C} & \boxed{B} \\ G & I & H \end{bmatrix}$$

After the third stage, the symbol *C* will always be the element at the center of the matrix: the element n + 1 of the line n + 1 (in our case n = 1).

NOTE: The symbol C is drawn by our algorithm towards the center of the matrix, hence its name "centrifuged algorithm".

– Introduction to the quantum algorithm:

The protocol demands that Alice and Bob eliminate their data when they identify an error, consequently they will never be able to exchange a secret key using this protocol. In order to solve this problem, we should create an additional stage for the protocol, a stage that enables Alice and Bob to send a key more securely. To this effect, Alice and Bob should use protocol BB84 with the blind detection method for a new approach that makes the correction rather than eliminating their data when they identify errors. In order to make an entirely secure transmission, in this section we introduce changes in the protocol, before the basis choice is made by Alice and so before the transmission of photons through the quantum channel (see Figure 11.17).

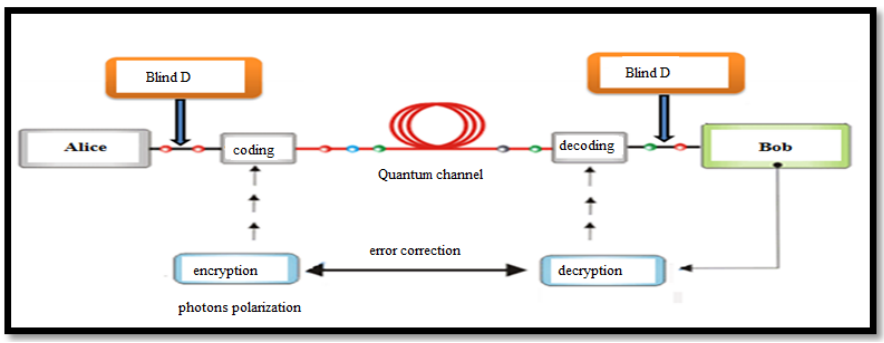
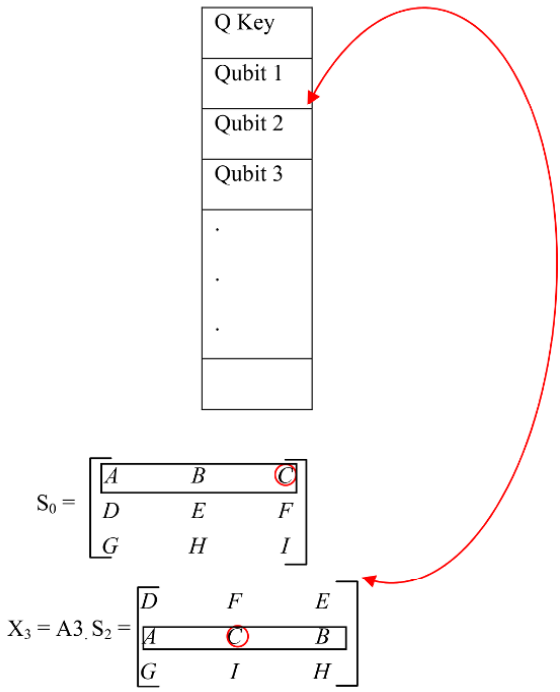


Figure 11.17. *The structure of the algorithm after combining protocol BB84 with blind detection*

– The matrix of mix S contains the qubit of the key that should be transmitted from Alice to Bob.

$$S = \begin{bmatrix} S_{11} & S_{12} & . & . & S_{1i} \\ S_{21} & S_{22} & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ S_{i1} & . & . & . & S_{ii} \end{bmatrix}$$

In our suggestion, the aim is to find symbol C, but by applying protocol BB84 the proposed detection is to replace all the key's qubits by C.



The matrix of the quantum bites

$$\begin{bmatrix} |D\rangle & |F\rangle & |E\rangle \\ |A\rangle & |C\rangle & |B\rangle \\ |G\rangle & |I\rangle & |H\rangle \end{bmatrix}$$

The final matrix that results is then transmitted through the quantum channel. This transmitted message matrix contains information for no one except Bob because apart from him, no one is aware of this method. Our aims are the following:

– A high security key: Through the creation of masking and coding stages at the beginning of the transmission between Alice and Bob.

– Thanks to this method, rather than sending the key directly, Alice sends the key's mask and the coding so as not to be detected by a spy (Eve).

– Let us suppose that Eve discovers the secret key that Alice and Bob will try to exchange, with this method, she will not be able to decipher it.

– Let us now suppose that Eve tries to discover the key, Bob can easily detect this and he can even inform Alice during the correction that there has been an interception during the transmission of the secret key.

11.4.4. *The time coding method for error correction: application in BB84*

This method hinges on the quantum key distribution used in BB84 and protocol BB92 [BEN 84]. It is based on single-photon pulses limited by the Fourier transform. We use the time–frequency uncertainty product that results from it and which has a non-null value dependent on the pulse's shape. In the examples that we describe, in this method, we will use coherent pulses whose time profile is rectangular and of duration T. The coherence's length is therefore equal to C_T.

The benefit of time coding lies mainly in the simplicity with which it can be used experimentally. The amplitude modulators created in integrated optics have bandwidths that can reach 40 GHz. It is therefore possible to produce pulses with ascent and descent times much shorter than a nanosecond.

The photon counters can have response times shorter than a nanosecond (300 ps for the silicon counters). Moreover, the pulses' travel time in a fiber is a robust parameter not very sensitive to defects in the fiber. The effects of group velocity dispersions are not noticeable on a scale of nanoseconds. The effects of depolarization do not directly influence the shape of the pulses and their moment of arrival.

Alice and Bob share a synchronized clock that enables the sending and detection of the pulses to be synchronized. In the simplest instance in the two-state protocol, Alice sends pulses by choosing at random and with identical probabilities a delay of 0 or a delay of T/2 in relation to the clock's signal (Figure 11.18).

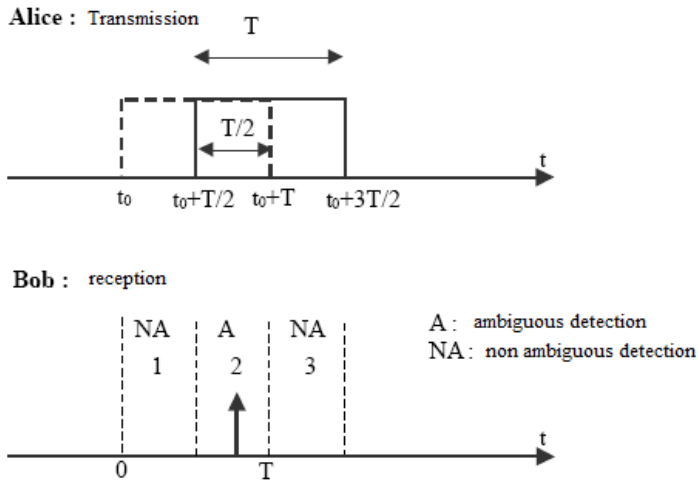


Figure 11.18. *Principle of the two-state protocol*

These two delays code bit 0 and bit 1. In order to determine the bit sent, Bob measures the photon's moment of detection with the help of a rapid photon counter. Depending on the window in which the detection is made, the result is ambiguous or nonambiguous. A detection in windows 1 or 3 enables Bob to identify the bit sent by Alice. A detection in window 2 gives no information on the bit sent by Alice. The ambiguity on half the results also applies to Eve. Having detected a photon in 2, she has a chance of one in two of resending a pulse different to the one received and therefore of creating an error in the key exchanged between Alice and Bob.

After studying this method, we were able to solve this problem. We will now explain this below.

11.4.5. *Correction of time code errors using the repetition method*

To correct the quantum errors in the key exchanged between Alice and Bob, in this work, we will use the coding method by repetition. That is to say, we will integrate two methods at the same time for the coding:

– the clock method and

– the repetition method.

– *Explanation of this method*:

Alice transmits for example a key whose shape is the following:

01100100111……

So each bit is sent twice:

11 11 *00 00* …….

So you can understand fully, you can see our method on the following figure:

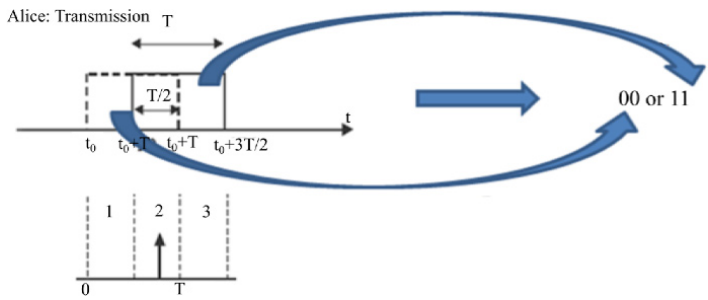


Figure 11.19. *Illustration of the bits transmitted by Alice*

Bob measures the moment the photon is detected with the help of a rapid photon counter:

– A detection in windows 1 or 3 enables Bob to know the qubit easily sent by Alice (Figure 11.20).

– If the first bit received in the window 1 is "*0*" and the second qubit will be "*0*" so the sensor gives us the information "*00*" directly.

– If the first bit received in the window 3 is "1" the second qubit will be "1" so the sensor gives us the information "11" directly.

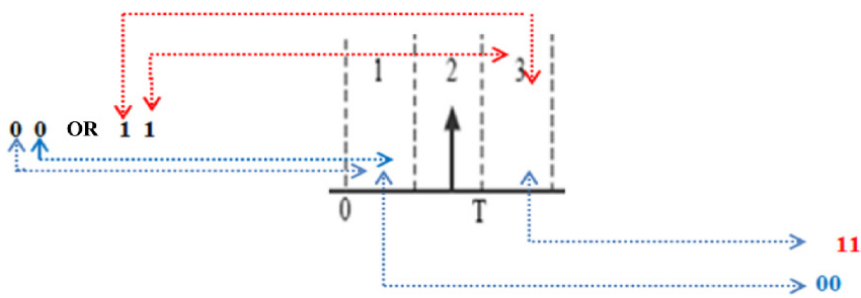


Figure 11.20. *This figure shows the bit received in window 1 and 3*

If the detection of the first qubit in window 2 gives none of the information sent by Alice, there is a problem with correction. But to solve this problem, we will automatically set the first qubit to "0" and calculate the logical OR sum directly with the qubit detected in window 1 or 3, that is to say :

If the first qubit is "0" and the second "*0*" "0" OR "0"= *0*

If the first qubit is "1" the sensor is always "0" and the second "1" ⟹ 0 OR 1= 1

– But there is a problem, if the two qubits sent by Alice are not detected, then window 2 will not succeed in correcting the first, that is to say that the second qubit cannot correct the first qubit. The two empty qubits do not give the information sent by Alice.

– To solve this problem, it is desirable to use the same protocol with a 3-qubit repetition code (we send another qubit that carries the same information transmitted by Alice). Therefore *the 3-qubit repetition method*:

"*0*" we send "*000*"

And for

"1" we send "111"

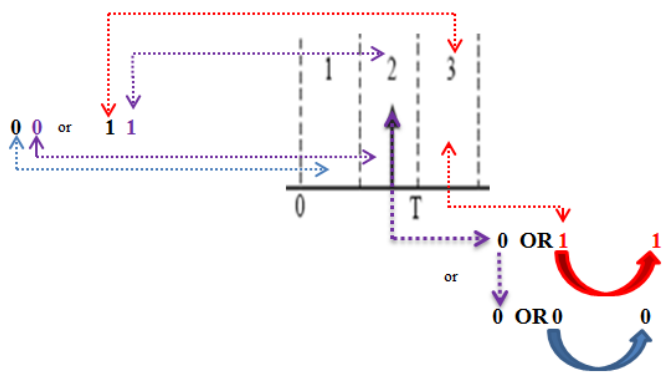


Figure 11.21. *Sensing bits in window 3*

11.4.6. *Conclusion*

Protocol BB84 enables two partners, Alice and Bob, to communicate a secret cryptographic key to each other. but because of Heisenberg's uncertainty principle and because the two bases form a pair of complementary properties, any spy carrying out this attack runs the risk of introducing incoherences in Alice and Bob's data.

There is a large range of error correcting codes in literature, but using protocol BB84 with such a quantum key distribution using time coding requires this technique to be mixed with a 3-qubit repetition code to exchange a secret key following the protocol with the same conditions.

Large-scale data protection in quantum computing is the aim of our research but it is necessary to improve some methods for correcting errors.

We will therefore try to pair these coding methods with others, to achieve a secret quantum transmission over long distances and on a large scale.

Conclusion

A combined ENS/CNRS/CEA-Saclay team from the Pierre Aigrain Laboratory has for the first time demonstrated how remarkably an electronic circuit behaves when its miniaturization is pushed to the extreme. These results are published in the journal *Science*. The researchers have shown that the fundamental laws of electricity, established since 1845, can no longer describe the properties of an electronic circuit when its dimensions reach nanometric scale. These studies confirm Markus Büttiker's theoretical predictions (University of Geneva) made 10 years ago and never since verified.

The laws of ordinary macroscopic physics do not take account of electrons' microscopic behavior, which is governed by the laws of quantum mechanics. This form of mechanics, since its discovery nearly 100 years ago, has revealed utterly astonishing behavior, far removed from our intuitive understanding of the phenomena. Due to the miniaturization of electronic circuits, the size of the components becomes so small that the physical description of the phenomena at work is affected by it: the laws of macroscopic physics are no longer applicable. The quantum effects will be unavoidable in the electronic circuits of tomorrow.

Light already plays a leading role in IT: it enables information to be transported at a very high rate, through optical fibers. But on a computer, the data are always handled and stored by electronic means. And the electronic exchange of data between processors, as well as memory, limits the speed of modern computers. Consequently, scientists seek methods of carrying out calculations and storing data purely optically – this is one of the domains studied in photonics. Thus, researchers from the Karlsruhe Institute of Technology (KIT) have created a completely optical memory by using materials known as "phase change" materials.

These are new materials whose optical properties vary depending on how the atoms that form them are arranged. Under the effect of ultra short laser pulses, they

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

transform from a regular, crystalline state, to an irregular, amorphous state. This property has been used by scientists at KIT to manufacture a nonvolatile PRAM (phase-change random access memory). To read the data, less powerful light pulses are used. The researchers presented their discovery in *Nature Photonics*.

Teams from the France Telecom Research Center succeeded in March 1999 in transporting a terabit, which is 1,000 billion bits per second, over a distance of 1,000 km via a conventional optic fiber. This is equivalent to transmitting 100 28,000-page encyclopedias per second.

For this demonstration, wavelength multiplexing is linked to a means of soliton transmission, forming a combination that does not lack advantages: compatible with existing infrastructure, it optimizes the transport capacities of very long-distance optical links at the least possible cost.

More and further data flow, at low costs: this summarizes the aims of the work undertaken by Cnet, the France Telecom Research Center, as data flow is a polymorphous technical field. In order to push the limits of information transport capacities indefinitely, three parameters must be juggled: flow, distance and the gaps between amplifiers. It is therefore where the components intersect that performance should be assessed.

Reconfigurable optical add-drop multiplexers (ROADM) shows notable limitations because of their analogical character, especially in terms of management, sub-wavelength multiplexing and capacity for fully exploiting the GMPLS control plane. However, a new class of ROADM, relying on digital technology, is currently emerging to overcome these obstacles and offer a range of additional advantages to service providers.

Operators have now acquired direct operational experience of using entirely optical ROADM multiplexers, and this experience makes it clear that ROADMs result in unforeseen costs and do not offer the flexibility necessary for sustaining the Internet's current growth rate. Designed in the last century to provide a flexible network capacity at a low cost, ROADMs are undoubtedly no longer suitable to today's environment.

In the middle of the 1990s, the DWDM industry developed what was thought to be an answer to this problem: the all-optical switch. The most common type of all-optical switch is the optical add/drop multiplexer (or OADM), which is generally used in ring topologies. The all-optical method aims to maintain the majority of wavelengths in the optical domain when they move through the OADM, which inserts or extracts only the wavelengths that need to enter or leave the network at

this point. The need for a OEO conversion is thus avoided for the wavelengths in transit and, theoretically, this in particular reduces the cost of the system.

Processes and devices for quantum coding on a DWDM (ROADM) network and optic fiber links have been the subject of a patent. The invention enables the following complex problems to be solved: development of a procedure for extracting the secret key of a lower layer optical signal, even in the presence of noise in a fiber optic cable, implemented from an amplification protocol for quantum protection to clean the states of photons polarization-entangled by noise in the optical channels, especially when an Einstein-Podolsky-Rozen procedure using a single-photon source is used to transmit and measure the polarization of photons in secret keys in a ROADM network refined from a key code transmission system that meets the random and confidentiality conditions with an increase in the speed of key production in a ROADM network; acceptable amplification of the optic fiber without loss of behavior and determination of a protocol enabling us to detect and correct errors on bits in an optic fiber cable and a ROADM network, resulting from linear and non-linear effects; development of quantum coding systems developed for use in telecommunication topologies.

As in classical telecommunications, the photons are well adapted for transmitting quantum information, given their high propagation speed and their low decoherence. Nevertheless, their advantage is also their weakness; the photons can only be used in a probabilistic fashion for quantum calculations where transmission between different information carriers is needed. Finally, photons are difficult to store. Consequently, many applications in the domain of communication and quantum calculation require the reversible transfer of non-classical photonic states on the electronic excitations of atoms or solids. Such a quantum memory would, for example, permit the creation of single-photon sources on demand, based on known single-photon sources. Moreover, this hypothesis will act as a step toward the time coding of quantum information and would represent a key element for quantum calculation based on a method for quantum error correction.

Current quantum communications (quantum cryptography) are fundamentally limited in their distance due to losses caused in the optic fibers (quantum noise) and the noise of the detectors, as well as the impossibility of using optic amplifiers, as in classical communications. The establishment of a quantum error correcting method will enable the maximal carrying capacity to be increased and thus enable future quantum communications networks to be extended. At the root of a quantum correction method, we find important concepts such as quantum teleportation or even entanglement transfer.

By coding information in the quantum states of individual photons, we can create communication principles totally inaccessible to classical IT. For example, following an idea put forward in 1984 by Charles Bennett and Gilles Brassard,

information can be transmitted with the certainty that a spy intercepting it can be detected. This is “quantum cryptography”. This process, whose feasibility has been demonstrated experimentally since 1993, is of course highly interesting to industrialists concerned about confidentiality, as well as governments.

The implementation of this process in ordinary optic fibers is, however, obstructed by a significant obstacle. Despite their remarkable quality, current optic fibers, in fact, lose half the photons travelling along them every 15 km: after 150 km, only one photon in 210 remains, which is around a thousandth. For classic optical telecommunications, this is not a problem: amplifiers placed at regular intervals along the line maintain the signal at a suitable level. But for quantum telecommunications, such a solution is not possible: the laws of quantum mechanics indicate that an amplifier able to replicate, identically a quantum state not known in advance cannot exist. The stimulated transmission, which is at the root of the optical amplification process, is accompanied in fact necessarily by a spontaneous transmission, a source of noise that inevitably masks the quantum signal.

Here, the involvement of a quantum repeater using teleportation would be useful.

This again is more easily said than done. First, the optical fibers and countless components used in optical communication have been optimized and standardized for circulating photons of wavelengths known as “telecom”, comprised of between 1.3 and 1.55 μm. The use of optical fibers over long distances means that we need to code the state to be teleported, as well as the entanglement, in a variable other than photon polarization. This is in fact disrupted in a non-negligible way in optical fibers and, above all, in a way that varies over time. We therefore use two “time modes”: pairs of photons transmitted with a very low time lag.

Applications for quantum communications in the domain of telecommunications require the conjunction of three factors: photonics, solitons and quantum mechanics. Quantum mechanics approached in the sense of generalized probability theory seems more practical in the sense of a signal. Achievements will be supported by the developments reached on quantum transistors, nanocrystals, nanoclusters and quantum dots.

Bibliography

[ABL 91] ABLOWITZ M.J., CLARKSON P.A., *Solitons, Nonlinear Evolution Equations and Inverse Scattering*, Cambridge University Press, 1991.

[ABL 11] ABLOWITZ M.J., *Nonlinear Dispersive Waves, Asymptotic Analysis and Solitons*, Cambridge University Press, 2011.

[ABR 11] ABRANSKY S., BRANDENBURGER, A., "The sheaf theoretic structure of non locality and contextuality", *New Journal of Physics*, vol. 13, p. 113036, 2011.

[AHA 59] AHARANOV Y., BOHM D., "Significance of electromagnetic potentials in the quantum theory", *Physical Review*, vol. 115, no. 3, pp. 485–491, 1959.

[AKA 03] AKAHANE Y., MOCHIZUKI M., ASANO T. *et al.*, "Design of a channel drop filter by using a donor-type cavity with high-quality factor in a two-dimensional photonic crystal slab", *Applied Physics Letters*, vol. 82, no. 9, pp. 1341–1343, 2003.

[ANT 12] ANTONOSYAN D.A., TAMAZYAN A.R., KRYUCHKYAN G.Y., "Chirped quasi phase matching with Gauss sums for production of biphotons", *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 45, pp. 1–7, 2012.

[ANW 14] ANWAR H., BROWN B., CAMPBELL E.T. *et al.*, "Fast decoder for qudit topological codes", *New Journal of Physics*, vol. 16, p. 063038, 2014.

[ARA 11] ARAD I., "A note about a partial no-go theorem for quantum PCP", *Journal Quantum Information & Computation*, vol. 11, nos. 11–12, pp. 1019–1027, 2011.

[ARN 97] ARNON S., KOPEIKA N.S., "Laser satellite networks: vibration effects and possible solutions", *Proceedings of IEEE*, vol. 85, no. 10, pp. 1646–1661, 1997.

[ARN 98a] ARNON S., KOPEIKA N.S., "Adaptive bandwidth for satellite optical communication", *IEE Proceedings – Optoelectronics*, vol. 145, no. 2, pp. 109–115, 1998.

[ARN 98b] ARNON S., KOPEIKA, N.S., "Performances limitations of free space optical communication satellite network due to vibrations: heterodyne detection", *Applied Optics*, vol. 37, pp. 6366–6374, 1998.

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.

© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

[ARN 98c] ARNON S., ROTMAN S., KOPEIKA N.S., "Optimum transmitter optics aperture for satellite optical communication", *IEEE Transaction on Aerospace and System*, vol. 34, no. 2, pp. 590–596, 1998.

[ARN 99] ARNON S., "Power versus stabilization for laser satellite communication", *Applied Optics*, vol. 38, no. 15, pp. 3229–3233, 1999.

[ARR 14] ARRAZOLA J.M., LÜTKENHAUS N., "Quantum communication with coherent states and linear optics", *Physical Review A*, vol. 90, no. 4, p. 42335, 2014.

[ASA 14] ASANO M., HASHIMOTO T., KHRENNIKOV A. *et al.*, "Violation of contextual generalization of the Legget–Garg inequality for recognition of ambiguous figures", *Physica Scripta*, vol. T163, pp. 014006–014016, 2014.

[BAR 85] BARRY J.D., MECHERLE G.S., "Beam pointing error as a significant parameter for satellite borne, free space optical communication systems", *Optical Engineering*, vol. 24, no. 6, pp. 1049–1054, 1985.

[BEN 92] BENNETT C.H., "Quantum cryptography using any two non orthogonal states", *Physical Review Letters*, vol. 68, pp. 3121–3124, 1992.

[BEN 04] BENENTI G., CASATI G., STRINI G., *Principles of Quantum Computation and Information. Vol. 1: Basic Concepts*, World Scientific, 2004.

[BEN 16] BENSLAMA M., BATATIA H., MESSAI A., *Transitions from Digital Communications to Quantum Communications: Concepts and Prospects*, ISTE, London and John Wiley & Sons, New York, 2016.

[BEN 15a] BENSLAMA M., BOUCENNA M.L., BATATIA H., *Ad Hoc Networks Telecommunications and Game Theory*, ISTE, London and John Wiley & Sons, New York, 2015.

[BEN 15b] BENSLAMA M., KIAMOUCHE, BATATIA H., *Connections Management Strategies in Satellite Cellular Networks*, ISTE, London and John Wiley & Sons, New York, 2015.

[BER 49] BERNAYS P., "Paulette Destouches-Février, Sur les rapports entre la logique et la physique théorique, logique adaptée aux théories quantiques", *Journal of Symbolic Logic*, vol. 4, no. 2, pp. 128–129, 1949.

[BER 96] BERENGER J.P., "Three-dimensional perfectly matched layer for the absorption of electromagnetic waves", *Journal of Computational Physics*, vol. 127, pp. 363–379, 1996.

[BIR 31] BIRKHOFF G.D., "Proof of the ergodic theorem", *Proceedings of the National Academy of Sciences*, vol. 17, pp. 656–660, 1931.

[BIT 98] BITBOL M., "La mécanique quantique comme théorie des probabilités généralisées", in KLEIN E., SACQUIN Y. (eds), *Prévision et probabilités dans les sciences*, Editions Frontières, 1998.

[BLI 29] BLIGH N.M., "The evolution of the new quantum mechanics", *Science Progress in the Twentieth Century (1919–1933)*, vol. 23, no. 92, pp. 619–632, 1929.

[BOH 52] BOHM D., "A suggested interpretation of the quantum theory in terms of 'Hidden' variables", *Physical Review*, vol. 85, no. 2, pp. 166–179, 1952.

[BOS 13] BOSCA M.C., "Some observations upon 'realistic' trajectories in Bohmian quantum mechanics. Theoria: an international journal for theory, history and foundations of science", *Segunda Epoca*, vol. 28, no. 1, pp. 45–60, 2013.

[BOW 12] BOWLES P., GUTA M., ADESSO G., "Asymptotically optimum quantum channel reversal for qudit ensembles and multimode Gaussian states", *New Journal of Physics*, vol. 14, pp. 113041–1, 113041–17, 2012.

[BRI 98] BRIEGEL H.J., DUR W., CIRAC J.I. *et al*., "Quantum repeaters: the role of imperfect local operation in quantum communication", *Physical Review Letters*, vol. 81, p. 5932, 1998.

[CAL 92] CALLAWAY T.K., SWARTZLANDER E.E., "Optimizing arithmetic elements for signal processing", *IEEE Workshop on VLSI Signal Processing*, vol. V, pp. 91–100, 1992.

[CHE 85] CHEN K.J., STACH J.F., WU T.H., "A new method for topological design in large traffic laden packet switched networks", *ACM*, vol. 15, no. 4, pp. 115–121, 1985.

[CHE 10] CHEN Y., TANG W., "Reconfigurable asymmetric optical burst switching for concurrent DWDM multimode switching: architecture and research directions", *IEEE Communications Magazine*, vol. 48, no. 5. pp. 57–65, 2010.

[CHI 03] CHILDS A.M., CLEVE R., DEOTTO E. *et al*., "Exponential algorithmic speedup by a quantum walk", *STOC'03*, p. 59, 2003.

[CHO 04a] CHOU E.Y., HUANG J.C., HUNG M.S. *et al*., "Baud rate channel equalization in nanometer technologies", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 11, pp. 1174–1181, 2004.

[CHO 04b] CHOWDHARY G.V., SIVA C., MURTHY R., "Dynamic multicast traffic engineering in WDM groomed mesh networks", *Proc. IEEE Broadnets*, 2004.

[CHO 11] CHOI B.S., METER R.V., "On the effect of quantum interaction distance on quantum addition circuits", *ACM Journal on Emerging Technologies in Computing Systems*, vol. 7, no. 3, pp. 11:1–11:17, 2011.

[CHO 12] CHOI B.S., METER R.V., "A q(√n) depth quantum adder on the 2D NTC quantum computer architecture", *ACM Journal on Emerging Technologies in Computing Systems*, vol. 8, no. 3, pp. 24:1–24:22, 2012.

[CHU 99] CHUTINAN A., NODA S., "Highly confined waveguides and waveguides bends in 3D photonic crystal", *Applied Physics Letters*, vol. 75, pp. 3739–3741, 1999.

[CLE 98] CLEVE R., EKERT A., MACCHIAVELLO C. *et al*., "Quantum algorithms revisited", *Proceedings of the Royal Society of London A*, vol. 454, pp. 339–354, 1998.

[COE 09] COELHO L.D., GAETE O., HANIK N., "An algorithm for global optimization of optical communication systems", *International Journal of Electronics and Communications (AEU)*, vol. 63, no. 7, pp. 541–550, 2009.

[COH 89] COHEN L., "Time frequency distributions, a review", *Proceedings of the IEEE*, vol. 47, no. 7, pp. 941–981, 1989.

[COL 11] COLLINS B., NECHITA I., "Gaussianization and eigenvalue statistics for random quantum channel (III)", *The Annals of Applied Probability*, vol. 21, no. 3, pp. 1136–1179, 2011.

[COQ 01] COQUEREAUX R., "Classical and quantum interaction, a fusion graph algebra point of view", *AIP Conference Proceedings*, vol. 581, pp. 181–203, 2001.

[DAS 13] DAS S., ARAVINDA S., SRIKANTH R. *et al*., "Unification of Bell, Legget–Garg and Kochen–Specker inequalities; hybrid spatio temporal inequalities", *Europhysics Letters*, vol. 104, p. 60006, 2013.

[DE 97] DE MARTINI F., JEDRKIEWICZ O., MATALONI P., "Generation of quantum photon states in an active microcavity trap", *Journal of Modern Optics*, vol. 44, pp. 2053–2066, 1997.

[DEH 10] DEHGAN M., TALEEI A., "A compact split step finite difference method for solving the nonlinear Schrodinger equations with constant and variable coefficients", *Computer Physics Communications*, vol. 181, no. 1, pp. 43–51, 2010.

[DJE 16] DJEFFAL N., Techniques d'accès optiques et marches quantiques généralisées pour des applications WDM, PhD thesis, University of Constantine, available at: bu.umc.edu.dz/theses/electronique/DJE6923.pdf, 2016,

[DOP 98] DOPFER B., Zwei experimente interferenz von zwei photonen zuständer ein Heisenbergmikroshop und pendellönsung, Thesis, University of Innsbruck, 1998.

[DZH 14] DZHAFAROV E.N., KUJALA J.V., "Contextuality is about identity of random variables", *Physica Scripta*, vol. T163, pp. 014009–014013, 2014.

[EIN 35] EINSTEIN A., PODOLSKY B., Rosen N., "Can quantum mechanical description of physical reality be considered complete", *Physical Reviews*, vol. 47, pp. 777–780, 1935.

[EKE 91] EKERT A.K., "Quantum cryptography based on Bell's theorem", *Physical Review Letters*, vol. 67, p. 661, 1991.

[EKI 85] EKIMOV A.I., LEFROS A.I., ONUSCHCHENKO A.A., "Quantum size effect in semiconductors crystals", *Solid States Communications*, vol. 56, no. 11, pp. 921–924, 1985.

[ELD 01] ELDAR Y.C., Quantum signal processing, PhD Thesis, MIT, 2001.

[ELD 02] ELDAR Y.C., OPPENHEIM A.V., "Quantum signal processing", *IEEE Signal Processing Magazine*, vol. 19, no. 6, pp. 12–32, 2002.

[ELI 55] ELIAS P., "Coding for noisy channels", *IRE Convention Record*, vol. 3, Part 4, pp. 37–46, 1955.

[FAN 99] FAN S., CHAPLINE M.G., FRANKLIN N.R., "Self oriented regular arrays of carbon nanotubes and their fields emission properties", *Science*, vol. 283, no. 5401, pp. 512–514, 1999.

[FAS 04] FASEL S., GISIN N., RIBORDY G. *et al*., "Quantum key distribution over 30 km standard fiber using energy-time entangled photon pairs", *The European Physical Journal D*, vol. 30, pp. 143–148, 2004.

[FDT 16] FDTD, The FDTD simulations were carried out with fullwave commercial software by RSoft Design Group, version 6.1, license 16847214, 2016.

[FER 08] FERRIE C., EMERSON J., "Frame representations of quantum mechanics and the necessity of negativity in quasi probability representations", *Journal of Physics A: Mathematical and Theoretical*, vol. 41, pp. 352001–352012, 2008.

[FER 09] FERRIE C., EMERSON J., "Framed Hilbert space; hanging the quasi-probability pictures of quantum theory", *New Journal of Physics*, vol. 11, p. 063040, 2009.

[FER 11] FERRIE C., "Quasi probability representations of quantum theory with applications to quantum information science", *Reports on Progress in Physics*, vol. 74, pp. 116001-1–116001-24, 2011.

[FRA 94] FRANSON J.D., ILVES H., "Quantum cryptography using polarization feedback", *Journal of Modern Optics*, vol. 41, p. 2391, 1994.

[FUR 12] FURUICHI S., YANAGI K., "Schrödinger uncertainty relation, Wigner–Yanase–Dyson skew information and metric correlation measure", *Journal of Mathematical Analysis and Applications*, vol. 388, pp. 1147–1156, 2012.

[FUY 10] FUYU H., GANG L., HONGBIN S., "Simulation of earth background radiation characteristic for satellite borne laser warning system", *Optics Communication*, vol. 283, no. 18, pp. 3415–3418, 2010.

[GHA 12] GHATAK A., THYAGARAJAN K., *An Introduction to Fiber Optics*, Cambridge University Press, 2012.

[GIS 07] GISIN N., THEW R., "Quantum communication," *Nat Phot*., vol. 1, no. 3, pp. 165–171, March. 2007.

[GIS 10] GISIN N., THEW R., "Quantum communication technology," *Electronic Letters*, vol. 46, no. 14, p. 961, 2010.

[GLE 57] GLEASON A., "Measures on the closed subspaces of a Hilbert space", *Indiana University Mathematics Journal*, vol. 6, no. 4, pp. 885–893, 1957.

[GLI 97] GLISIC S., VUCETIC B., *Spread Spectrum CDMA Systems for Wireless Communications*, Artech House, 1997.

[GOB 04] GOBBY C., YUAN Z.L., SHIELDS A.J., "Unconditionally secure quantum key distribution over 50 km of standard telecom fibre", *Electronics Letters*, vol. 40, p. 1603, 2004.

[GOG 11] GOGGIN M.E., ALEIDA M.P., BARBIERI M. *et al.*, "Violation of the Legget–Garg inequality with weak measurement of photons", *Proceedings of the National Academy of Sciences of the United States of America*, vol. 108, no. 4, pp. 1256–1261, 2011.

[GUE 05] GUERREAU O.L., MALASSENET F.J., MCLAUGHLIN S.W. *et al.*, "Quantum key distribution without a single-photon source using a strong reference", *IEEE Photonics Technology Letters*, vol. 17, no. 8, pp. 1755–1757, 2005.

[HAM 50] HAMMING R.W., "Error detecting and error correcting codes", *Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950.

[HAS 03] HASEGAWA Y., LOIDL R., BADUREK G. *et al.*, "Violation of a Bell-like inequality in single-neutron interferometry", *Nature*, vol. 425, pp. 45–48, 2003.

[HEI 27] HEISENBERG W., "Uber den anschaulichen inhalt der quantentheoretischen kinematic und mechanic", *Zeitschrift für Physik*, vol. 43, no. 3, pp. 172–198, 1927.

[HER 10] HERBRÜGGEN T.S., SANDER U., ZEIER R., "Symmetry principles in quantum system theory of multi qubit systems made simple", *IEEE 4th International Symposium on Communications*, *Control and Signal Processing*, pp. 1–5, 2010.

[HO 90] HO K.M., CHAN C.T., SOUKOULIS M., "Existence of a photonic gap in periodic structures", *Physical Review Letters*, vol. 65, p. 3152, 1990.

[HOL 13] HOLLECZEK A., BARTER O., NISBET-JONES P.B.R. *et al.*, "Quantum networking with time bin encoded qudits using single photons emitted on demand from an atom cavity system", *IEEE Conference on Lasers and Electrooptics and International Quantum Electronic*, p. 1, 2013.

[HOW 14] HOWARD M., WALLMAN J., VEITCH V. *et al*., "Contextuality supplies the 'magic' for quantum computation", *Nature*, vol. 510, pp. 351–355, 2014.

[HUT 15] HUTTER A., LOSS D., WOOTTON J.R., "Improved HDRG decoders for qudit and non abelian quantum error correction", *New Journal of Physics*, vol. 17, p. 035017, 2015.

[IAF 96] IAFRATE G.J., STROSCIO M.A., "Application of quantum based devices; trends and challenges", *IEEE Transactions on Electron Devices*, vol. 43, no. 10, pp. 1621–1625, 1996.

[JAY 14] JAYASHREE H.V., THAPLIYAL H., AGRAWAL V.K., "Design of dedicated reversible quantum circuitry for square computation", *IEEE 13th International Conference on Embedded Systems and 27th International Conference on VLSI Design*, pp. 551–556, 2014.

[JI 13] JI Y.Q., WEN J.J., WANG Y.L. *et al.*, "Deterministic quantum logic gates and quantum cloning based on quantum dot cavity coupled system", *Optics Communications*, vol. 303, pp. 56–61, 2013.

[JIA 13] JIANG M., JIANG F., "Deterministic joint remote preparation of arbitrary multi-qudit states", *Physics Letters A*, vol. 377, pp. 2524–2530, 2013.

[JOA 95] JOANNOPOULOS J.D., MEADE R.D., WINN J.N., *Photonic Crystals-Molding the Flow of Light*, Princeton University Press, 1995.

[JOH 87] JOHN S., "Strong localization of photons in certain disordered dielectric superlattices", *Physical Review Letters*, vol. 58, pp. 2486–2489, 1987.

[JON 08] JONES J.A., "NMR implementations of Gauss sums", *Physics Letters A*, vol. 372, pp. 5758–5799, 2008.

[JOZ 98] JOZSA R., "Quantum algorithms and the Fourier transform", *Proceedings of the Royal Society of London. Series A*, vol. 454, pp. 323–337, 1998.

[JOZ 08] JOZSA R., MIYAKE A., "Matchgates and classical simulation of quantum circuits", *Proceedings of the Royal Society of London. Series A*, vol. 464, pp. 3089–3106, 2008.

[KAR 07] KARAKOSTAS V., "Nonseparability, potentiality and the context dependence of quantum objects", *Journal for General Philosophy of Science*, vol. 38, p. 279–297, 2007.

[KAS 01] KASAI S., YUMOTO M., HASEGAWA H., "Fabrication of GaAs based integrated 2-bit half and full adders by novel hexagonal BDD quantum circuit approach", *IEEE International Symposium on Semiconductor Device Research*, pp. 622–625, 2001.

[KHA 04] KHALIL A., ASSI C., HADJIANTONIS A. *et al*, "On multicast traffic grooming in WDM networks," *Computers and Communications*, vol. 1, pp. 282–287, 2004.

[KIR 09] KIRCHMAIR G., ZÄHRINGER F., GERRITSMA R. *et al.*, "State-independent experimental test of quantum contextuality", *Nature*, vol. 460, pp. 494–497, 2009.

[KNI 00] KNIGHT J.C., ARRIAGA J., BIRKS T.A. *et al.*, "Anomalous dispersion in photonic crystal fiber", *IEEE Photonics Technology Letters*, vol. 12, no. 7, pp. 807–809, 2000.

[KNI 01] KNILL E., LAFLAMME R., MILBURN G.J., "A scheme for efficient quantum computation with linear optics", *Nature*, vol. 409, pp. 46–52, 2001.

[KNI 11] KNILL E., LAFLAMME R., BARNUM H. *et al.*, "Introduction to quantum information processing", in FURUSAWA A. (ed.), *Quantum Teleportation and Entanglement*, Peter Van Loock, Wiley, 2011.

[KOK 11] KOKSMA J.F., PROKOPEC T., SCHMIDT M.G., "Decoherence in quantum mechanics", *Annals of Physics*, vol. 326, pp. 1548–1576, 2011.

[KRE 14] KRENNIKOV A., "Classical probability model for Bell inequality", *Journal of Physics: Conference Series*, vol. 504, p. 012019, 2014.

[KUM 98] KUMMERER B., MAASSEN H., "Elements of quantum probability", *Quantum Probability Communications*, vol. 10, pp. 73–100, 1998.

[LAM 95] LAMBERT S.G., CASEY W.L., *Laser Communication in Space*. Boston, Artech House, 1995.

[LAN 61] LANDAUER R., "Irreversibility and heat generation in the computing process", *IBM Journal of Research and Development*, vol. 35, no. 3, pp. 183–191, 1961.

[LAW 97] LAW C.K., KIMBLE H.J., "Deterministic generation of a bit-stream of single-photon pulses", *Journal of Modern Optics*, vol. 44, pp. 2067–2074, 1997.

[LOU 00] LOUNIS B., MOERNER W.E., "Single photons on demand from a single molecule at room temperature", *Nature*, vol. 407, pp. 491–493, 2000.

[LOU 03] LOURTIOZ J.M., BENISTY H., BERGER V. *et al.*, *Les cristaux photoniques ou la lumière en cage*, Hermes-Science−Lavoisier, Paris, 2003.

[LU 12] LU W., LIU L., SUN J. *et al.*, "Control analysis of acquirement and locking in intersatellite laser communications", *Optik*, vol. 123, no. 19, pp. 1750–1754, 2012.

[MAL 10] MALHOTRA J.S., KUMAR M., "Performance analysis of NRZ, RZ, CRZ and CSRZ data formats in 10 Gb/s optical soliton transmission link under the impact of chirp and TOD", *Optik*, vol. 121, no. 9, pp. 800–807, 2010.

[MAN 13] MAN'KO M.A., "Mathematical methods of studying physical phenomena", *Pysica Scripta*, vol. 87, pp. 030201–030203, 2013.

[MAO 09] MAOR E., "How I got to understand Heisenberg's uncertainty principle", *Math Horizons*, vol. 16, no. 4, pp. 5–7, 2009.

[MAR 10] MARØY O., LYDERSEN L., SKAAR J., "Security of quantum key distribution with arbitrary individual imperfections," *Physical Review A*, vol. 82, no. 3, pp. 1–7, 2010.

[MAS 71] MASSEY J.L., COSTELLO D.J., "Non systematic convolutional codes for sequential decoding in space applications", *IEEE Transactions on Communications Technology*, vol. 19, no. 5, pp. 806–813, 1971.

[MAS 07] MASLOV D., FALCONER S.M., MOSCA M., "Quantum circuit placement; optimizing qubit to qubit interactions through mapping quantum circuits into a physical experiment", *DAC 2007*, pp. 962–965, 2007.

[MEK 99] MEKIS A., FAN S., JOANNOPOULOS J.D., "Absorbing boundary conditions for FDTD simulations of photonic crystal waveguides", *IEEE Microwave and Guided Wave Letters*, vol. 9, no. 12, pp. 502–504, 1999.

[MIG 09] MIGUEL DE I., VALLEJOS R., BEGHELLI A. *et al*, "Genetic Algorithm for Joint Routing and Dimensioning of Dynamic WDM Networks", *IEEE/OSA Journal of Optical Communications and Networking*, vol. 1, no. 7. pp. 608–621, 2009.

[MOH 14] MOHAMMADI R., "An exponential spline solution of a nonlinear Schrödinger equations with constant and variable coefficients", *Computer Physics Communications*, vol. 185, no. 3, pp. 917–932, 2014.

[MOS 01] MOSSERI R., DANDOLOFF R., "Geometry of entangled states, Bloch spheres and Hopf fibrations", *Journal of Physics A: Mathematical and General*, vol. 34, no 47, pp. 10243–10253, 2001.

[NAI 00] NAIK D.S., PETERSON C.G., WHITE A.G. *et al*., "Entangled state quantum cryptography: eavesdropping on the Ekert protocol", *Physical Review Letters*, vol. 84, pp. 4733–4736, 2000.

[NAT 15] NATSHEH AL A., GBADEGESHIN S.A., RIMPILÄINEN A. *et al*, "Identifying the challenges in commercializing high technology: a case study of quantum key distribution technology," *Technology Innovation Management Review*, vol. 5, no. 1, 2015.

[NEE 06] NEEL D., Etude en champ proche optique de guides à cristaux photoniques sur SOI, PhD Thesis, University of Lyon, 2006.

[NEE 09] NEELY M., ANSMANN M., BIALCZAK R.C. *et al*., "Emulation of a quantum spin with superconducting phase qudit", *Science*, vol. 325, pp. 722–725, 2009.

[NEU 33] NEUMANN J.V., "Mathematische grundlagen der quantenmechanik", *Monatshefte for Mathematics and Physics*, vol. 40, no. 1, pp. A31–A32, 1933.

[NIE 00] NIELSEN M.A., CHUANG I.L., *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[NIS 13] NISBET-JONES P.B.R., DILLEY J., HOLLECZEK A. *et al*., "Photonic qubits, qutrits and ququads accurately prepared and delivered on demand", *New Journal of Physics*, vol. 15, no. 053007, pp. 1–11, 2013.

[NOD 07] NODA S., FUJITA M., ASANO T., "Spontaneous-emission control by photonic crystals and nanocavities", *Nature Photonics*, vol. 1, pp. 449–458, 2007.

[PEL 02] PELTON M., SANTORI C., VUCKOVIC J. *et al*., "Efficient source of single photons: a single quantum dot in a micropost microcavity", *Physical Review Letters*, vol. 89, p. 233602, 2002.

[PET 90] PETERSON I., "Bits of uncertainty: quantum security", *Science News*, vol. 137, no. 2, pp. 342–343, 1990.

[PIT 89] PITOWSKY I., *Quantum Probability, Quantum Logic*, Springer, 1989.

[POT 99] POTTIER P., SEASSAL C., LETARTRE X. *et al*., "Triangular and hexaghonal high Q-factor 2-D photonic bandgap cavities on III–V suspended membranes", *IEEE Journal of Lightwave Technology*, vol. 17, p. 2058, 1999.

[PWM 16] PWM, The PWM simulations were carried out with Bandsolve commercial software by RSoft Design Group, version 4.3, license 16847214, 2016.

[QIU 03] QIU M., JASKORZYNSKA B., "Design of a channel drop filter in a two-dimensional triangular photonic crystal", *Applied Physics Letters*, vol. 83, p. 1074, 2003.

[RAB 14] RABELO R., DUARTE C., TARRIDA A.J.L. *et al*., "Multigraph approach to quantum non locality", *Journal of Physics A: Mathematical and Theoretical*, vol. 47, pp. 424021–424042, 2014.

[RAS 15] RASTEGIN A.E., "On generalized entropies and information theoretic Bell inequalities under decoherence", *Annals of Physics*, vol. 355, pp. 241–257, 2015.

[REE 01a] REESE C., BECHER C., IMAMOGLU A. *et al*., "Photonic crystal microcavities with self-assembled InAs quantum dots as active emitters", *Applied Physics Letters*, vol. 78, p. 2279, 2001.

[REE 01b] REESE C., GAYRAL B., GERARDOT B.D. *et al*., "High Q photonic crystal microcavities fabricated in a thin GaAs membrane", *Journal of Vacuum Science & Technology B*, vol. 19, p. 2749, 2001.

[SAK 01] SAKODA K., *Optical Properties of Photonic Crystals*, Springer-Verlag, Berlin, 2001.

[SCH 98] SCHERER A., PAINTER O., D'URSO B. *et al*., "InGaAsP photonic band gap crystal membrane microresonators", *Journal of Vaccum Science and Technology B*, vol. 16, p. 3906, 1998.

[SCH 07] SCHLOSSHAUER M., *Decoherence and the Quantum-To-Classical Transition*, Springer-Verlag, 2007.

[SHO 94] SHOR P., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, p. 124, 1994.

[SHO 99] SHOR P.W., "Polynomial time algorithm for primer factorization and discrete algorithms on a quantum computer", *SIAM Review*, vol. 41, no. 2, p. 303–332, 1999.

[SIN 03] SINGHAL N.K., MUKHERJEE B., "Protecting multicast sessions in WDM optical mesh networks", *Journal of Lightwave Technology*, vol. 21, no. 4, pp. 884–892, 2003.

[SIN 09] SINGH J.P., "Quantum entanglement – a primer", *African Journal of Mathematical Physics*, vol. 7, no. 1, pp. 71–98, 2009.

[SMI 99] SMITH C.J.M., BENISTY H., LABILLOY D. *et al*., "Near-infrared microcavities confined by two-dimensional photonic crystals", *Electronics Letters*, vol. 35, p. 228, 1999. *Lett*., vol. 58, pp. 2059–2062, 1987.

[SPI 68] SPIEGEL M.R., *Mathematical Handbook of Formulas and Tables*, McGraw-Hill, New York, 1968.

[STU 02] STUCKI D., GISIN N., GUINNARD O. *et al*., "Quantum key distribution over 67 km with a plug & play system", *New Journal of Physics*, vol. 4, p. 41.1, 2002.

[SUT 98] SUTO K., KIMURA T., SAITO T. *et al*., "Raman amplification in GaP-AlxGa1-xP waveguides for light frequency discrimination", *IEE Proceedings in Optoelectronics*, vol. 145, no. 2, April 1998.

[TAF 75a] TAFLOVE A., BRODWIN M.E., "Numerical solution of steady-state electromagnetic scattering problems using the time-dependent Maxwell's equations", *IEEE Transactions on Microwave Theory and Techniques*, vol. MTT-23, no. 8, pp. 623–630, August 1975.

[TAF 75b] TAFLOVE A., BRODWIN M.E., "Numerical solution of steady-state electromagnetic scattering problems using the time-dependent Maxwell's equations", *IEEE Transactions on Microwave Theory and Techniques*, vol. MTT-23, no. 11, pp. 888–896, November 1975.

[TAF 05] TAFLOVE A., HAGNESS S.C., *Computational Electrodynamics: the Finite Difference Time Domain Method*, 2nd ed., Artech House, Norwood, 2005.

[TAK 05] TAKESUE H., DIAMANTI E., HONJO T. *et al*., "Differential phase shift quantum key distribution experiment over 105 km fibre", *New Journal of Physics*, vol. 7, p. 232, 2005.

[TAL 02] TALNEAU A., LALANNE P., AGIO M. *et al*., "Low-reflection photonic-crystal taper for efficient coupling between guide sections of arbitrary widths", *Optics Letters*, vol. 27, pp. 1522–1524, 2002.

[TAM 14] TAMAKI K., CURTY M., KATO G. *et al*, "Loss-tolerant quantum cryptography with imperfect sources", *Physical Review A*, vol. 90, no. 5, p. 52314, 2014.

[THA 15] THAPLIYAL K., BENERJEE S., PATHAK A. *et al*., "Quasiprobability distributions in open quantum systems: spin-qubit systems", *Annals of Physics*, vol. 362, pp. 261–286, 2015.

[TOL 13] TOLLAKSEN J., "New insights on emergence from the perspective of weak values and dynamical non locality", *Journal of Physics: Conference Series*, vol. 504, p. 012029, 2013.

[TOW 94] TOWNSEND P.D., THOMPSON I., "A quantum key distribution channel based on optical fibre", *Journal of Modern Optics*, vol. 41, p. 2425, 1994.

[TUR 50] TURING A.M., "Computing machinery and intelligence", *Mind*, vol. 59, no. 236, pp. 433–460, 1950.

[TUR 12] TURITSYN S.K., BALE B.G., FEDORUK M., "Dispersion-managed solitons in fibre systems and lasers", *Physics Reports*, vol. 521, pp. 135–203, 2012.

[VAL 05] VALENTINE A., WESTMAN H., "Dynamical origin of quantum probabilities", *Proceedings of the Royal Society of London A*, vol. 461, pp. 253–272, 2005.

[VAZ 02] VAZIRI A., WEIHS G., ZEILINGER A., "Experimental two-photon, three-dimensional entanglement for quantum communication", *Physical Review Letters*, vol. 89, no. 24, pp. 240–401, 2002.

[VER 26] VERNAM G., "Cipher printing telegraph systems for secret wire and radio telegraphic communications", *Journal of the American Institute of Electrical Engineers*, vol. 45, pp. 109–115, 1926.

[VUK 03] VUKUSIC P., SAMBLES J.R., "Photonic structures in biology", *Nature*, vol. 424, pp. 852–855, 2003.

[WAN 13a] WANG H.F., WEN J.J., ZHU A.D. *et al*., "Deterministic CNOT gate and entanglement swapping for photonic qubits using a quantum dot spin in a double sided optical microcavity", *Physics Letters A*, vol. 377, pp. 2870–2876, 2013.

[WAN 13b] WANG X.H., WANG Z.D., LIANG X.J., "Research on PMD compensation in high speed optical fiber communication network", *The Journal of China Universities of Posts and Telecommunications*, vol. 20, suppl. 2, pp. 152–155, 2013.

[WAN 15] WANG D.S., SANDERS B.C., "Quantum circuit design for accurate simulation of qudit channels", *New Journal of Physics*, vol. 17, p. 043004, 2015.

[WEI 12] WEI L. *et al*, "Control analysis of acquirement and locking in inter-satellite laser communications", *Optik*, vol. 123, pp. 1750–1754, 2012.

[WIG 32] WIGNER E., "On the quantum correction for thermodynamic equilibrium", *Physical Review*, vol. 40, no. 5, p. 749, 1932.

[WIN 14] WINTER A., "What does an experimental test of quantum contextuality prove or disprove", *Journal of Physics A: Mathematical and Theoretical*, vol. 47, pp. 424031–424045, 2014.

[WOO 82] WOOTERS W.K., ZUREK W.H., "A single quantum cannot be cloned", *Nature*, vol. 299, pp. 802–803, 1982.

[WU 09] WU X.J., XU C., CUI C.Y., "Application of quantum evolutionary algorithm in blind source separation", *ICNC'09 Fifth International Conference on Natural Computation*, vol. 6, pp. 505–509, 2009.

[XU 13] XU J., "Analytical expressions of global quantum discord for two classes of multi-qubit states", *Physics Letters A*, vol. 377, pp. 238–242, 2013.

[YAB 87] YABLONOVITCH E., "Inhibited spontaneous emission in solid-state physics and electronics", *Physical Review Letters*, vol. 58, pp. 2059–2061, 1987.

[YAB 91a] YABLONOVITCH E., GMITTER T.J., LEUNG K.M., "Photonic band structure: the face centered-cubic case employing non spherical atoms", *Physical Review Letters*, vol. 67, no. 17, pp. 2295–2298, 1991.

[YAB 91b] YABLONOVITCH E., GMITTER T.J., MEADE R.D. *et al*., "Donor and acceptor modes in photonic band structure", *Physical Review Letters*, vol. 67, pp. 3380–3383, 1991.

[YAB 93] YABLONOVITCH E., "Photonic band-gap crystals", *Journal of Physics: Condensed Matter*, vol. 5, pp. 2443–2460, 1993.

[YEE 66] YEE K.S., "Numerical solution of initial boundary value problems involving Maxwell's equations in isotropic media", *IEEE Transactions on Antennas and Propagation*, vol. 14, pp. 302–307, 1966.

[YOS 01] YOSHIE T., VUCKOVIC J., SCHERER A. *et al*., "High-quality slab photonic crystals slab cavities", *Applied Physics Letters*, vol. 79, pp. 4289–4291, 2001.

[YU 15] YU X.D., GUO Y.Q., TONG D.M., "A proof of the Kochen–Specker theorem can always be converted to a state independent non contextuality inequality", *New Journal of Physics*, vol. 17, p. 093001, 2015.

[ZEH 70] ZEH H.D., "On the interpretation of measurement in quantum theory", *Foundations of Physics*, vol. 1, no. 1, pp. 69–76, 1970.

[ZEN 87] ZENGERLE R., "Light propagation in singly and doubly periodic planar waveguides", *Journal of Modern Optics*, vol. 34, pp. 1589–1617, 1987.

[ZHU 03] ZHU K., ZANG H., MUKHERJEE B., "A comprehensive study on next-generation optical grooming switches," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 7. pp. 1173–1186, 2003.

[ZI 03] ZI J., YU X., LI Y. *et al*., "Coloration strategies in peacock feathers", *Proceedings of the National Academy of Sciences*, vol. 100, pp. 12576–12578, 2003.

[ZIO 14] ZIOLKOWSKI A., "A numerical approach to a nonlinear propagation of light in photorefractive media", *Computer Physics Communications*, vol. 185, pp. 504–511, 2014.

[ZUR 05] ZUREK W.H., Decoherence and the Transition from Quantum to Classical-Revisited, Séminaire Poincaré, 2005.

Index

Quantum Communications in New Telecommunications Systems, First Edition.
Malek Benslama, Achour Benslama and Skander Aris.
© ISTE Ltd 2017. Published by ISTE Ltd and John Wiley & Sons, Inc.

G, H, I

K, L, M

N, O, P

Q, R, S

T, V, W, X, Y

Other titles from

in

Networks and Telecommunications

2016

AL AGHA Khaldoun, PUJOLLE Guy, ALI-YAHIYA Tara
Mobile and Wireless Networks (Advanced Network Set – Volume 2)

BATTU Daniel
Communication Networks Economy

BENSLAMA Malek, BATATIA Hadj, MESSAI Abderraouf
Transitions from Digital Communications to Quantum Communications: Concepts and Prospects

CAMARA Daniel, NIKAEIN Navid (Eds.)
Wireless Public Safety Networks 2: A Systemic Approach

CHIASSERINI Carla Fabiana, GRIBAUDO Marco, MANINI Daniele
Analytical Modeling of Wireless Communication Systems (Stochastic Models in Computer Science and Telecommunication Networks Set – Volume 1)

EL FALLAH SEGHROUCHNI Amal, ISHIKAWA Fuyuki, HÉRAULT Laurent, TOKUDA Hideyuki
Enablers for Smart Cities

PEREZ André
VoLTE and ViLTE

RAMOS Angel, LAZARO Antonio, GIRBAU David, VILLARINO Ramon
RFID and Wireless Sensors using Ultra-Wideband Technology

SENOUCI Mustapha Reda, MELLOUK Abdelhamid
Deploying Wireless Sensor Networks

VENA Arnaud, PERRET Etienne, TEDJINI Smail
Chipless RFID based on RF Encoding Particle

2015

BENSLAMA Malek, KIAMOUCHE Wassila, BATATIA Hadj
Connections Management Strategies in Satellite Cellular Networks

BENSLAMA Malek, BATATIA Hadj, BOUCENNA Mohamed Lamine
Ad Hoc Networks Telecommunications and Game Theory

BERTHOU Pascal, BAUDOIN Cédric, GAYRAUD Thierry, GINESTE Matthieu
Satellite and Terrestrial Hybrid Networks

CÂMARA Daniel
Bio-inspired Networking

CÂMARA Daniel, NIKAEIN Navid (Eds.)
Wireless Public Safety Networks 1: Overview and Challenges

CUADRA-SANCHEZ Antonio, ARACIL Javier
Traffic Anomaly Detection

JARRY Pierre, BENEAT Jacques N.
Digital Communications

LE RUYET Didier, PISCHELLA Mylène
Digital Communications 1: Source and Channel Coding

PEREZ André
LTE and LTE Advanced: 4G Network Radio Interface

PISCHELLA Mylène, LE RUYET Didier
Digital Communications 2: Digital Modulations

PUJOLLE Guy
Software Networks (Advanced Network Set – Volume 1)

2014

ANJUM Bushra, PERROS Harry
Bandwidth Allocation for Video under Quality of Service Constraints

BATTU Daniel
New Telecom Networks: Enterprises and Security

BEN MAHMOUD Mohamed Slim, GUERBER Christophe, LARRIEU Nicolas, PIROVANO Alain, RADZIK José
Aeronautical Air−Ground Data Link Communications

BITAM Salim, MELLOUK Abdelhamid
Bio-inspired Routing Protocols for Vehicular Ad-Hoc Networks

CAMPISTA Miguel Elias Mitre, RUBINSTEIN Marcelo Gonçalves
Advanced Routing Protocols for Wireless Networks

CHETTO Maryline
Real-time Systems Scheduling 1: Fundamentals
Real-time Systems Scheduling 2: Focuses

EXPOSITO Ernesto, DIOP Codé
Smart SOA Platforms in Cloud Computing Architectures

MELLOUK Abdelhamid, CUADRA-SANCHEZ Antonio
Quality of Experience Engineering for Customer Added Value Services

OTEAFY Sharief M.A., HASSANEIN Hossam S.
Dynamic Wireless Sensor Networks

PEREZ André
Network Security

PERRET Etienne
Radio Frequency Identification and Sensors: From RFID to Chipless RFID

REMY Jean-Gabriel, LETAMENDIA Charlotte
LTE Standards
LTE Services

TANWIR Savera, PERROS Harry
VBR Video Traffic Models

VAN METER Rodney
Quantum Networking

XIONG Kaiqi
Resource Optimization and Security for Cloud Services

2013

ASSING Dominique, CALÉ Stéphane
Mobile Access Safety: Beyond BYOD

BEN MAHMOUD Mohamed Slim, LARRIEU Nicolas, PIROVANO Alain
Risk Propagation Assessment for Network Security: Application to Airport Communication Network Design

BEYLOT André-Luc, LABIOD Houda
Vehicular Networks: Models and Algorithms

BRITO Gabriel M., VELLOSO Pedro Braconnot, MORAES Igor M.
Information-Centric Networks: A New Paradigm for the Internet

BERTIN Emmanuel, CRESPI Noël
Architecture and Governance for Communication Services

DEUFF Dominique, COSQUER Mathilde
User-Centered Agile Method

DUARTE Otto Carlos, PUJOLLE Guy
Virtual Networks: Pluralistic Approach for the Next Generation of Internet

FOWLER Scott A., MELLOUK Abdelhamid, YAMADA Naomi
LTE-Advanced DRX Mechanism for Power Saving

JOBERT Sébastien *et al.*
Synchronous Ethernet and IEEE 1588 in Telecoms: Next Generation Synchronization Networks

MELLOUK Abdelhamid, HOCEINI Said, TRAN Hai Anh
Quality-of-Experience for Multimedia: Application to Content Delivery Network Architecture

NAIT-SIDI-MOH Ahmed, BAKHOUYA Mohamed, GABER Jaafar, WACK Maxime
Geopositioning and Mobility

PEREZ André
Voice over LTE: EPS and IMS Networks

2012

AL AGHA Khaldoun
Network Coding

BOUCHET Olivier
Wireless Optical Communications

DECREUSEFOND Laurent, MOYAL Pascal
Stochastic Modeling and Analysis of Telecoms Networks

DUFOUR Jean-Yves
Intelligent Video Surveillance Systems

EXPOSITO Ernesto
Advanced Transport Protocols: Designing the Next Generation

JUMIRA Oswald, ZEADALLY Sherali
Energy Efficiency in Wireless Networks

KRIEF Francine
Green Networking

PEREZ André
Mobile Networks Architecture

2011

BONALD Thomas, FEUILLET Mathieu
Network Performance Analysis

CARBOU Romain, DIAZ Michel, EXPOSITO Ernesto, ROMAN Rodrigo
Digital Home Networking

CHABANNE Hervé, URIEN Pascal, SUSINI Jean-Ferdinand
RFID and the Internet of Things

GARDUNO David, DIAZ Michel
Communicating Systems with UML 2: Modeling and Analysis of Network Protocols

LAHEURTE Jean-Marc
Compact Antennas for Wireless Communications and Terminals: Theory and Design

RÉMY Jean-Gabriel, LETAMENDIA Charlotte
Home Area Networks and IPTV

PALICOT Jacques
Radio Engineering: From Software Radio to Cognitive Radio

PEREZ André
IP, Ethernet and MPLS Networks: Resource and Fault Management

TOUTAIN Laurent, MINABURO Ana
Local Networks and the Internet: From Protocols to Interconnection

2010

CHAOUCHI Hakima
The Internet of Things

FRIKHA Mounir
Ad Hoc Networks: Routing, QoS and Optimization

KRIEF Francine
Communicating Embedded Systems / Network Applications

2009

CHAOUCHI Hakima, MAKNAVICIUS Maryline
Wireless and Mobile Network Security

VIVIER Emmanuelle
Radio Resources Management in WiMAX

2008

CHADUC Jean-Marc, POGOREL Gérard
The Radio Spectrum

GAÏTI Dominique
Autonomic Networks

LABIOD Houda
Wireless Ad Hoc and Sensor Networks

LECOY Pierre
Fiber-optic Communications

MELLOUK Abdelhamid
End-to-End Quality of Service Engineering in Next Generation Heterogeneous Networks

PAGANI Pascal *et al.*
Ultra-wideband Radio Propagation Channel

2007

BENSLIMANE Abderrahim
Multimedia Multicast on the Internet

PUJOLLE Guy
Management, Control and Evolution of IP Networks

SANCHEZ Javier, THIOUNE Mamadou
UMTS

VIVIER Guillaume
Reconfigurable Mobile Radio Systems