UNIVERSITÀ DEGLI STUDI DI ROMA "LA SAPIENZA"

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Dottorato di ricerca in Fisica – XVIII ciclo

Tesi di Dottorato
Settore Disciplinare FIS/03

Quantum information processing in solid state and optical devices

Gian Luca Giorgi

Tutore
Prof. Ferdinando de Pasquale

Coordinatore del corso di dottorato
Prof. Valeria Ferrari

Novembre 2005

Abstract

The emerging field of quantum information concerns ways in which quantum mechanics can be exploited to transmit and process information. The milestones of this field are indubitably represented by the development, by C. Bennett and G. Brassard in the early 80s, of the so-called "quantum cryptography", a provably secure way of sharing a key distribution through a public channel, and by the discovery of the polynomial-time algorithm of P. Shor for finding the prime factors of large integers.

The interesting aspect to remark is that a philosophical debate about locality in quantum mechanics, usually referred as the Einstein-Podolski-Rosen paradox, originated a new method for information processing. One of peculiar aspects of quantum mechanics, the postulate of the reduction of the wave packet, considered so far as a limit, becomes a resource and projective measurements are exploited giving rise to unexpected phenomena, such as quantum teleportation.

The starting element of any description of quantum information is the qubit, the state of a two-level system, which represents the counterpart of the bit, known to be the unit of classical information. Various two-level systems are being considered as physical realization of qubits for quantum information processing. It is worth citing NMR in bulk liquids, cold ions, cold atoms, superconducting circuits (SQUIDs), semiconductor electronic devices containing electron spin and charge (quantum dots), and photons, especially in the framework of the so-called Linear

Optics Quantum Computation (LOQC). Both theoretical and experimental fronts have seen remarkable progresses in the past several years in any of these fields. Experimentalists address their attention towards a full control of coherent dynamics of extended quantum systems, while most theoreticians are motivated by the idea of deeply understanding the fundamental properties of such systems.

A solid state approach to quantum information seems to be the most likely scenario for the realization of hardware, since large-scale integration is possible within the present chip technology. On the other hand, solid state devices suffer decoherence, that is the loss of quantum behaviour because of the interaction with an external environment. Thus the study of methods and techniques to avoid decoherence are themselves an arena where to concentrate interest and energies.

Conversely, photons are, with obvious motivations, the best vehicle of information over long distances. Then, although LOQC contains non trivial aspects that it is worth considering, the natural battle ground where to use and exploit photons is the subfield of quantum communication, which concerns the possibility of manipulating and transferring qubits in the space.

This thesis arises from the fusion of two different "ways of life" inside the world of quantum information. The first one is that of my supervisor, Prof. Ferdinando de Pasquale, a physicist who has studied for long times statistical mechanics, with particular attention to the topic of phase transitions, and would apply many-body techniques to develop and characterize new configurations for the definition and the transfer of qubits. The second one derives from my prior experience in a quantum optics laboratory. I tried to preserve what I learned, and continue to think to photons and to their possible use.

Therefore the aim of this work is to provide a series of original schemes for quantum information processing both in solid state devices and in optical ones. In the latter case it is worth speaking about true experimental proposals, perfectly feasible

using today's technology, whereas, referring to solid state applications, the experimental implementation is not obvious, and the scope is that of pointing towards new methods and ideas which could stimulate experimentalists.

The thesis is articulated as follows. Chapter 1 is a brief collection of general concepts and instruments which will be used in the subsequent chapters. In particular, I shall present some of the reasons that make interesting the study of quantum information, and focus on two typical concepts, the first one being entanglement, tight connected to quantum non-locality, and the second one being decoherence, the loss of quantum behaviour in open systems due to qubit-environment coupling in the time evolution.

The original work presented here is contained in chapters 2,3,4, and 5. Chapter 2 is mostly devoted to the description of a method to create macroscopic qubits through an array of a large number of quantum-dot pairs. Starting from the very common situation where a pair of quantum dots defines a charge qubit, it will be shown how a strong interaction between nearest neighbors dot pairs creates an effective two-level system which is defined over all the array. In the thermodynamical limit, a phase transition appears at zero absolute temperature. Moreover, the analysis of decoherence effects demonstrates a counterintuitive feature: the more extended is such system, the more resilient it is against zero-temperature decoherence effects. As an application of these properties, a teleportation protocol will be applied by adiabatic variation of the system's parameters.

A more general approach to solid state quantum information processing is presented in chapter 3, where the concept of quantum bus is introduced. A quantum state, encoded in a local site, can be transferred asymptotically unchanged in a distant site, by using a chain as a channel. The main result of this part is that quantum diffusion is avoided whenever the energy of the state to transfer is outside of the energy band of the quantum bus, or when the channel has a discrete spectrum and

the energy is resonant with one of the channel energies. The model Hamiltonian introduced to describe this mechanism allows one to choose the preferred physical realization of the channel, because of the independence from the quantum statistics.

In the last two chapters (4 and 5) I shall focus my attention on optical realizations of quantum information protocols. In particular, chapter 4 will be devoted to the introduction of a scheme which allows one to realize a non-deterministic two-qubit gate using linear optics and single photons, following the idea introduced recently by Knill, Laflamme, and Milburn, and whose the present model represents a simplification. Finally, in chapter 5, I shall present a setup that could be used for cryptographic purposes. It consists in a mechanism of bit exchange between two sites which enables the sharing of a secret key. In each of two last chapters an introductory paragraph will be useful to frame the work in its own milieu.

Two appendices conclude the thesis. The appendix A contains the analytical derivation of a function defined in the third chapter, and has been introduced merely to lighten the discussion. The second appendix has a different role. In fact, I present the results of a study about the possibility of transferring quantum information through a spin chain exploiting redundant encoding methods. Being the results not completely satisfying, I decided to treat this argument without emphasizing it.

Acknowledgments

Perché questo spazio acquisti un valore reale intendo riservarlo ai ringraziamenti verso quelle persone che hanno davvero avuto un qualche ruolo nella compilazione scientifica di questa tesi.

Non posso quindi che cominciare col citare l'insostituibile contributo che ha dato al mio lavoro il Prof. de Pasquale. Egli si è rivelato eccellente motivatore ed appassionato ricercatore, rendendo facile, anche se spesso faticoso, lavorare con lui. Simone Paganelli ha avuto un ruolo altrettanto significativo, avendo lavorato quotidianamente al mio fianco negli ultimi tre anni. I risultati presentati in questa tesi sono inscindibilmente connessi alla collaborazione con loro.

Vorrei inoltre ringraziare M. Lucamarini per aver avuto col sottoscritto lunghi scambi di vedute circa la crittografia quantistica e M. Ricci per aver collaborato con me, qualche tempo fa, alla elaborazione di una tesina poi utilizzata nella stesura della parte introduttiva del quarto capitolo.

Table of contents

Chapter 1

Introductory concepts

The scope of this chapter is to review and focalize some aspects about the world of quantum information and computation and to familiarize with the language and the instruments which will be utilized widely throughout the thesis. In Sec. 1.1 a list of physical requirements to realize a quantum processor is presented. In Sec. 1.2 the concept of entanglement is introduced together with the protocol of quantum teleportation. Finally, Sec. 1.3 contains a brief description of decoherence in open systems.

1.1 Why quantum information and computation?

Quantum computation and quantum information is the study of the information processing tasks that can be accomplished using quantum mechanical systems [1]. The theoretical and experimental work carried out in the past several years has greatly clarified the potential of the field.

The first intuition about the possibility of exploiting quantum mechanics for computational purposes is due to Feynman [2], who pointed out that, being Newtonian mechanics just a limit of quantum mechanics, it is not reasonable to suppose that

systems obeying quantum laws should have the same limitations in their computational power as classical machines. The computational power of a classical machine can represent a lower bound in the quantum world.

Enlightening evidences about the potentialities of quantum information are the algorithms introduced by P. Shor and L. Grover. Shor invented an algorithm which exploited quantum parallelism to offer an exponential speed-up over classical machines for solving the problem of the factorization of large integers [3]; Grover introduced an algorithm for unstructured search problems [4].

In a quantum computer the indivisible unit of information is the qubit, that is the state of a two-level system, which represents the analog of the classical bit. A large variety of approaches has arisen towards the physical realization of qubits. Studies in such direction involve different branches as mesoscopic physics, atom physics, quantum optics, quantum electronics, superconducting device physics, NMR.

The requirements for the implementation of quantum computation have been synthesized by D. DiVincenzo [5], and are the following:

- a scalable physical system with well characterized qubits
- the ability to initialize of the qubits to a simple fiducial state
- long relevant decoherence times, much longer than the gate operation time
- a universal set of quantum gates
- a qubit-specific measurement capability

The five criteria above mentioned suffice for computational scopes. With the idea of extending the advantages deriving from quantum tools to other information-processing tasks, two further requirements are in order:

- the ability to inconvert stationary and flying qubits

- the ability to faithfully transmit flying qubits between specified locations

I shall not give a detailed description of all the issues introduced so far. The last two points raised will be largely discussed in the Chapter 3, which is devoted specifically to the study of conditions that allow one to transmit qubit in the space with high fidelity, and decoherence will be the subject of one of following paragraphs.

Here, I give just some detail about the fourth of DiVincenzo's criteria. It has been shown [6] that quantum gates operating on just two qubits at a time are sufficient to construct a general quantum circuit.

1.2 Entanglement and teleportation

Entanglement is a distinctive feature of quantum mechanics and a fundamental resource for quantum information.

Given a Hilbert state $\mathcal{H} = \otimes_{i=1}^{n} \mathcal{H}_i$, a quantum pure state $|\Psi\rangle$ is separable with respect to the partition $\{\mathcal{H}_1, \ldots \mathcal{H}_n\}$ when it admits the following decomposition:

$$|\Psi\rangle = \otimes_{i=1}^{n} |\psi\rangle_i \,, \qquad |\psi\rangle_i \in \mathcal{H}_i. \tag{1.1}$$

If this condition is not satisfied, $|\Psi\rangle$ is said to be entangled. An example of two-qubit entangled state is the singlet state of two spin 1/2 :

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle\right). \tag{1.2}$$

This state is one of four so-called Bell states (known also as EPR, or Einstein-Podolski-Rosen pairs [7]), which represent a complete set of vectors in the two-qubit state. Using conventional notations they are

$$\begin{aligned} \left|\Psi^\pm\right\rangle &= \frac{1}{\sqrt{2}} \left(|01\rangle \pm |10\rangle\right), \\ \left|\Phi^\pm\right\rangle &= \frac{1}{\sqrt{2}} \left(|00\rangle \pm |11\rangle\right). \end{aligned} \tag{1.3}$$

When the state under study is not a pure one, but it is a statistical mixture ρ, the definition of entanglement is generalized as follows. Given the composite space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \mathcal{H}_l$, the state ρ is called separable if it can be written as

$$\rho = \sum_i \mu_i \rho_i^{(1)} \otimes \rho_i^{(2)} \otimes \ldots \rho_i^{(l)}, \tag{1.4}$$

where $\rho_i^{(j)} \in \mathcal{H}_j$, and with weights $\mu_i > 0$ satisfying the sum rule $\sum_i \mu_i = 1$. Otherwise, it is entangled.

Quantifying the entanglement degree of a multipartite state is not a trivial question. The exclusive requirement for a function of a multipartite quantum state to be a good measure of entanglement is that it be non-increasing, on average, under the set of local quantum operations and classical communication (LOCCs). When dealing with pure bipartite states, a natural way to measure entanglement is to use the "entropy of entanglement", which derives from the definition of Von Neumann entropy of a state ρ:

$$S = -\mathrm{Tr}\left\{\rho \log_2 \rho\right\}. \tag{1.5}$$

Given a bipartite system $\mathcal{H}_1 \otimes \mathcal{H}_2$ and a state $|\psi\rangle$the entropy of entanglement is

$$E_S = S\left(\rho_1\right) = S\left(\rho_2\right), \tag{1.6}$$

where ρ_1 (ρ_2) is the reduced density matrix:

$$\rho_{1(2)} = \mathrm{Tr}_{2(1)}\left\{|\psi\rangle\langle\psi| \log_2\left(|\psi\rangle\langle\psi|\right)\right\}, \tag{1.7}$$

where Tr_i indicates the partial trace on the subsystem i.

On the other hand, if the state is a statistical mixture, classical correlations sums to quantum ones, and entropy of entanglement is no longer a good indicator. In this case, we recur to "concurrence" C, introduced by W. Wootters [8], defined as follows. Given a bipartite state ρ and its spin-flip $\tilde{\rho} = \sigma_y \otimes \sigma_y \rho^* \sigma_y \otimes \sigma_y$ (ρ^* denotes the complex conjugate of ρ and σ_y is one of Pauli matrices),

$$C\left(\rho\right) = \max\left\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\right\} \tag{1.8}$$

where the λ_is are the square roots of the eigenvalues of the non-Hermitian matrix $\rho\tilde{\rho}$.

Entanglement is responsible of nonlocal quantum correlation and allows quantum information to overcome some of the limitations posed by classical information, as exemplified by some peculiar application, as dense coding and teleportation.

Quantum teleportation is a counterintuitive and fascinating idea which relies on entanglement in a indissoluble way [9]. Let us suppose that Alice has an unknown quantum state $|\chi\rangle$ and wants to send it to Bob, who is far apart. Furthermore, suppose that they can communicate only through a classical channel. Entanglement is the resource that allows them to perfectly accomplish the transfer. A quantitative description of teleportation can be done as follows. Assume that Alice has the state $|\chi_1\rangle = \alpha\,|0_1\rangle + \beta\,|1_1\rangle$ and she does not know either α nor β. Assume also that Alice and Bob share an EPR pair, for instance $\left|\Psi^-_{2,3}\right\rangle$. Thus the initial state is

$$|\Psi_{1,2,3}\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0_1\rangle + \beta\,|1_1\rangle\right]\left[|0_2 1_3\rangle - |1_2 0_3\rangle\right] \tag{1.9}$$

A simple algebraic manipulation allows one to write

$$\begin{aligned} |\Psi_{1,2,3}\rangle \;=\; & \frac{1}{2}[\left|\Phi^+_{1,2}\right\rangle(\alpha\,|1_3\rangle - \beta\,|0_3\rangle) + \left|\Phi^-_{1,2}\right\rangle(\alpha\,|1_3\rangle + \beta\,|0_3\rangle) \\ & + \left|\Psi^+_{1,2}\right\rangle(-\alpha\,|0_3\rangle + \beta\,|1_3\rangle) + \left|\Psi^-_{1,2}\right\rangle(\alpha\,|0_3\rangle + \beta\,|1_3\rangle)] \end{aligned} \tag{1.10}$$

or, better,

$$|\Psi_{1,2,3}\rangle = \frac{1}{2}\left[\left|\Phi^+_{1,2}\right\rangle i\sigma^y_3\,|\chi_3\rangle + \left|\Phi^-_{1,2}\right\rangle \sigma^x_3\,|\chi_3\rangle + \left|\Psi^+_{1,2}\right\rangle \sigma^z_3\,|\chi_3\rangle + \left|\Psi^-_{1,2}\right\rangle |\chi_3\rangle\right], \tag{1.11}$$

where σ^x_3,σ^y_3, and σ^z_3 are the standard Pauli matrices acting on the Hilbert space of the third qubit. Then, Alice performs a local Bell measurement (that is a measurement in the basis represented by the Bell states) on the qubits 1 and 2, and transmits the result on the classical channel. Bob receives the classical data and acts on the third qubit with a proper unitary operation in order to recover the state $|\chi\rangle$. For instance, if Alice would measure $\left|\Phi^-_{1,2}\right\rangle$, Bob's had to make the unitary rotation σ^x_3, and so on. Fig. 1.1 illustrates in a pictorial way the process of teleportation.

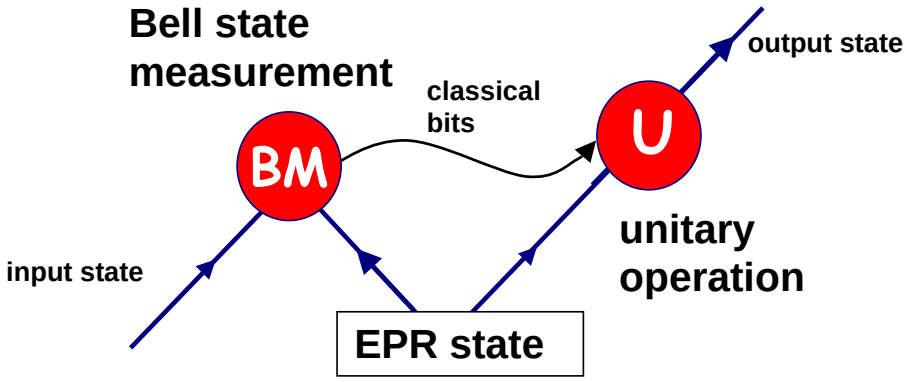

Figure 1.1. Schematic description of the teleportation protocol. BM stays for Bell measurement , while U indicates the classically selected unitary transformation.

1.3 Decoherence

It is a common wisdom that a quantum state will, soon or later, loose coherence due to the interaction with an environment. If the whole system is described by quantum mechanics, because of the time reversibility of the evolution, decoherence is observed in the time scale where energy has been dispersed in the degrees of freedom of the environment [10, 11]. This time scale is macroscopic if the number of degrees of freedom of the environment is macroscopic. On the time scale of decoherence, the environment is considered to have a continuous energy spectrum and decoherence occurs when the energies of the isolated quantum system belong to the spectrum of the environment. Many basic ideas have been developed in various formulations, such as master equation to study the behaviour of open systems.

As said in Sec. 1.1, one of essential ingredients to build a quantum computer is to deal with decoherence times much longer than the gate operation time. Then, it is essential to identify those systems that interact weakly with their environment, or, better, find particular subspaces whose evolution is preserved from dissipation. In this latter case one speaks about "decoherence-free subspaces" [12].

A very general method to treat the problem of decoherence is represented by the

use of system-bath theories. Roughly speaking, the world is divided in two parts, "system" and "bath". The system is the part we are really interested in, while the bath is the rest of the world, and we do not care about what happens there. The Hilbert space is defined as the tensor product system+bath:

$$\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_B, \tag{1.12}$$

with obvious notations, while the Hamiltonian is

$$H = H_S + H_B + H_{SB}, \tag{1.13}$$

where the last term takes into account interaction between system and bath. Whenever $H_{SB} = 0$, the system is isolated from the environment and the usual quantum mechanical treatment takes place. Starting at the time $t = 0$ from a factorized state ($\rho(0) = |S\rangle\langle S| \otimes |B\rangle\langle B|$), the effect of the interaction is to entangle the system with the bath. Then, at any time $t > 0$, the whole system is no longer factorized. The typical tool to isolate the evolution of the system alone is the reduced density matrix:

$$\rho_S(t) = \mathrm{Tr}_B\left\{\rho_{SB}(t)\right\}, \tag{1.14}$$

where the symbol Tr_B denotes the partial trace realized on the bath's degrees of freedom. As a consequence of the system-bath entanglement, $\rho_S(t)$ is a statistical mixture. In general there is no way to study exactly the time evolution of the system, and approximations are in order. Due to the interaction, the evolution of the system implies the excitation of phonons in the bath. As we shall see in the next chapter, it is possible that, considering a weak coupling regime and zero temperature, all bath's states which present phonons can be neglected to the leading order in the coupling constant, and only self-energy contribution are kept. In that case, the calculation of the Green functions for the system is all we must do. In practice, entanglement between system and bath manifests itself through the corrections to the unperturbed system's energies.

Chapter 2

Elementary excitations of an array of double quantum dots

Realizing macroscopic qubits would be very advantageous for many aspects. In fact, the macroscopic character implies an enhancement of robustness with respect to decoherence.

Moreover, it is well known that a quantum system which undergoes a phase transition lives in one of a particular set of states, for a time which becomes infinitely large in the thermodynamical limit. Considering the number of states large but finite, it appears an energy separation between these states, and oscillations are expected, if the system is initialized in a state which is a superposition of these eigenstates. In particular, if the ground state is twofold degenerate, one can associate these states to a macroscopic quantum bit.

In this chapter I study of the elementary excitations of an array of double quantum dots (DQDs), showing that this physical system is a suitable candidate as a macroscopic qubit. In Sec. 2.1 I introduce the charge qubit and define the nature of interactions that appear in a DQD array. Sec. 2.2 is devoted to the study of the time evolution of the array. As a result, an effective two-level system behaviour will

appear [13]. In Sec. 2.3 the study of decoherence effects is performed by means of the introduction of a bath of acoustic phonons interacting with the electron charge. The robustness of the array in the macroscopic limit is the main result of this chapter. Finally (Sec. 2.4), the time evolution of the DQD array is exploited to achieve quantum teleportation [14]. A brief conclusion is given in Sec. 2.5.

2.1 Quantum dots and quantum information

Quantum dots (QDs) are artificial atoms (molecules) in which atomic (molecular)-like electronic states can be controlled with external voltages [15, 16]. They provide confinement in three spatial dimensions and have a size that can range from a few nanometers up to one hundred nanometers, which is comparable to the de Broglie wavelength of electrons in semiconductors, showing well-separated discrete levels for electronic states. The first idea to realize the qubit using pairs of coupled of quantum dots is due to D. Loss and D. DiVincenzo [17]. In their proposal, two QDs, each having one excess electron are coupled through electric gates, and the qubit is given by the superposition of the two-spin state. Alternatively, charge states can be used to define the qubit. In this scenario two coupled quantum dots share just one excess electron, which can stay coherently around the first or the second dot, defining in such a way a two-level state. The charge can oscillate between the two dots through a tunneling barrier, whose height is determined by an external electrostatic potential. Coherent charge oscillations in these systems have been observed experimentally [18, 19]. The array we have in mind has the geometry of Fig. 2.1. There is tunneling between dots of each of N pairs, and nearest neighbors interaction due to electrostatic repulsion between electrons which appears only between dots belonging to the same row, while dots of different pairs and different rows never interact. Double occupation on a single dot, as well as double occupation on a DQD

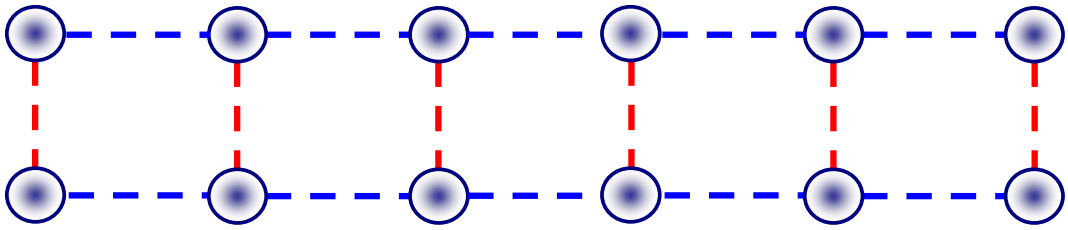

Figure 2.1. Array of double quantum dots. Red lines indicate tunneling between dots of the same pair. Blue lines represent electrostatic repulsion

will be completely neglected. The model Hamiltonian is

$$H_S = U \sum_{l=1}^{N-1} \sum_{\alpha=1}^{2} n_{l,\alpha} n_{l+1,\alpha} - w \sum_{l=1}^{N} \left(c_{l,1}^{\dagger} c_{l,2} + h.c. \right), \tag{2.1}$$

where $c_{l,\alpha}^{\dagger}$ creates an electron on the l(th) dot on the α(th) row of the array and $n_{l,\alpha} = c_{l,\alpha}^{\dagger} c_{l,\alpha}$, and having indicating with w the tunneling amplitude and with U the electrostatic energy.

Each pair can be mapped to spin 1/2 system, where up and down correspond to the extra charge on one of the two dots, and Coulomb interaction between pairs corresponds to antiferromagnetic interaction. Therefore, making the mapping $\sigma_l^z = (n_{l,1} - n_{l,2})$ and $\sigma_l^x = (c_{l,1}^{\dagger} c_{l,2} + h.c.)$, the Hamiltonian describing this system becomes

$$H = -w \sum_{l=1}^{N} \sigma_l^x + \frac{U}{2} \sum_{l=1}^{N-1} \left(\sigma_l^z \sigma_{l+1}^z + 1 \right). \tag{2.2}$$

2.2 Asymptotic two-level behaviour of the DQD array

The Hamiltonian of Eq. (2.2) reproduces exactly the one-dimensional Ising model in a transverse magnetic field, whose solution has been carried out some decades ago [20, 21, 22]. It is our intention to obtain, using perturbation theory, some asymptotic limit that shows very interesting and unexplored features. To do it, we adopt the resolvent method [23], writing

$$H = H_0 + H_I, \tag{2.3}$$

and identifying respectively $-w \sum \sigma_l^x$ with H_I and $U/2 \left[\sum_l \left(\sigma_l^z \sigma_{l+1}^z + 1 \right) \right]$ with H_0. The idea is to assume $U \gg w$ and consider H_I as a perturbation with respect to H_0. The resolvent method allows one to write the evolution of a generic state $|\psi\rangle$in the Laplace space as

$$|\psi(\omega)\rangle = \frac{1}{\omega - H} |\psi(t=0)\rangle \tag{2.4}$$

or

$$|\psi(\omega)\rangle = \frac{1}{\omega - H_0}|\psi(t=0)\rangle + \frac{1}{\omega - H}H_I\frac{1}{\omega - H_0}|\psi(t=0)\rangle . \tag{2.5}$$

The absence of boundary conditions in Eq. (2.2) plays an essential role in the following development. Let us define the two antiferromagnetic states (with zero Coulomb energy) $|\Phi\rangle \equiv |\downarrow,\uparrow,\downarrow,\uparrow,\ldots\uparrow\rangle$ and $|\Psi\rangle \equiv |\uparrow,\downarrow,\uparrow,\downarrow,\ldots\downarrow\rangle$ and apply H_I to each of them. Applying H_I on $|\Phi(t=0)\rangle$ the system is driven in a new configuration labeled as $|\Phi_1(t=0)\rangle$. The action of H_I generates a sum of states each of them differentiates from $|\Phi(t=0)\rangle$ due to one spin flip in a different place along the array. Here it is important to note that flips on the first and the last qubit put the system in a state with Coulomb energy U, while all intermediate transitions lead to a state with a $2U$ electrostatic energy. In the limit of U large with respect to w, we shall neglect all configurations involving intermediate states with energy greater than U. In each step of a repeated application of H_I it is possible to go towards new configurations or to come back. Then, for $n > 0$, we write

$$H_I|\Phi_n(t=0)\rangle = -w\left[|\Phi_{n-1}(t=0)\rangle + |\Phi_{n+1}(t=0)\rangle\right]. \tag{2.6}$$

After N steps the system reaches $|\Psi\rangle$ and after $2N$ steps it comes back to the initial configuration. Relabeling $|\Psi\rangle = |\Phi_N\rangle$ and $|\Phi\rangle = |\Phi_{2N}\rangle = |\Phi_0\rangle$, we study the evolution in the Laplace space:

$$|\Phi_n(\omega)\rangle = \frac{1}{\omega - H}|\Phi_n(t=0)\rangle \tag{2.7}$$

or

$$|\Phi_n(\omega)\rangle = \frac{1}{\omega - H_0}|\Phi_n(t=0)\rangle - w\frac{1}{\omega - H}H_1\frac{1}{\omega - H_0}|\Phi_n(t=0)\rangle . \tag{2.8}$$

Noting that

$$\frac{1}{\omega - H_0}|\Phi_n(t=0)\rangle = \frac{1}{\omega - U + U(\delta_{n,0} + \delta_{n,N})}|\Phi_n(t=0)\rangle , \tag{2.9}$$

we obtain the following equation which holds for all n from 0 to $2n-1$:

$$(\omega - U)\left|\Phi_n(\omega)\right\rangle = \left|\Phi_n(t=0)\right\rangle - w\left[\left|\Phi_{n-1}(\omega)\right\rangle + \left|\Phi_{n+1}(\omega)\right\rangle\right] - U\left(\delta_{n,0}+\delta_{n,N}\right)\left|\Phi_n(\omega)\right\rangle. \tag{2.10}$$

The system is solved by means of the discrete Fourier transform defined through

$$\left|\widetilde{\Phi}_k(\omega)\right\rangle = \frac{1}{\sqrt{2N}}\sum_{n=0}^{2N-1}\left|\Phi_n(\omega)\right\rangle e^{ink}, \tag{2.11}$$

$$\left|\Phi_n(\omega)\right\rangle = \frac{1}{\sqrt{2N}}\sum_{k=0}^{2N-1}\left|\widetilde{\Phi}_k(\omega)\right\rangle e^{-ink}. \tag{2.12}$$

As a consequence of periodicity conditions, $k = 2\pi n/N$.

From Eq. 2.10 follows

$$\left[\omega - U + 2w\cos k\right]\left|\widetilde{\Phi}_k(\omega)\right\rangle = \left|\widetilde{\Phi}_k(t=0)\right\rangle - \frac{U}{\sqrt{2N}}\left(\left|\Phi_0(\omega)\right\rangle + e^{iNk}\left|\Phi_N(\omega)\right\rangle\right). \tag{2.13}$$

It is now possible to extract two equations connecting $|\Phi_0\rangle$ to $|\Phi_N\rangle$:

$$\left|\Phi_0(\omega)\right\rangle = \frac{\left[1+B_0(\omega)\right]\left|A_0(\omega)\right\rangle - B_N(\omega)\left|A_N(\omega)\right\rangle}{\left[1+B_0(\omega)\right]^2 - B_N^2(\omega)}, \tag{2.14}$$

$$\left|\Phi_N(\omega)\right\rangle = \frac{\left[1+B_0(\omega)\right]\left|A_N(\omega)\right\rangle - B_N(\omega)\left|A_0(\omega)\right\rangle}{\left(1+B_0(\omega)\right)^2 - B_N^2(\omega)}, \tag{2.15}$$

where

$$\left|A_n(\omega)\right\rangle = \frac{1}{\sqrt{2N}}\sum_{k=0}^{2\pi\left(\frac{2N-1}{2N}\right)}\frac{e^{-ink}\left|\widetilde{\Phi}_k(t=0)\right\rangle}{\omega - U + 2w\cos k}, \tag{2.16}$$

$$B_n(\omega) = \frac{1}{2N}\frac{U}{\omega - U}\sum_{q=0}^{2N-1}\frac{e^{-in\frac{\pi}{N}q}}{1 - a(\omega)\cos\frac{\pi}{N}q}, \tag{2.17}$$

with $a(\omega) = 2w/(U-\omega)$ and noting that $B_N = B_{-N}$.

The asymptotic behaviour is determined by values of ω close to zero. Then $a(\omega) << 1$ and the denominator of $B_n(\omega)$ reads as geometric series:

$$B_n(\omega) = \frac{1}{2N}\frac{U}{\omega - U}\sum_{q=0}^{2N-1}e^{-in\frac{\pi}{N}q}\sum_{l=0}^{\infty}a^l(\omega)\cos^l\frac{\pi}{N}q, \tag{2.18}$$

or

$$B_n(\omega) = \frac{1}{2N}\frac{U}{\omega - U}\sum_{q=0}^{2N-1}\sum_{l=0}^{\infty}\sum_{m=0}^{l}\binom{l}{m}\left(\frac{a(\omega)}{2}\right)^l \exp\left[i\frac{\pi}{N}(l-2m-n)\,q\right]. \quad (2.19)$$

The sum over q gives

$$B_n(\omega) = \frac{1}{2N}\frac{U}{\omega - U}\sum_{l=0}^{\infty}\sum_{m=0}^{l}\binom{l}{m}\left(\frac{a(\omega)}{2}\right)^l \frac{1 - e^{2i\pi(l-2m-n)}}{1 - e^{i\frac{\pi}{N}(l-2m-n)}}. \quad (2.20)$$

The condition for a non vanishing $B_n(\omega)$ is $(l-2m-n) = 2NK$, where K is any integer between $-\infty$ and $+\infty$:

$$B_n(\omega) = \frac{U}{\omega - U}\sum_{l=0}^{\infty}\sum_{m=0}^{l}\frac{l!}{m!\,(l-m)!}\left(\frac{a(\omega)}{2}\right)^l \delta_{(l-2m-n),2NK}, \quad (2.21)$$

or, using the Kronecker Delta function

$$B_n(\omega) = \frac{U}{\omega - U}\sum_{l=0}^{\infty}\sum_{K=-\infty}^{\infty}\frac{l!}{\left(\frac{l+n+2NK}{2}\right)!\left(\frac{l-n-2NK}{2}\right)!}\left[\frac{a(\omega)}{2}\right]^l. \quad (2.22)$$

Since the coefficients of a Newton's binomial formula have to be real and positive, in the limit $a(\omega) << 1$ we obtain

$$B_0(\omega) \simeq \frac{U}{\omega - U}(1 + M), \quad (2.23)$$

where

$$M = 1 - \frac{1}{2N}\sum_{q=0}^{2N-1}\frac{1}{1 - \frac{2w}{U}\cos q} \quad (2.24)$$

contains powers of w/U and has to be calculated at the desired order in q, and

$$B_N(\omega) \simeq -\frac{1}{2^N}\left(\frac{2w}{U}\right)^N. \quad (2.25)$$

Here we note that the last contribution cannot be ignored because it gives rise to the energy separation between $|\Phi_0\rangle$ and $|\Phi_N\rangle$.

Furthermore we obtain

$$|A_0(\omega)\rangle \simeq \frac{1}{U}|\Phi_0(t=0)\rangle \quad (2.26)$$

and

$$|A_N(\omega)\rangle \simeq \frac{1}{U}|\Phi_N(t=0)\rangle . \tag{2.27}$$

As a result, after an inverse Laplace transform, we get

$$|\Phi_0(t)\rangle = e^{iMUt}\left[|\Phi_0(t=0)\rangle \cos \Delta t + i\,|\Phi_N(t=0)\rangle \sin \Delta t\right] + O\left(\frac{w}{U}\right), \tag{2.28}$$

and

$$|\Phi_N(t)\rangle = e^{iMUt}\left[|\Phi_N(t=0)\rangle \cos \Delta t + i\,|\Phi_0(t=0)\rangle \sin \Delta t\right] + O\left(\frac{w}{U}\right), \tag{2.29}$$

having introduced the energy gap

$$\Delta = 2w\,(2w/U)^{N-1} . \tag{2.30}$$

We eventually obtain the long time behaviour of a two-level system with energy separation exponentially vanishing in the large N limit. Actually, in Ref. [20] (see equation (3.32c)) the eigenvalue of Eq. 2.30 was derived. On the basis of this result the phenomenon of asymptotic degeneracy was established and shown to be directly related to the appearance of the ordered phase in the large N limit.

The result just obtained shows that in the limit of weak tunneling amplitude, the array behaves as an effective qubit defined in the basis $\{|\Phi_0(t)\rangle, |\Phi_N(t)\rangle\}$. Transitions from one state to the other are possible and require the transition through N intermediate configurations. This is the cause of the exponential growth of the transition frequency Δ. In the limit $N \to \infty$ the phase space is divided in two separate regions that cannot communicate. Then there is a phase transition associate to this symmetry breaking.

2.3 Decoherence effects in the DQD evolution

As said in the concluding remarks of Sec. 2.2, the two-level behaviour of the DQD array emerges whenever $w \ll U$. On the other hand, the computational time required for any kind of logical operation grows with Δ, and decoherence effects can

limit the length of the array.

Under these premises, a study of decoherence is in order. The main environmental effect to consider is due to the presence of acoustic phonons which interact with the electron charge of any quantum dot [24]. The overall Hamiltonian describing the array-phonon bath interaction is

$$H = H_S + H_B + H_{SB}, \tag{2.31}$$

$$H_S = -w \sum_l \sigma_l^x + \frac{U}{2} \sum_l \left(\sigma_l^z \sigma_{l+1}^z + 1 \right), \tag{2.32}$$

$$H_B = \sum_{\mathbf{q}} \omega_{\mathbf{q}} a_{\mathbf{q}}^\dagger a_{\mathbf{q}}, \tag{2.33}$$

$$H_{SB} = \sum_{\mathbf{q},l} g_{\mathbf{q}} n_l e^{iq \cos\theta l} \left(a_{\mathbf{q}}^\dagger + a_{-\mathbf{q}} \right), \tag{2.34}$$

where the symbols H_S,H_B, and H_{SB} have been already introduced in Sec. 1.3. We indicate with θ the angle between the phonon mode $\mathbf{q}$ and the dot chain direction. This notation is useful for describing a generic d-dimensional environment coupled with a one-dimensional system. The constant $g_{\mathbf{q}}$ represents the coupling of the dot charge with the mode $\mathbf{q}$. The explicit mathematical expression for $g_{\mathbf{q}}$ depends on the specific configuration of the system and the type of interaction. In Ref. [25] the explicit form for $g_{\mathbf{q}}$ in some remarkable case is given.

The system introduced represents a variation of the spin-boson model [26], whose exact solution is not known. In the following we shall assume a regime of zero temperature and calculate, through the resolvent method, a solution using perturbation theory. At the initial time $t = 0$ system and bath are uncoupled: $|\Xi(t=0)\rangle = |S\rangle \otimes |0\rangle$, where $|0\rangle$ is the vacuum phonon state. The time evolution of the state $|\Xi(t)\rangle = \exp(-iHt)\,|\Xi(t=0)\rangle$ is studied in the complex Laplace space. Using the identity already introduced in Eq. (2.5) and performing a projection on the vacuum phonon state, we define a new system state $|\Phi_S(\omega)\rangle = \langle 0|\Xi(\omega)\rangle$ that

obeys to the evolution equation

$$|\Phi_S(\omega)\rangle = \frac{1}{\omega - H_S}|\Phi_S(t=0)\rangle + \langle 0|\frac{1}{\omega - H_S}H_{SB}\frac{1}{\omega - H}|\Xi(t=0)\rangle . \qquad (2.35)$$

Here the bath ground state energy is set to zero, $H_0 = H_S + H_B$ and $H_I = H_{SB}$.

The aim of this derivation is to keep only self-energy contributions to $|\Phi_S(\omega)\rangle$, which can give rise to an imaginary part, neglecting the rest. To feature the important terms, first we iterate $(\omega - H)^{-1}$ inside the right hand side of Eq. (2.35) and introducing a complete set of intermediate phonon states:

$$\begin{aligned} |\Phi_S(\omega)\rangle &= \frac{1}{\omega - H_S}|\Phi_S(t=0)\rangle + \langle 0|\frac{1}{\omega - H_S}H_{SB}\frac{1}{\omega - H_S - H_B}|\Xi(t=0)\rangle + \\ &\sum_k \langle 0|\frac{1}{\omega - H_S}H_{SB}\frac{1}{\omega - H_S - H_B}H_{SB}|k\rangle\langle k|\frac{1}{\omega - H}|\Xi(t=0)\rangle \end{aligned} \qquad (2.36)$$

The term of the sum leading to self-energy corresponds to $k = 0$, since the element $\langle 0|(\omega - H)^{-1}|\Xi(t=0)\rangle$ is exactly $|\Phi_S(\omega)\rangle$. Then, all other linear and quadratic contributions in H_{SB} will be neglected. Hence, Eq. 2.36 becomes

$$\left[1 - \frac{1}{\omega - H_S}G(H_S)\right]|\Phi_S(\omega)\rangle = \frac{1}{\omega - H_S}|\Phi_S(t=0)\rangle , \qquad (2.37)$$

where

$$G(H_S) = \langle 0|H_{SB}\frac{1}{\omega - H_S - H_B}H_{SB}|0\rangle \qquad (2.38)$$

is the self-energy operator acting on the system subspace. The right term of Eq. (2.37) describes the evolution of the macroscopic state isolated from phonons. As we have shown in Sec. 2.2, in the limit of $w/U \ll 1$, the macroscopic dot chain behaves as a two level system oscillating between the H_S's asymptotic eigenstates

$$|\pm\rangle = 2^{-1/2}(|\Phi\rangle \pm |\Psi\rangle) \qquad (2.39)$$

with energies $E_\pm$. So, Eq. (2.37) becomes

$$\begin{aligned} \left[1 - \frac{1}{\omega - H_S}G(H_S)\right]|\Phi_S(\omega)\rangle &= \frac{1}{\omega - E_+}|+\rangle\langle +|\Phi_S(t=0)\rangle \\ &+ \frac{1}{\omega - E_-}|-\rangle\langle -|\Phi_S(t=0)\rangle . \end{aligned} \qquad (2.40)$$

Noting that the operator $G(H_S)$ maps the subspace spanned by $|\pm\rangle$ into itself, it is possible to reduce Eq. (2.40) in terms of two coupled equations:

$$\left(\omega - E_+ - G^{++}\right)\langle +|\Phi_S(\omega)\rangle - G^{+-}\langle -|\Phi_S(\omega)\rangle = \langle +|\Phi_S(t=0)\rangle, \quad (2.41)$$

$$\left(\omega - E_- - G^{--}\right)\langle -|\Phi_S(\omega)\rangle - G^{-+}\langle +|\Phi_S(\omega)\rangle = \langle -|\Phi_S(t=0)\rangle, \quad (2.42)$$

where $G^{\pm\pm} = \langle \pm| G |\pm\rangle$.

To the leading order in the system-bath coupling, we obtain

$$\langle +|\Phi_S(\omega)\rangle = \frac{1}{\omega - E_+ - G^{++}}\langle +|\Phi_S(t=0)\rangle, \quad (2.43)$$

$$\langle -|\Phi_S(\omega)\rangle = \frac{1}{\omega - E_- - G^{--}}\langle -|\Phi_S(t=0)\rangle. \quad (2.44)$$

The solution in the time domain is obtained assuming first the correction introduced by the matrix elements of G as negligible, and then calculating the latter in $\omega = E_+$ or $\omega = E_-$.

For instance, the integral

$$\int_C \frac{e^{-i\omega t}}{\omega - E_+ - G^{++}} d\omega \quad (2.45)$$

is calculated assuming first $G^{++} = 0$, obtaining for the pole $\omega = E_+$, and then substituting this value inside G^{++}, which depends on ω. After, the principal value of G^{++} will be ignored, and only the imaginary part will matter.

In order to check the validity of the approximation performed, let us apply our method to a model whose solution is already known. We introduce a double quantum dot in contact with a bosonic bath with Hamiltonian $H = H_S + H_B + H_{SB}$, where

$$H_S = \frac{\varepsilon}{2}\sigma_z + T\sigma_x, \quad (2.46)$$

$$H_B = \sum_q \omega_q a_q^\dagger a_q, \quad (2.47)$$

$$H_{SB} = \frac{1}{2}\sigma_z \sum_q g_q \left(a_q^\dagger + a_q\right). \quad (2.48)$$

This model has been discussed extensively in Ref. [24]. Here a one-dimensional bath is considered for simplicity. Labeling with $|L\rangle$ and $|R\rangle$ the eigenstates of σ_z with respective eigenvalues $+1$ and-1, the eigenstates of H_S are

$$|\pm\rangle = \frac{1}{N_\pm}\left[\pm 2T\,|L\rangle + (\Delta \mp \varepsilon)\,|R\rangle\right], \tag{2.49}$$

where $\Delta = \sqrt{\varepsilon^2 + 4T^2}$ and $N_\pm = \sqrt{(\Delta \mp \varepsilon)^2 + 4T^2}$ while the respective eigenvalues are $\varepsilon_\pm = \pm\frac{1}{2}\Delta$.

By inversion we obtain

$$|L\rangle = N_+\frac{\Delta+\varepsilon}{4T\Delta}\,|+\rangle - N_-\frac{\Delta-\varepsilon}{4T\Delta}\,|-\rangle, \tag{2.50}$$

$$|R\rangle = \frac{N_+}{2\Delta}\,|+\rangle + \frac{N_-}{2\Delta}\,|-\rangle. \tag{2.51}$$

Eq. 2.37 has now to be solved using

$$G(H_S) = \frac{1}{4}\sum_q |g_q|^2\,\sigma_z\frac{1}{\omega-\omega_q-H_S}\sigma_z. \tag{2.52}$$

We need to calculate $\langle+|\,G(H_S)\,|+\rangle$ and $\langle-|\,G(H_S)\,|-\rangle$. Actually, obtaining G^{++} will be enough, due the intrinsic robustness of the ground state $|-\rangle$ [27] which implies that G^{--} has to be zero (this feature is easily checked in the present formalism). To do it first we write $|+\rangle$ in the $|L,R\rangle$ basis, then apply σ_z, come back in the $|\pm\rangle$ basis in order to apply $(\omega-\omega_q-H_S)^{-1}$, rewrite the new state through $|L,R\rangle$ to apply the second σ_z operator, and finally re-express the result in terms of $|+\rangle$ and $|-\rangle$. The result is

$$G^{++} = \frac{1}{4}\sum_q |g_q|^2\left[\frac{1}{\omega-\omega_q-\frac{\Delta}{2}}\left(\frac{\varepsilon}{\Delta}\right)^2 + \frac{1}{\omega-\omega_q+\frac{\Delta}{2}}\left(\frac{\Delta-\varepsilon}{\Delta}\right)^2\right]. \tag{2.53}$$

The sum over q is performed as an integral through the introduction of the density of states ρ which is assumed to be different from zero only for positive values of its argument [24]. The second term inside the square bracket gives the contribution to the imaginary part, which is $\gamma = -\left[\pi T^2\rho(\Delta)\right]/\Delta^2$. The evolution is thus

$$\langle+|\Phi_S(t)\rangle = \langle+|\Phi_S(t=0)\rangle\,e^{-i\frac{\Delta}{2}t}e^{-\pi\frac{T^2}{\Delta^2}\rho(\Delta)t}, \tag{2.54}$$

$$\langle -|\Phi_S(t)\rangle = \langle -|\Phi_S(t=0)\rangle\, e^{i\frac{\Delta}{2}t}. \tag{2.55}$$

The density matrix in the basis $|\pm\rangle$ is then

$$\rho(t) = \begin{pmatrix} \rho^{++}(0)\, e^{-2\gamma t} & \rho^{-+}(0)\, e^{-\gamma t} e^{i\Delta t} \\ \rho^{-+}(0)\, e^{-\gamma t} e^{i\Delta t} & 1-\rho^{++}(0)\, e^{-2\gamma t} \end{pmatrix}. \tag{2.56}$$

with the same dephasing rate obtained in [24], in the regime of zero temperature, using markovian assumptions.

After this digression, let us come back to our main problem, that is the study of decoherence of the DQD array. According to the previous analysis we can limit ourself to consider only the first two states $|\pm\rangle$ of the array. The decoherence rate will be however modified by the extensive interaction with the bath.

We have to calculate the matrix elements of $G(H_S)$ in the subspace of $|+\rangle$ and $|-\rangle$ taking into account the particular system-bath interaction H_{SB} defined in Eq. 2.34. Here

$$G(H_S) = \sum_{\mathbf{q},l,l'} e^{iq\cos\theta(l-l')}\, |g_{\mathbf{q}}|^2\, n_{l'} \frac{1}{\omega - H_S - \omega_{\mathbf{q}}} n_l, \tag{2.57}$$

where the sum over l,l' runs over the array sites where electrons are present.

We choose the basis elements $|+\rangle$ and $|-\rangle$ defined in Eq. (2.39). The matrix element of $G(H_S)$ are obtained explicitly. Considering that $|\Psi\rangle$ and $|\Phi\rangle$ have excess electrons in alternate sites,

$$\sum_l n_l e^{iql\cos\theta}\, |\Phi\rangle = \sum_{l=0}^{N-1} e^{i2ql\cos\theta}\, |\Phi\rangle\,, \tag{2.58}$$

$$\sum_l n_l e^{iql\cos\theta}\, |\Psi\rangle = \sum_{l=0}^{N-1} e^{i2q(l+1)\cos\theta}\, |\Psi\rangle\,. \tag{2.59}$$

Then,

$$\sum_l n_l e^{iql\cos\theta}\, |+\rangle = \frac{1}{\sqrt{2}} \Lambda_q \left(|\Phi\rangle + e^{iq\cos\theta}\, |\Psi\rangle \right), \tag{2.60}$$

$$\sum_l n_l e^{iql\cos\theta}\, |-\rangle = \frac{1}{\sqrt{2}} \Lambda_q \left(|\Phi\rangle - e^{iq\cos\theta}\, |\Psi\rangle \right), \tag{2.61}$$

where

$$\Lambda_{q\cos\theta} = \frac{1 - e^{i2qN\cos\theta}}{1 - e^{i2q\cos\theta}}. \tag{2.62}$$

Rewriting $|\Phi\rangle$ and $|\Psi\rangle$ through $|+\rangle$ and $|-\rangle$, we get

$$\sum_l n_l e^{iql\cos\theta} |+\rangle = \Lambda_{q\cos\theta} e^{i\frac{q\cos\theta}{2}} \left(\cos\frac{q\cos\theta}{2} |+\rangle - i \sin\frac{q\cos\theta}{2} |-\rangle \right), \tag{2.63}$$

$$\sum_l n_l e^{iql\cos\theta} |-\rangle = \Lambda_{q\cos\theta} e^{i\frac{q\cos\theta}{2}} \left(\cos\frac{q\cos\theta}{2} |-\rangle - i \sin\frac{q\cos\theta}{2} |+\rangle \right), \tag{2.64}$$

which implies

$$\begin{aligned} G(H_S)|+\rangle &= \sum_{\mathbf{q},l'} e^{-iql'\cos\theta} |g_{\mathbf{q}}|^2 n_{l'} e^{i\frac{q\cos\theta}{2}} \Lambda_{q\cos\theta} \\ &\quad \times \left(\frac{\cos\frac{q\cos\theta}{2}}{\omega - E_+ - \omega_{\mathbf{q}}} |+\rangle - i \frac{\sin\frac{q\cos\theta}{2}}{\omega - E_- - \omega_{\mathbf{q}}} |-\rangle \right), \end{aligned} \tag{2.65}$$

$$\begin{aligned} G(H_S)|-\rangle &= \sum_{\mathbf{q},l'} e^{-iql'\cos\theta} |g_{\mathbf{q}}|^2 n_{l'} e^{i\frac{q\cos\theta}{2}} \Lambda_{q\cos\theta} \\ &\quad \times \left(\frac{\cos\frac{q\cos\theta}{2}}{\omega - E_- - \omega_{\mathbf{q}}} |-\rangle - i \frac{\sin\frac{q\cos\theta}{2}}{\omega - E_+ - \omega_{\mathbf{q}}} |+\rangle \right). \end{aligned} \tag{2.66}$$

By applying the second operator $n_{l'}$ one finds the following matrix elements:

$$G^{++} = \sum_{\mathbf{q}} |g_{\mathbf{q}}|^2 |\Lambda_{q\cos\theta}|^2 \left[\frac{\cos^2\frac{q\cos\theta}{2}}{\omega - E_+ - \omega_{\mathbf{q}}} + \frac{\sin^2\frac{q\cos\theta}{2}}{\omega - E_- - \omega_{\mathbf{q}}} \right], \tag{2.67}$$

$$G^{--} = \sum_{\mathbf{q}} |g_{\mathbf{q}}|^2 |\Lambda_{q\cos\theta}|^2 \left[\frac{\cos^2\frac{q\cos\theta}{2}}{\omega - E_- - \omega_{\mathbf{q}}} + \frac{\sin^2\frac{q\cos\theta}{2}}{\omega - E_+ - \omega_{\mathbf{q}}} \right], \tag{2.68}$$

$$G^{+-} = i \sum_{\mathbf{q}} |g_{\mathbf{q}}|^2 |\Lambda_{q\cos\theta}|^2 \cos\frac{q\cos\theta}{2} \sin\frac{q\cos\theta}{2} \left[\frac{1}{\omega - E_- - \omega_{\mathbf{q}}} - \frac{1}{\omega - E_+ - \omega_{\mathbf{q}}} \right], \tag{2.69}$$

$$G^{-+} = i \sum_{\mathbf{q}} |g_{\mathbf{q}}|^2 |\Lambda_{q\cos\theta}|^2 \cos\frac{q\cos\theta}{2} \sin\frac{q\cos\theta}{2} \left[\frac{1}{\omega - E_+ - \omega_{\mathbf{q}}} - \frac{1}{\omega - E_- - \omega_{\mathbf{q}}} \right]. \tag{2.70}$$

Introducing a set of generalized densities of states, defined as

$$\rho^{+-}(\epsilon) = -i \sum_{\mathbf{q}} |g_{\mathbf{q}}|^2 |\Lambda_{q\cos\theta}|^2 \cos\frac{q\cos\theta}{2} \sin\frac{q\cos\theta}{2} \delta(\epsilon - \omega_{\mathbf{q}}), \tag{2.71}$$

$$\rho^{-+}(\epsilon) = i\sum_{\mathbf{q}} |g_{\mathbf{q}}|^2 |\Lambda_{q\cos\theta}|^2 \cos\frac{q\cos\theta}{2}\sin\frac{q\cos\theta}{2}\delta(\epsilon-\omega_{\mathbf{q}}), \tag{2.72}$$

$$\rho_1(\epsilon) = \sum_{\mathbf{q}} |g_{\mathbf{q}}|^2 |\Lambda_{q\cos\theta}|^2 \cos^2\frac{q\cos\theta}{2}\delta(\epsilon-\omega_{\mathbf{q}}), \tag{2.73}$$

$$\rho_2(\epsilon) = \sum_{\mathbf{q}} |g_{\mathbf{q}}|^2 |\Lambda_{q\cos\theta}|^2 \sin^2\frac{q\cos\theta}{2}\delta(\epsilon-\omega_{\mathbf{q}}), \tag{2.74}$$

we obtain

$$G^{++} = \int d\epsilon \left[\frac{\rho_1(\epsilon)}{\omega - E_+ - \epsilon} + \frac{\rho_2(\epsilon)}{\omega - E_- - \epsilon}\right], \tag{2.75}$$

$$G^{+-} = -i\int d\epsilon \rho^{+-}(\epsilon)\left[\frac{1}{\omega - E_+ - \epsilon} - \frac{1}{\omega - E_- - \epsilon}\right], \tag{2.76}$$

$$G^{+-} = -i\int d\epsilon \rho^{+-}(\epsilon)\left[\frac{1}{\omega - E_+ - \epsilon} - \frac{1}{\omega - E_- - \epsilon}\right], \tag{2.77}$$

The real part of G gives a negligible contribution to the pole location if compared with E_- and E_+. Thus, assuming a density of state different from zero only for positive ϵ, as in Ref. [24], the only non vanishing contribution is $\gamma = -\operatorname{Im} G^{--}$:

$$\gamma = -\pi\rho_2(\Delta), \tag{2.78}$$

where $\Delta = E_- - E_+$ is the energy gap of the two level system and is positive (being $|+\rangle$ the ground state).

Then the solution for $\langle +|\Phi_S(t)\rangle$ and $\langle -|\Phi_S(t)\rangle$ is

$$\langle +|\Phi_S(t)\rangle = e^{iE_+ t}\langle +|\Phi_S(t=0)\rangle, \tag{2.79}$$

$$\langle -|\Phi_S(\omega)\rangle = e^{iE_- t-\gamma t}\langle -|\Phi_S(t=0)\rangle. \tag{2.80}$$

As expected, the ground state is not affected by decoherence, while the excited state relaxes. Damping is proportional to the density of states calculated at the energy gap. The density of states is however quite different from that of a single dot pair. Two competitive effects appear. The first one is represented by the presence of the form factor $\Lambda_{q\cos\theta}$ inside ρ_2, which, in the large N limit, increases the dephasing

rate by a factor proportional to N^2. The second, predominant, effect to be considered is the exponential reduction with N of the energy separation.

For instance, in the simple case of $|g_{\mathbf{q}}|^2 = 1/N$ and $\omega_{\mathbf{q}} = cq$ (longitudinal phonons)

$$\gamma(\Delta) \propto \int d\cos\theta d^d q \frac{\sin^2 qN}{\sin^2 q\cos\theta} \sin^2 \frac{q\cos\theta}{2} \delta\left(\Delta - c^2 q^2\right), \tag{2.81}$$

where d is the dimension of the bath and c is the speed of sound. If we compare this quantity with the system oscillation frequency we obtain

$$\frac{\gamma(\Delta)}{\Delta} \propto N^2 \Delta^{d/2-1}. \tag{2.82}$$

This result indicates that, for a phonon bath in three dimensions, the macroscopic limit involves a growth of the robustness with respect to decoherence.

2.4 A teleportation scheme

As an application of the two-level behaviour of the DQD array, we propose a possible original implementation of quantum teleportation in a solid state device. So far, experimental realizations of teleportation have been performed with optical systems [28, 29, 101], NMR techniques [31], and, recently, also working with atomic states [32, 33]. On the other hand, turning to solid state systems, experimental demonstration of teleportation in charge qubits is still lacking, and only few theoretical schemes are proposed [34, 35].

Let us consider a system composed by a DQD with just one excess electron with respect to the ground state. We indicate the basis elements of the two-level system with $|0_1,1_2\rangle$ and $|1_1,0_2\rangle$. If dots are coupled by tunneling, in the presence of a vector potential $\mathbf{A}$ directed from dot 1 to dot 2, the system is described by the following Hamiltonian:

$$H_{12} = -(we^{-i\varphi} c_1^\dagger c_2 + we^{i\varphi} c_2^\dagger c_1) + \epsilon(c_2^\dagger c_2 + c_1^\dagger c_1), \tag{2.83}$$

where $c_i(c_i^\dagger)$ represents the annihilation (creation) fermionic operator on the site i and $\varphi = eA/\hbar$. For the sake of simplicity and without loss of generality we shall assume $\epsilon = 0$. This Hamiltonian has eigenvalues $E^\pm = \pm w$ associated to the eigenvectors $|E^\pm\rangle = \frac{1}{\sqrt{2}}\left[e^{\mp i\varphi}\,|0_1,1_2\rangle \mp |1_1,0_2\rangle\right]$.

If, we suppose that the system is in a particular state at $t = 0$ (e.g. $|\phi(0)\rangle = |0_1,1_2\rangle$), the time evolution creates the coherent superposition $|\phi(t)\rangle = \cos wt\,|0_1,1_2\rangle + i\sin wte^{2i\varphi}\,|1_1,0_2\rangle$. Thus, by instantaneously switching off the tunneling at a suitable time $\bar{t}$, we can encode the generic qubit $|\phi(\bar{t})\rangle = |\chi\rangle = \alpha\,|0_1,1_2\rangle + \beta\,|1_1,0_2\rangle$.

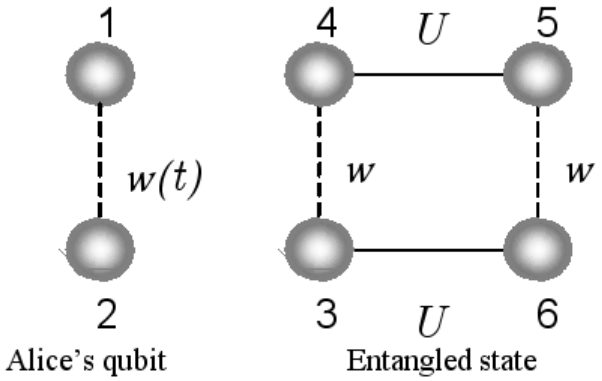

Figure 2.2. QD's 1 and 2 represent the unknown qubit to teleport. QD's $3 \to 6$ are in the entangled state $\frac{1}{\sqrt{2}}\left[|0_3,1_4,0_5,1_6\rangle + |1_3,0_4,1_5,0_6\rangle\right]$. Initially the system are separated. Solid lines represent tunneling, while dash lines represent Coulomb repulsion

The entangled support for teleportation is an array of four QDs labeled with subscripts 3,4,5,6 disposed as indicated in Fig. 2.2. The Hamiltonian

$$H_{3456} = -w\left(c_3^\dagger c_4 + c_5^\dagger c_6 + h.c.\right) + U\,(t)\,(n_3 n_6 + n_4 n_5) \tag{2.84}$$

takes into account both the tunneling interaction along vertical lines and the Coulomb repulsion along horizontal lines. Starting from $U(0) = 0$ the Hamiltonian is separable: $H_{3456} = H_{34} + H_{56}$. For convenience we shall assume that the system is prepared in its ground state:

$$|\psi(0)\rangle = \frac{1}{2}\left[|0_3,1_4\rangle + |1_3,0_4\rangle\right]\left[|0_5,1_6\rangle + |1_5,0_6\rangle\right]. \tag{2.85}$$

An adiabatic growth of Coulomb repulsion between dots localized on the same row will create a near maximally entangled state. Here adiabatic means slow with respect to the lower frequency of the system. Due to the adiabatic theorem [36], the overall system will remain in its instantaneous ground state. The asymptotic behaviour is a good approximation of a maximally entangled state in the limit of $w/U \to 0$:

$$|\psi(t \to \infty)\rangle \propto |0_3,1_4,0_5,1_6\rangle + |1_3,0_4,1_5,0_6\rangle - \frac{2w}{U}\left|\tilde{\psi}\right\rangle, \tag{2.86}$$

where $\left|\tilde{\psi}\right\rangle = |0_3,1_4,1_5,0_6\rangle + |1_3,0_4,0_5,1_6\rangle$ and $U = U(t \to \infty)$. Note that we are applying the two-level behaviour discussed in Sec. 2.2 to the simple case $N = 2$. Considering a finite time T of Coulomb switching, the adiabatic approximation works if the condition $T >> \varepsilon/\Delta_{min}^2$ is satisfied. Here ε is the maximum rate of the interaction variation and Δ_{min} the minimum energy gap between ground and first excited state [37]. In our case $T >> \hbar U^3/w^4$. Bearing in mind the limit of approximation we consider as starting point for the following manipulation the state of Eq. 2.86, where the correction due to $\left|\tilde{\psi}\right\rangle$ is neglected.

The creation of these entangled states permits one to implement a quantum teleportation protocol, as discussed in Sec. 1.2. The Bell measurement process can be performed (as suggested by G. Brassard and coworkers) in two sequential steps [38]: first, Bell states are rotated in the computational basis ($|0,0\rangle$,$|0,1\rangle$,$|1,0\rangle$,$|1,1\rangle$), then the projective measure is performed in this latter basis. Here we propose a slightly modified procedure wherein the Bell states involved are two instead of four; furthermore, we exploit temporal evolution to perform the first step of Brassard method, making simple the final one. Our protocol exploits an adiabatic switching on of Coulomb interaction between the qubit we want to teleport and the entangled state. Now we deal with a system composed by three DQDs (see Fig. 2.3), one of

them is used to encode the unknown qubit and the other two as entangled support. The Hamiltonian is

$$\begin{aligned} H_{123456} &= -w\left(a_3^\dagger a_4 + a_4^\dagger a_3\right) - w'(t)\left(a_5^\dagger a_6 + a_6^\dagger a_5\right) - w''(t)\left(a_1^\dagger a_2 + a_2^\dagger a_1\right) \\ &\quad + U(t)\left(n_3 n_6 + n_4 n_5\right) + U'(t)\left(n_1 n_4 + n_2 n_3\right), \end{aligned} \tag{2.87}$$

where $U'(0)$and $w''(0)$ are zero, while $w'(0) = w$.

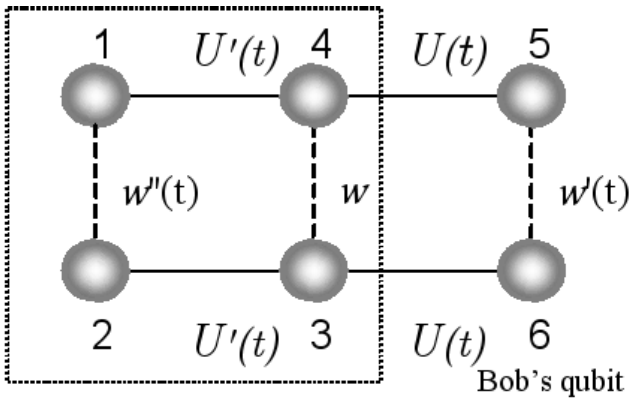

Figure 2.3. Final step of quantum teleportation: Bob's qubit is separated by others QD's which evolve providing a Bell measurement process

Making use of encoding technique and entanglement generation above described, the incoming overall state is

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(\alpha\,|0_1,1_2\rangle + \beta\,|1_1,0_2\rangle\right)\left(|0_3,1_4,0_5,1_6\rangle + |1_3,0_4,1_5,0_6\rangle\right). \tag{2.88}$$

If $U'(t)$ is adiabatically increased until it reaches the value U, the state evolves and reaches its new ground state

$$|\Psi(t)\rangle = \alpha\,|0_1,1_2,0_3,1_4,0_5,1_6\rangle + \beta\,|1_1,0_2,1_3,0_4,1_5,0_6\rangle. \tag{2.89}$$

So far we have described the coupling between unknown qubit and entangled state. Next step represents the analogous of Bell measurement. To prepare it

we need to detach Bob QDs (5 and 6) from the others and to start a temporal evolution of the state which involves dots from 1 to 4. By instantaneously turning on the tunneling $w''(t)$, and turning off the tunneling $w'(t)$ and the Coulomb interaction $U(t)$ (from now on the time will be measured starting form the switching instant), the system is forced to belong to a state in which dots from 1 to 4 evolve following the Hamiltonian of Eq. 2.84 (with appropriate indices), while Bob's dots are frozen. Neglecting terms of the order of w/U, $|0_1,1_2,0_3,1_4\rangle$ evolves into $(\cos\omega t\,|0_1,1_2,0_3,1_4\rangle + i\sin\omega t\,|1_1,0_2,1_3,0_4\rangle)$, while the state $|1_1,0_2,1_3,0_4\rangle$ evolves into $(\cos\omega t\,|1_1,0_2,1_3,0_4\rangle + i\sin\omega t\,|0_1,1_2,0_3,1_4\rangle)$, where $\omega = 4w^2/U$. Thus, the whole state becomes

$$|\Psi(t)\rangle = \frac{1}{\sqrt{2}}(|0_1,1_2,0_3,1_4\rangle \left|\chi^+(t)\right\rangle_{56} + i\,|1_1,0_2,1_3,0_4\rangle \left|\chi^-(t)\right\rangle_{56}), \tag{2.90}$$

having introduced $|\chi^{\pm}(t)\rangle_{56} = [(\cos\omega t)\,\alpha\,|0_5,1_6\rangle \pm i\,(\sin\omega t)\,\beta\,|1_5,0_6\rangle]$. Waiting a suitable time ($\omega t = \pi/4$) we obtain, associated with two orthogonal computational states on the four Alice's dots, $\alpha\,|0_5,1_6\rangle + i\beta\,|1_5,0_6\rangle$ and $\alpha\,|0_5,1_6\rangle - i\beta\,|1_5,0_6\rangle$. Measuring the charge on a dot (e.g. the number 1), Alice transmits the result as classical bit to Bob, that can choose the correct unitary rotation to perform in order to completely recover $|\chi\rangle$ on its site. Note that due to the nonlinearity of interactions involved in this model, there are no conceptual obstacles for which Bell measurements cannot reach a 100% of success probability [39, 40, 41].

2.5 Conclusions

Among all possible physical realizations of quantum information devices, quantum dots present several advantages, such as scalability and possibility of defining very small effective Hilbert spaces using coupled quantum dots, where Coulomb interactions between electrons can be exploited. On the other hand, short decoherence times are the main drawback. We have introduced a channel of coupled double

quantum dots which permits quantum teleportation protocols, and shown that the longer is the channel, the shorter is its decoherence time. This model could be very useful towards the realization of the hardware of a quantum computer, i.e. for information transfer in devices where photon use is discouraged by the fact the channel needs to be more short than optical wavelengths.

Chapter 3

High efficiency quantum information transfer in mesoscopic quantum channels

In this chapter, I point out my attention on a general problem of quantum information processing, i.e. the possibility of realizing a reliable quantum state transfer (QST) from one point in the space to another. In the preceding chapters we have spoken about quantum teleportation, which has exactly this scope. An alternative scenario provides the use of physical quantum channels, which could be very useful when considering very small quantum information processing devices such as condensed matter systems, where the length scale both of the component parts and of their separation will be generally below typical optical wavelengths, and photons cannot work as flying qubits. The chapter has the following organization. In Sec. 3.1 I describe how diffusion limits the possibility of using a quantum chain to transfer quantum information. In Sec. 3.2 I introduce a suggestion (quantum chain as a quantum bus) which is promising to overcome the problem of diffusion. The heart of the chapter is Sec. 3.3, where I introduce a Hamiltonian model and I study various

asymptotic limits which allow high efficiency QST [42]. In Sec. 3.4 the model is extended to the presence of disorder. It will be shown that weak disorder does not affect QST. Then, in Sec. 3.6 I will conclude the chapter.

3.1 Quantum state transfer in a spin chain

The use of local excitations in quantum chains, first suggested by S. Bose [43], is far from being optimal, due to quantum diffusion [44, 45]. Different physical realizations of quantum channels have been suggested: ferromagnetic spin chains [43, 46], Josephson arrays [47], nanoelectromechanical oscillators [49]. Diffusion appears in each of these models.

To understand what happens in these cases, we review the basic ideas present in the model proposed by Bose in a slightly different context.

We define a one-dimensional spin chain of N sites with XY interaction:

$$H = -w \sum_{i=0}^{N-1} \left[(1+\gamma)\, \sigma_i^+ \sigma_{i+1}^- + (1-\gamma)\, \sigma_i^- \sigma_{i+1}^+ \right], \tag{3.1}$$

where γ measures the anisotropy, and w is the tunneling amplitude.

When $\gamma = 0$, the Hamiltonian reduces to

$$H = -w \sum_{i=0}^{N-1} \left[\sigma_i^+ \sigma_{i+1}^- + \sigma_i^- \sigma_{i+1}^+ \right], \tag{3.2}$$

the operator of the total z component of the spin,

$$\sigma_{tot}^z = \sum_{i=1}^{N} \sigma_i^z, \tag{3.3}$$

commutes with H, and the total z component of spin is a constant of motion.

Let us start from the ground state $|G\rangle = |\uparrow_0, \uparrow_1, \ldots \uparrow_{N-1}\rangle$ and flip the first spin with a probability amplitude β. Then we have the state

$$|\Phi\rangle = \alpha\, |\uparrow_0, \uparrow_1, \ldots \uparrow_{N-1}\rangle + \beta\, |\downarrow_0, \uparrow_1, \ldots \uparrow_{N-1}\rangle, \tag{3.4}$$

where $|\alpha|^2 + |\beta|^2 = 1$. Alice would send this state to Bob, who is far apart in the chain. An alternative notation can help to study the time evolution of $|\Phi\rangle$. We indicate with $|n\rangle$ the state $|\uparrow_0, \uparrow_1, \ldots, \downarrow_n, \ldots \uparrow_{N-1}\rangle$. Relatively to the subspace with exactly one spin up and all other spins down (one-magnon subspace), the N eigenvectors of H are

$$|q\rangle = \frac{1}{\sqrt{N}} \sum_n e^{-iqn} |n\rangle , \tag{3.5}$$

whose eigenvalues are

$$\epsilon_q = -2w \cos q, \tag{3.6}$$

where $q = 2\pi k/N$ $(k = 0,1,\ldots,N-1)$.

The inversion of Eq. (3.5) allows one to write

$$|n\rangle = \frac{1}{\sqrt{N}} \sum_q e^{iqn} |q\rangle \tag{3.7}$$

Then

$$|\Phi(t)\rangle = \alpha |G\rangle + \sum_n \beta_n(t) |n\rangle , \tag{3.8}$$

where

$$\beta_n(t) = \frac{\beta}{\sqrt{N}} \sum_q e^{i\epsilon_q t} e^{-iqn}. \tag{3.9}$$

Let us suppose that Bob, who is placed in the r(th) site of the chain, wants to receive the state $|\Phi\rangle$. The state on his site, obtained by tracing out all sites but r, is a statistical mixture:

$$\rho_r(t) = \left(1 - |\beta_r(t)|^2\right) |\uparrow\rangle\langle\uparrow| + |\beta_r(t)|^2 |\downarrow\rangle\langle\downarrow| + \alpha\beta_r^*(t) |\uparrow\rangle\langle\downarrow| + \alpha^*\beta_r(t) |\downarrow\rangle\langle\uparrow| . \tag{3.10}$$

A quantitative measure of the distance of two states ρ_1 and ρ_2 is the fidelity:

$$F(\rho_1,\rho_2) = \left[Tr\sqrt{\rho_1^{1/2}\rho_2\rho_1^{1/2}}\right]^2 . \tag{3.11}$$

When one of two states is a pure one, the fidelity assumes the intuitive structure

$$F(\rho_1, |\Phi\rangle) = \langle\varphi| \rho_1 |\varphi\rangle . \tag{3.12}$$

In our case the average fidelity, obtained by integrating over all possible input states, is given as [43]

$$F_{Av}\left(\rho_r\left(t\right),\left|\Phi\right\rangle\right)=\frac{\left|\beta_r\left(t\right)\right|^2}{6}+\frac{\left|\beta_r\left(t\right)\right|\cos\gamma}{3}+\frac{1}{2}, \tag{3.13}$$

where $\gamma=\arg\left\{\beta_r\left(t\right)\right\}$. It will exist a time $\bar{t}$ which maximize F_{Av}, but, for any $N>3$, there is no way to reconstruct perfectly the input state. The spin chain acts as an "amplitude damping channel" [48].

Another way to observe the dissipative character of the channel is to study the evolution of entanglement as a function of time [46]. Now we start from the state

$$\left|\Phi_E\right\rangle=\frac{1}{\sqrt{2}}\left(\left|\uparrow_0,\downarrow_1,\uparrow_2,\ldots\uparrow_{N-1}\right\rangle+\left|\downarrow_0,\uparrow_1,\uparrow_2,\ldots\uparrow_{N-1}\right\rangle\right), \tag{3.14}$$

which exhibits the maximum degree of entanglement on the sites 0 and 1. The evolution of $\left|\Phi_E\right\rangle$ is calculated with the same rules used for $\left|\Phi\right\rangle$. We obtain

$$\left|\Phi_E\left(t\right)\right\rangle=\frac{1}{N\sqrt{2}}\sum_{q,n}e^{i\epsilon_q t}\left(1+e^{-iqn}\right)\left|n\right\rangle. \tag{3.15}$$

In the limit $N\rightarrow\infty$ we have

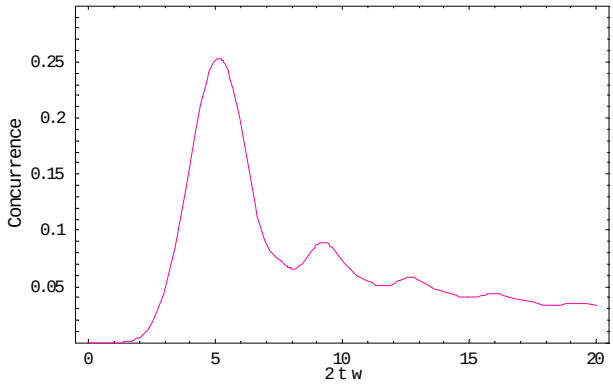

Figure 3.1. Concurrence as a function of time (see text for details). A two-site entangled state evolves in the chain. There exists an ideal time where Concurrence reaches a maximum. However, this peak value is far from 1

$$\left|\Phi_E\left(t\right)\right\rangle=\frac{1}{N\sqrt{2}}\sum_{q,n}\left[e^{-i\frac{\pi}{2}n}J_{-n}\left(2wt\right)+e^{i\frac{\pi}{2}\left(1-n\right)}J_{1-n}\left(2wt\right)\right], \tag{3.16}$$

where $J_m(x)$ is the Bessel function of order m and argument x. Entanglement evolution can be studied by means of concurrence (see Sec. 1.2). One can choose two sites in whatever place of the chain, calculate the reduced density matrix, and then obtain the degree of entanglement. Fig. 3.1 shows the concurrence for an infinite chain calculated on the sites 4 and 5, starting from $|\Phi_E\rangle$. Even in this case we observe a transmission by no means reliable.

The results obtained have a simple physical interpretation. The state we want to transfer is encoded through a local excitation, while the eigenstates of the chains are collective modes (the $|q\rangle$ states). Thus the initial state is a superposition of all the eigenstates with the same weight. During the evolution the wave packet spreads quite rapidly and the probability of reproducing the initial state in a different site is strongly limited by quantum diffusion.

Ideally, this drawback can be overcome by using parallel chains and conditional gates [50] or through the adoption of engineered couplings between the nodes of the network [51, 52]. However, these proposal are very hard to be realized.

3.2 Beating diffusion through the use of external couplings

QST among optical cavities, as proposed by Cirac et al. some years ago [53], is possible due to the fact that each atom inside the cavity interacts only with a nearly monochromatic photon of the radiation field, and that photon can be transmitted unchanged to a distant site, before interacting with another atom in a second cavity. As said, in mesoscopic devices, an interaction localized in the space involves all the modes of the support and the state reconstruction is affected by interference.

On the other hand, it has been shown [54, 55] that there are some configurations which reproduce a bahaviour similar to that found in optical systems. In particular,

Plenio and Semião [54] have proposed a model which allows high fidelity entanglement transfer on a chain of harmonic oscillators, or equivalently on a XY spin chain. The idea is as follows. A ring of interacting quantum systems forms the quantum data bus. At arbitrary positions on the ring two further quantum systems may be coupled weakly to the ring. The subsequent time evolution will allow the transfer of quantum information or the establishment of entanglement between the two distinguished quantum systems. The authors show by means of numerical results the efficiency of the system and justify the result by introducing a simplified model which reproduces very well the exact evolution. In practice, the two external quantum systems interact effectively only with one of eigenmodes of the quantum data bus (the center of mass mode). Then, interference is avoided and perfect QST is reached asymptotically.

3.3 Mesoscopic continuous and discrete channels for quantum information transfer

In Sec. 3.2 we have learned that faithful QST using solid state channels is possible. In the following we want to understand why and to derive all possible conditions which allow this behaviour.

To treat this problem in a more genera way, we consider the Fano-Anderson model [56, 57, 58, 59] extended to two impurities:

$$H = \sum_k \epsilon_k c_k^\dagger c_k + \Omega \left(c_A^\dagger c_A + c_B^\dagger c_B \right) - \frac{g}{\sqrt{N}} \sum_k \left[c_k^\dagger \left(c_A + e^{ikL} c_B \right) + H.c. \right]. \quad (3.17)$$

The scheme is depicted in Fig. 3.2. We have two quantum systems (A and B) with creation and annihilation operators $c_A^\dagger$, c_A, $c_B^\dagger$, and c_B, a chain with N modes, described by $c_k^\dagger$ (c_k) which creates (annihilates) an excitation in the mode k, and interaction with the modes and A and B which amounts to tunneling processes in

the case when both A and B are associated with a solid state tight binding model, or to a transfer of energy when A and B are atomic systems interacting with a radiation field. The coupling constant g measures the strength of the interaction and the phase factor $\exp(ikL)$ takes into account the distance L between A and B. In the case of a continuous spectrum, sums must be thought as integrals. Due to the quadratic nature of the Hamiltonian, the evolution equation of each operator is independent from the corresponding quantum statistics. Then, the model works for fermions as well as for bosons and spins. All the characteristics of the system are synthesized by the energy dispersion ϵ_k.

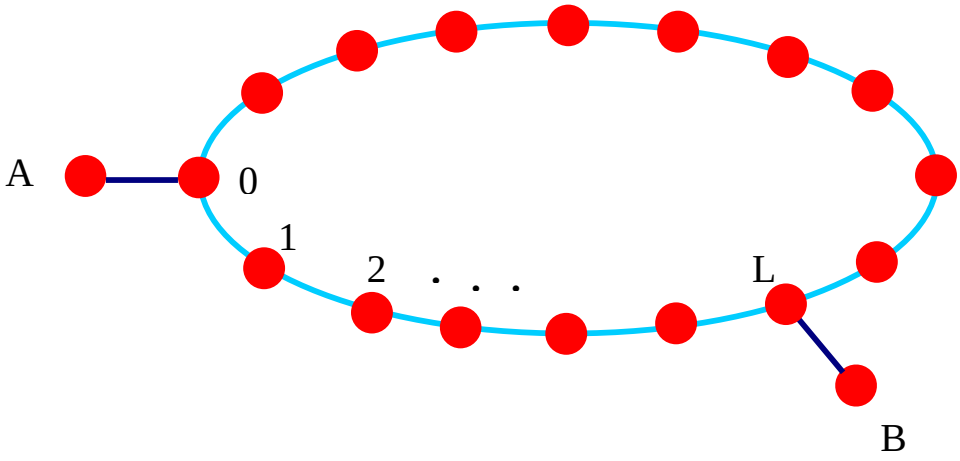

Figure 3.2. Schematic description of the quantum bus. We have two localized quantum systems (A and B) locally coupled with two different sites of a quantum chain with nearest neighbor interaction. L measures the distance between the sites connected respectively to A and B.

In the case of continuum of states, possible candidates as mesoscopic channels are conductors in the tight binding limit or one-dimensional wires with magnetic edge states [60], where there are experimental proofs of coherent hopping with quantum dots [61, 62]. As far as discrete sets of states are considered, the model is suitable to be implemented by arrays of quantum dots, or by nanoelectromechanical oscillators, or by a radiation confined in a finite-size cavity. An experimental evidence

of coherent oscillations in an all solid state realization of a Jaynes-Cummings-like scheme has been recently reported [63]. Keeping in mind this variety of suitable configurations, we will work assuming a tight binding model, and, consequently we will assume $\epsilon_k = -w\cos ka$, where k is defined in the first Brillouin zone limited by 0 and 2π ($k = 2\pi n/N$), being n any integer between 0 and $N-1$, and a is the lattice constant. Without loss of generality, we shall assume in the following $a = 1$ and $w = 1$. When necessary, we will specify whether the considerations that will be done are valid in general or only for the tight binding case.

3.3.1 The model

Let us start considering an initial state where an excitation is present in the impurity A and both the second impurity and the channel are in their respective vacuum states: $|\psi_{in}\rangle = c_A^\dagger |0\rangle$. The time evolution can be studied writing the Heisenberg equations

$$\frac{d}{dt}c_k = i\epsilon_k \left[c_k^\dagger c_k, c_k\right] - i\frac{g}{\sqrt{N}}\left[c_k^\dagger \left(c_A + c_B e^{-ikL}\right), c_k\right], \tag{3.18}$$

$$\frac{d}{dt}c_A = i\Omega \left[c_A^\dagger c_A, c_A\right] - i\frac{g}{\sqrt{N}}\sum_k \left[c_A^\dagger c_k, c_A\right], \tag{3.19}$$

$$\frac{d}{dt}c_B = i\Omega \left[c_B^\dagger c_B, c_B\right] - i\frac{g}{\sqrt{N}}\sum_k \left[c_B^\dagger c_k e^{ikL}, c_B\right], \tag{3.20}$$

which give

$$\frac{d}{dt}c_k = -i\epsilon_k c_k + i\frac{g}{\sqrt{N}}\left(c_A + c_B e^{-ikL}\right), \tag{3.21}$$

$$\frac{d}{dt}c_A = -i\Omega c_A + i\frac{g}{\sqrt{N}}\sum_k c_k, \tag{3.22}$$

$$\frac{d}{dt}c_B = -i\Omega c_B + i\frac{g}{\sqrt{N}}\sum_k c_k e^{ikL}, \tag{3.23}$$

and then introducing the Laplace transform, defined as

$$\tilde{c}^\dagger(\omega) = \int_0^\infty e^{i\omega t} c^\dagger(t)\, dt. \tag{3.24}$$

The system we obtain is

$$(\omega-\epsilon_k)\,\tilde{c}_k(\omega) = ic_k(t=0) - \frac{g}{\sqrt{N}}\left[\tilde{c}_A(\omega) + e^{-ikL}\tilde{c}_B(\omega)\right], \tag{3.25}$$

$$(\omega-\Omega)\,\tilde{c}_A(\omega) = ic_A(t=0) - \frac{g}{\sqrt{N}}\sum_k \tilde{c}_k(\omega), \tag{3.26}$$

$$(\omega-\Omega)\,\tilde{c}_B(\omega) = ic_B(t=0) - \frac{g}{\sqrt{N}}\sum_k \tilde{c}_k(\omega)\,e^{ikL}. \tag{3.27}$$

In the following we simplify the notation substituting $c_i(t=0)$ $(i=k,A,B)$ with c_i.

The formal solution leads to

$$\begin{aligned}\tilde{c}_A^\dagger(\omega) = {} & \frac{i}{D(\omega)}\Lambda_L(\omega)\left(c_B^\dagger - \frac{g}{\sqrt{N}}\sum_k \frac{e^{ikL}}{\omega-\epsilon_k}c_k^\dagger\right) \\ & + \frac{i}{D(\omega)}\left[\omega-\Omega-\Lambda_0(\omega)\right]\left(c_A^\dagger - \frac{g}{\sqrt{N}}\sum_k \frac{1}{\omega-\epsilon_k}c_k^\dagger\right),\end{aligned} \tag{3.28}$$

where we have introduced the kernel

$$\Lambda_d(\omega) = \frac{g^2}{N}\sum_k \frac{e^{ikd}}{\omega-\epsilon_k} \tag{3.29}$$

and

$$D(\omega) = \left[\omega-\Omega-\Lambda_0(\omega)\right]^2 - \Lambda_L^2(\omega). \tag{3.30}$$

Studying the zeroes of the spectral function $D(\omega)$, we extract all information about the system. Note that, from parity considerations, $\Lambda_d(\omega)$ depends on d only through its absolute value. The explicit derivation of $\Lambda_d(\omega)$ is given in appendix A. It will be shown that

$$\Lambda_d(\omega) = \frac{g^2}{(\omega^2-1)^{1/2}}\frac{K_d(\omega)+K_{N-d}(\omega)}{1-K_N(\omega)}, \tag{3.31}$$

where

$$K_r(\omega) = \left[-\omega + \left(\omega^2-1\right)^{1/2}\right]^r. \tag{3.32}$$

In order to evaluate its zeroes, the spectral function can be decomposed in two factors: $D(\omega) = D_+(\omega)D_-(\omega)$, where

$$D_\pm(\omega) = \omega - \Omega - \frac{g^2}{(\omega^2-1)^{1/2}}\frac{1+K_N(\omega)\pm\left[K_L(\omega)+K_{N-L}(\omega)\right]}{1-K_N(\omega)}. \tag{3.33}$$

The analytic structure of Eq. (3.28) consists in $2(N+1)$ real poles for every finite N, and, in the limit $N \to \infty$, only 4 real poles, related to the band extrema, remain, and poles inside the energy band are substituted by a cut. It can be useful to visualize the structure of poles considering the simple case of just one quantum system interacting with the chain, obtained considering $L = 0$. In Fig. 3.3 the emergence of all the poles is illustrated graphically.

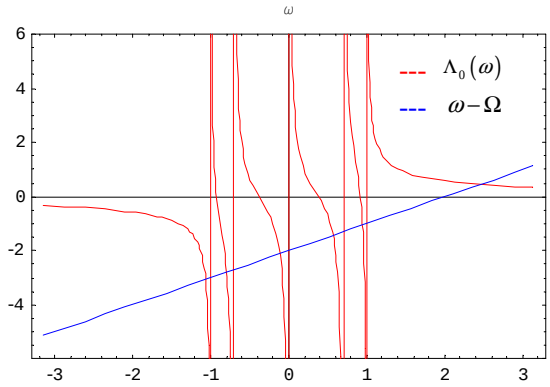

Figure 3.3. This plot illustrates the structure of the solutions of the equation $\omega - \Omega - \Lambda_0(\omega) = 0$. We have chosen $N = 8$, $\Omega = 2$, and $g = 1$. The poles are given by the intersections of the blue straight line representing $\omega - \Omega$ with the red function $\Lambda_0(\omega)$. Incrementing N, the poles within the energy band limited by $+1$ and -1 approach each others, and in the limit $N \to \infty$ a cut appears.

So far no approximations have been made, and the mathematical derivation illustrated in this paragraph is exact. In the following paragraphs, we will limit ourselves to study some asymptotic limits of this problem, looking for those configurations which warrant high efficiency quantum information transfer. In particular, we will consider weak coupling ($g \ll 1$) and strong coupling ($g \gg 1$), analyzing which are the conditions to fulfill in order to realize QST. We will show that coherent oscillations between A and B can be achieved using both continuous and discrete channels. In particular, discrete channels are suitable for our purposes when A and B are weakly coupled with the chain and Ω is resonant with one of its eigenvalues

ϵ_k. In this situation, only the resonant modes play a significant role and the effective Hamiltonian is that of a few-body problem. This result justifies the simplified model introduced in Ref. [54]. The same behaviour can be attained with continuous channels in the case of strong coupling, or, in the weak coupling limit, whenever Ω lies outside the energy band.

3.3.2 Strong coupling limit

In the strong coupling limit Eq.(3.33) is solved assuming that, at least in the case of tight binding we are considering, Ω does not play a really significant role, being compared with a term of the order of g^2/ω. Then we set $\Omega = 0$, and look for solutions of

$$\omega - \Lambda_0(\omega) \pm \Lambda_L(\omega) = 0. \tag{3.34}$$

We consider that ω will be approximatively of the order of g, develop $\Lambda_0(\omega)$ and $\Lambda_L(\omega)$ in powers of g^{-1}, and keep all terms up to g^{-2}. Another important remark to make is that, considering $g \gg 1$ and ω of the order of g, the solutions will be certainly far from the energy band. Then we can neglect the internal structure of the band itself, and assume $N \to \infty$. In this case

$$\Lambda_0(\omega) = \frac{g^2}{(\omega^2 - 1)^{1/2}}, \tag{3.35}$$

which leads to

$$\Lambda_0(\omega) \simeq \frac{g^2}{\omega}, \tag{3.36}$$

while

$$\Lambda_L(\omega) \simeq \frac{g^2 \left[-\frac{1}{2\omega}\right]^L}{\omega}. \tag{3.37}$$

Then the spectral function reduces to

$$D(\omega) \simeq \left(\omega - \frac{g^2}{\omega}\right)^2 - \frac{g^4 \left[-\frac{1}{2\omega}\right]^{2L}}{\omega^2} = \frac{\left(\omega^2 - g^2\right)^2 - g^4 \left[-\frac{1}{2\omega}\right]^{2L}}{\omega^2}. \tag{3.38}$$

Considering that the second term will be smaller than the first, it is correct to assume the zero order solution $\omega = \pm g$ and write

$$D(\omega) \simeq \frac{1}{\omega^2}\left[\left(\omega^2 - g^2\right)^2 - g^4\left[-\frac{1}{2g}\right]^{2L}\right]. \tag{3.39}$$

Therefore the zeroes of $D(\omega)$ are given by

$$\omega_{1,2,3,4} \simeq \pm g\sqrt{1 \pm \frac{1}{(2g)^L}}, \tag{3.40}$$

or

$$\begin{aligned}
\omega_1 &\simeq g\left(1 + \frac{1}{2(2g)^L}\right), \\
\omega_2 &\simeq g\left(1 - \frac{1}{2(2g)^L}\right), \\
\omega_3 &\simeq -g\left(1 + \frac{1}{2(2g)^L}\right), \\
\omega_4 &\simeq -g\left(1 - \frac{1}{2(2g)^L}\right).
\end{aligned} \tag{3.41}$$

The calculus of residues associated to the poles, to the end of calculating the time evolution of $c_A^\dagger$ (see Eq. (3.28)) is very lengthy and will not given here. The reduced density matrix of the systems A and B can be calculated by projecting $c_A^\dagger(t)\,|1,0;0\rangle$ onto the vacuum of the chain

$$\langle 0|1,0;0\rangle_t = \frac{1}{4}\left[\left(e^{i\omega_1 t} + e^{i\omega_2 t} + e^{i\omega_3 t} + e^{i\omega_4 t}\right)|1,0\rangle + \left(e^{i\omega_1 t} - e^{i\omega_2 t} + e^{i\omega_3 t} - e^{i\omega_4 t}\right)|0,1\rangle\right] \tag{3.42}$$

Since $\omega_1 = -\omega_4$ and $\omega_2 = -\omega_3$

$$\begin{aligned}
\langle 0|1,0;0\rangle_t &= \frac{1}{2}\left[\left(\cos\omega_1 t + \cos\omega_2 t\right)|1,0\rangle + i\left(\sin\omega_1 t - \sin\omega_2 t\right)|0,1\rangle\right] \\
&= \cos gt\left(\cos\frac{gt}{2(2g)^L}|1,0\rangle + i\sin\frac{gt}{2(2g)^L}|0,1\rangle\right).
\end{aligned} \tag{3.43}$$

The reduced density matrix is then

$$\bar{\rho} = \cos^2 gt\cos^2\frac{gt}{2(2g)^L}|1,0\rangle\langle 1,0| + \cos^2 gt\sin^2\frac{gt}{2(2g)^L}|0,1\rangle\langle 0,1|$$

$$+i\cos^2 gt\cos\frac{gt}{2\,(2g)^L}\sin\frac{gt}{2\,(2g)^L}\left(|0,1\rangle\langle 1,0| - |1,0\rangle\langle 0,1|\right)$$
$$+\sin^2 gt\,|0,0\rangle\langle 0,0|\,, \tag{3.44}$$

where the last term has been obtained considering that $\mathrm{Tr}\{\bar{\rho}\} = 1$.

In this case, we have high frequency oscillations between A and B and the channel modulated by a low frequency signal which enables QST. Note that the spectral weight is not entirely concentrated on the impurities, because at intermediate times the probability of finding the excitation in the channel is finite. It is clear that the channel is perfect only if corrections of the order of g^{-2} are neglected. In Fig. 3.4 the probabilities of finding the excitation on A and B are depicted as functions of time. The lower panel shows the high frequency oscillation. The discussion of this limit fails when infinitely extended discrete spectra are considered, as, for instance, in the case of finite-length cavities, because we need to consider only a polar singularity well far from all other poles.

3.3.3 Weak coupling limit

Now we are interested to the case $g \ll 1$. The zeroes of Eq. (3.33) can be calculated by iterating the zero order solution $\omega = \omega_0$ obtained in the limit $g \to 0$. Two very different discussions arise considering the impurities' energy Ω inside the band ($|\Omega| < 1$) or outside the band ($|\Omega| > 1$).

Let us start from $|\Omega| < 1$. In this case it can be useful to introduce an auxiliary complex variable γ defined by $\omega = -\cos\gamma$, with the constraint that $0 \leq Re\{\gamma\} \leq \pi$. So

$$D_{\pm}(\gamma) = \cos\gamma - \cos\Gamma + g^2\frac{1}{\sin\gamma\sin\gamma N/2}\left[\cos\gamma N/2 \pm \cos\gamma(L - N/2)\right], \tag{3.45}$$

having defined $\Omega = -\cos\Gamma$. Now we assume that Ω coincides with one of the unperturbed poles (what means the word "coincides" will appear clear at the end

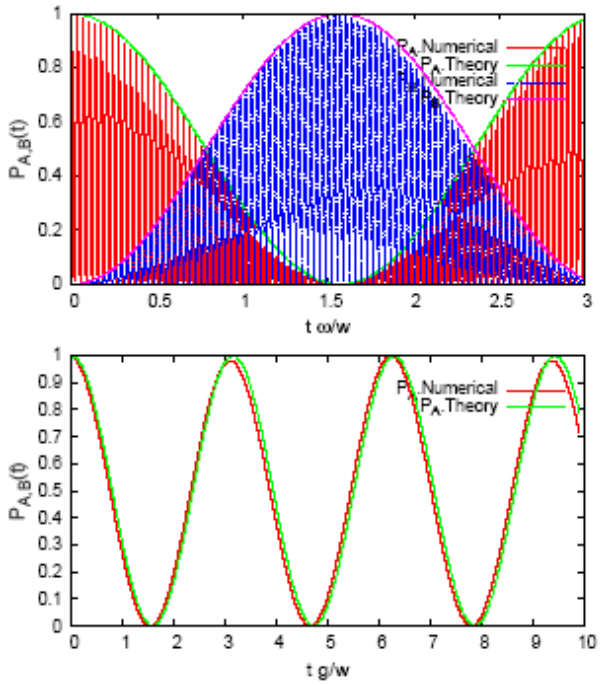

Figure 3.4. Strong coupling limit: $g = 10$, $\Omega = 0$, $L = 4$, $N = 50$. In the upper panel the low frequency oscillations are compared with the theory, the time unit is $\omega = g/[2(2g)^L]$. In the lower panel the same comparison is reported for the higher frequencies.

of this discussion). Since in the weak coupling limit the original energy levels are slightly modified, it is reasonable to assume that the resonant ones give the main contribution to the evolution and an expansion around them can be done. We write $\gamma = \Gamma + \delta$, with δ expected to vanish in the limit of $g = 0$. In the small δ limit

$$\delta \simeq \frac{g^2}{\sin^2 \Gamma} \left[\cot \frac{\delta N}{2} \left(1 \pm \cos \Gamma L\right) \pm \sin \Gamma L \right]. \tag{3.46}$$

Two different regimes appear for $|\delta| N \gg 1$ or $|\delta| N \ll 1$. In the first case the system is well approximated by its continuum limit, obtained replacing $\cot \delta N/2$ with $-i\ sign\{Im\{\delta\}\}$. It is easy to show that Eq. (3.46) does not provide polar solutions, but only singularities deriving from the cut. Under these conditions, the excitation diffuses in the channel and the QST efficiency is lost.

On the other hand, when $\delta N \ll 1$ the cotangent in Eq.(3.46) is expanded into $2/(\delta N)$ and $\sin \Gamma L$ is negligible. The solutions one obtains are then $\delta_1^{\pm} = \pm g \sqrt{2\left(1 - \cos \Gamma L\right)/N \sin^2 \Gamma}$ and $\delta_2^{\pm} = \pm g \sqrt{2\left(1 + \cos \Gamma L\right)/N \sin^2 \Gamma}$. The time evolution of $c_A^{\dagger}$ looks very simple when $\Omega = 0$ and L is even: in such a case

$$c_A^{\dagger}(t) = \cos^2 \frac{gt}{\sqrt{N}} c_A^{\dagger} + (-1)^{1+L/2} \sin^2 \frac{gt}{\sqrt{N}} c_B^{\dagger} + \frac{i}{2} \sin \frac{2gt}{\sqrt{N}} \left(c_{\bar{k}}^{\dagger} + c_{-\bar{k}}^{\dagger}\right), \tag{3.47}$$

where $\pm\bar{k}$ are the modes in resonance with $\Omega = 0$. This formula shows that, despite the non vanishing probability of finding the excitation in the channel, perfect QST is achieved. As in the strong coupling limit, we stress that we are performing an expansion, neglecting terms in g^2. In Fig. 3.5 we report the time evolution of P_A and P_B, which represent the occupation probabilities of A and B. On the other hand, assuming L odd, the second impurity is never populated:

$$c_A^{\dagger}(t) = \cos gt \sqrt{\frac{2}{N}} c_A^{\dagger} + \frac{i}{\sqrt{2}} \sin gt \sqrt{\frac{2}{N}} \left(c_{\bar{k}}^{\dagger} + c_{-\bar{k}}^{\dagger}\right). \tag{3.48}$$

The result of Eq. (3.47) is somewhat similar to that obtained in Ref. [54], showing an efficiency of transfer independent (limiting ourselves to even values of L) from

the distance. The condition $\delta N \ll 1$ (or $g\sqrt{N} \ll 1$) can be interpreted as follows: the interaction splits the resonant pole in two levels with an energy separation of the order of $g/\sqrt{N}$, while the energy spacing between different modes is about $1/N$. If none of the other modes falls inside this energy interval, then the excitation interacts effectively only with the resonant modes and the coherent behaviour appears. Vice versa, when $g/\sqrt{N} \gg 1/N$, the resonance is no more separated from the other modes and a continuum-like behaviour is expected.

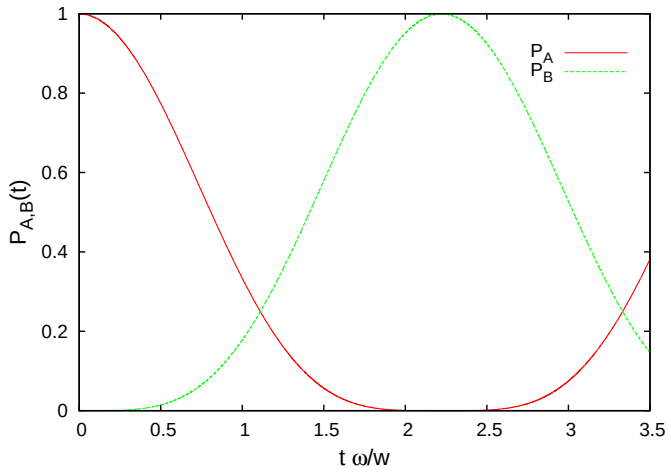

Figure 3.5. (Color online) Numerical simulation of the evolution of $P_A(t)$ and $P_B(t)$ in weak coupling and resonance with the following parameters: $g = 0.01$, $\Omega = 0$, $N = 16$, and $L = 8$. The time is normalized with respect to $\omega = g\sqrt{2}/\sqrt{N}$. The theoretical behaviour, calculated in the text, coincides perfectly with the numerical one.

Although the derivation performed above has the advantage of showing the physical meaning of resonance condition, the result can be obtained working directly with the expression

$$D(\omega) = \left[\omega - \Omega - \frac{g^2}{N}\sum_k \frac{1}{\omega - \epsilon_k}\right]^2 - \left[\sum_k \frac{e^{ikL}}{\omega - \epsilon_k}\right]^2. \tag{3.49}$$

Indeed we can keep in each sum only the modes $\bar{k}$ and $-\bar{k}$, corresponding to the resonance condition $\Omega = \epsilon_{\bar{k}}$. Further, we assume $\Omega = 0$, and then $\bar{k} = \pi/2$. The

kernels become

$$\Lambda(\omega) \simeq \frac{2g^2}{N\omega}, \tag{3.50}$$

$$\Lambda_L(\omega) \simeq \frac{2g^2\cos\frac{\pi L}{2}}{N\omega}, \tag{3.51}$$

and the spectral function is

$$D(\omega) = \left[\omega - \frac{2g^2\left(1+\cos\frac{\pi L}{2}\right)}{N\omega}\right]\left[\omega - \frac{2g^2\left(1-\cos\frac{\pi L}{2}\right)}{N\omega}\right], \tag{3.52}$$

or

$$D(\omega) = \left[\omega - \frac{4g^2\cos^2\frac{\pi L}{4}}{N\omega}\right]\left[\omega - \frac{4g^2\sin^2\frac{\pi L}{4}}{N\omega}\right]. \tag{3.53}$$

Limiting ourselves to even values for L,

$$D(\omega) = \left(\omega^2 - \frac{4g^2}{N}\right)\omega, \tag{3.54}$$

and there are three poles in $\omega_1 = 0$, $\omega_2 = 2g/\sqrt{N}$, $\omega_3 = -2g/\sqrt{N}$. At this stage the Laplace transform of the coefficients in Eq. (3.28) can be calculated easily, and the result found is the same as in Eq. (3.47).

The other interesting physical situation to study corresponds to Ω outside the band ($|\Omega| > 1$). In this case the zero order solution is $\omega_0 = \Omega$ and, by iteration,

$$\omega_{1,2} = \Omega + \Lambda_0(\Omega) \pm \Lambda_L(\Omega). \tag{3.55}$$

All roots are real and oscillations are expected. Residues associated to poles ω_1 and ω_2 in Eq.(3.28) are obtained neglecting terms in powers of order g^2. In such limit we find that all the spectral weight is concentrated on the impurities' modes. Then, we obtain a coherent oscillation between the two impurities:

$$c_A^\dagger(t) = e^{-\frac{i\omega_+ t}{2}}\left(\cos\frac{\omega_- t}{2}c_A^\dagger - i\sin\frac{\omega_- t}{2}c_B^\dagger\right), \tag{3.56}$$

where $\omega_+ = 2[\Omega + \Lambda_0(\Omega)]$ and $\omega_- = 2\Lambda_L(\Omega)$. In the limit of infinite number of modes, which is a good approximation also for N not so large, $\omega_+ = 2\Omega +$

$2g^2/\left(\Omega^2-1\right)^{1/2}$ and

$$\omega_- = 2g^2\left[\Omega-\sqrt{\Omega^2-1}\right]^L/\sqrt{\Omega^2-1}. \tag{3.57}$$

These solutions illustrate that the open system $A+B$ experiences a Rabi oscillation, and actually behaves as a closed one. Then, the system is suitable for QST or to create entanglement. In the case discussed above the dependence on the size-system is not crucial and the continuous limit is achieved even for not very large values of N. In Fig. 3.6 we report the probabilities of the excitation to be localized either on the first impurity or on the second one. It is worth outlining that this results holds only for systems with band structure in the energy spectrum.

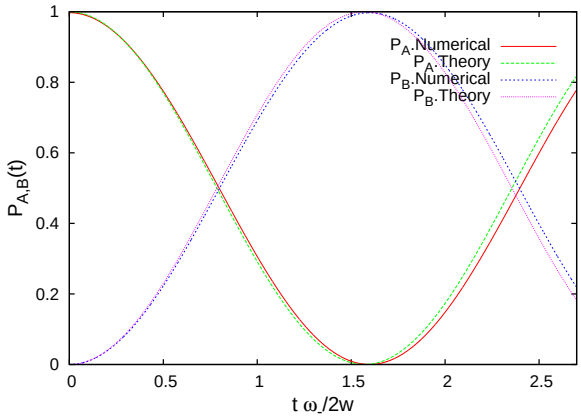

Figure 3.6. (Color online) Time evolution of the occupation probabilities of A and B (P_A and P_B) in weak coupling and off-resonance. The coupling strength is $g = 0.05$, the impurities' energy is $\Omega = 1.5$, the number of the channel's elements is $N = 30$, and the distance between A and B is $L = 6$. Here are reported both the numerical (exact) and theoretical curves.

3.4 Effects of disorder and Anderson localization

So far we have considered the case of a perfect chain and we have shown which are the conditions that permit high efficiency QST. In this section we devote our

attention to the possibility that the channel can be affected by some kind of disorder. We connect the effects of disorder with the Anderson localization [58]. Our aim is to show that in the limit of weak disorder high efficiency in QST processes is preserved.

3.4.1 Anderson Localization

Although Anderson localization is a largely studied physical phenomenon, having discussed so far systems whose size can be either finite or infinite, we find useful to derive the conditions which can cause localization considering explicitly the dependence on the size system. For this end, we derive localization in a tight binding disordered model using the resolvent formalism. We will use second order perturbation theory. Disorder is modelled considering on-site energies which are random variables distributed around zero with mean square deviation equal to σ: the Hamiltonian is

$$H = \sum_k \epsilon_k c_k^\dagger c_k + \sum_l \sigma_l c_l^\dagger c_l. \tag{3.58}$$

where k is a label for the modes, while l indicates the sites of the chain. In terms of modes we have

$$H_0 = \sum_k \epsilon_k c_k^\dagger c_k + \frac{1}{\sqrt{N}} \sum_{k,k'} \sigma_{k-k'} c_k^\dagger c_{k'}. \tag{3.59}$$

The Heisenberg equation in the Laplace space for c_k is

$$(\omega - \epsilon_k)\, c_k(\omega) = i c_k + \frac{1}{\sqrt{N}} \sum_{k'} \sigma_{k-k'} c_{k'}(\omega). \tag{3.60}$$

Perturbation theory can be performed by iterating the zero order solution in the right hand side of Eq. (3.60),

$$(\omega - \epsilon_k)\, c_k(\omega) = i c_k + \frac{1}{\sqrt{N}} \sum_{k'} \sigma_{k-k'} \left[\frac{i c_{k'}(t=0)}{\omega - \epsilon_{k'}} + \frac{1}{\sqrt{N}} \sum_{k'} \frac{\sigma_{k'-k''}}{\omega - \epsilon_{k'}} c_{k''}(\omega) \right], \tag{3.61}$$

and then keeping just self-energy corrections:

$$c_k(\omega) = \frac{i}{\omega - \epsilon_k - \frac{1}{N} \sum_{k'} \frac{\sigma_{k-k'} \sigma_{k'-k}}{\omega - \epsilon_{k'}}} c_k, \tag{3.62}$$

that is

$$c_k(\omega) = \frac{i}{\omega - \epsilon_k - \frac{\sigma^2}{N}\sum_{k'}\frac{1}{\omega-\epsilon_{k'}}} c_k. \tag{3.63}$$

Thus, the effect of disorder is to shift the eigenenergies of the chain by an amount dependent on the frequency under observation.

Let us introduce the Green function

$$G^+_{0L}(\omega) = \lim_{\eta\to 0^+} \langle L| \frac{1}{\omega + i\eta - H} |0\rangle, \tag{3.64}$$

representing the propagator from the site 0 to the site L. In terms of modes

$$G^+_{0L}(\omega) = \lim_{\eta\to 0^+} \sum_k \frac{e^{ikL}}{\omega + i\eta - \epsilon_k}. \tag{3.65}$$

We see that $G^+_{0L}(\omega)$ coincides with the kernel Λ_L introduced in Eq. (3.29), aside from the explicit dependence on the coupling parameter g.

The localization length λ can be defined in the following way [64]:

$$\frac{1}{\lambda} = -\lim_{L\to\infty} \frac{\log\left|G^+_{0L}(\omega)\right|^2}{2L}. \tag{3.66}$$

Intuitively, localization is possible only if $G^+_{0L}(\omega) \propto \exp(-\alpha L)$. Let us stress that localization appears in the thermodynamical limit: in that case we know that

$$G^+_{0L}(\omega) = \frac{\left[-\omega + (\omega^2-1)^{1/2}\right]^L}{(\omega^2-1)^{1/2}}, \tag{3.67}$$

or, using the mapping $\omega = -\cos\gamma$,

$$G^+_{0L}(\omega) = \frac{e^{i\gamma L}}{i\sin\gamma}. \tag{3.68}$$

In absence of disorder, considering those frequencies which fall inside the energy band, γ is a real number and there is no localization. This result is somewhat obvious, considering that the eigenfunctions of the system are Bloch waves.

The presence of disorder changes the terms of the problem. In fact, we have to change ω in $\bar{\omega} = \omega - \sigma^2/\left(\omega^2 - 1\right)^{1/2}$. It can be useful to map this new quantity in $-\cos z$. Then

$$\cos z = \cos\gamma - i\frac{\sigma^2}{\sin\gamma}. \tag{3.69}$$

In the case of weak disorder we can write $z = z_1 + z_2$, and identify $z_1 = \gamma$ and $z_2 = i\sigma^2/\sin^2\gamma$. Therefore

$$\frac{1}{\lambda} = \frac{\sigma^2}{\omega^2 - 1}. \tag{3.70}$$

This result, aside from numerical factors deriving from contributes which are ignored at the second order in the perturbation theory [64], is in agreement with the existing literature.

3.4.2 Anderson localization and quantum communication

Now we extend the description of Anderson localization to the Hamiltonian introduced in Eq. (3.17) describing our quantum bus. It is simple to show that, using second order perturbation theory, and neglecting also sums with argument $\sigma_{k-k'}$, considering that σ has mean value equal to 0, $c_A^\dagger(\omega)$ has the same expression obtained in Eq. (3.28), apart from the energy shift $\omega \to \bar{\omega}$. Hence, the propagator is

$$G_{0L}^{+}(\bar{\omega}) = \frac{\Lambda_L(\bar{\omega})}{\left[\bar{\omega} - \Omega - \Lambda_0(\bar{\omega})\right]^2 - \Lambda_L^2(\bar{\omega})}. \tag{3.71}$$

Actually, for the localization length, it can be shown that the sole significative contribution comes from $\Lambda_L(\bar{\omega})$ and is the same as in absence of impurities, apart from the frequency shift. Therefore,

$$G_{0L}^{+}(z) = \frac{e^{izL}}{i\sin z}, \tag{3.72}$$

where z has been defined in Eq. (3.69). To obtain a finite value for λ we need to have a non vanishing imaginary part in z.

Then, we analyze the cases described in Sec. 3.3. We start assuming Ω outside the energy band ($|\Omega| > 1$). For these energies the time evolution of the quantum bus is dominated by the new frequency $\bar{\Omega} = \Omega - \sigma^2/\sqrt{\Omega^2 - 1}$. Being $\bar{\Omega}$ real, disorder simply renormalizes the isolated eigenvalue, slightly modifying the oscillation frequency in Eq. (3.56). Actually, it is worth noting that, for Ω only slightly larger than 1, it is possible that $\bar{\Omega} < 1$, and the pole falls inside the band, changing the oscillation regime. In some sense, σ is related to the minimum distance between the energy band edge and Ω to consider Ω itself as an isolated eigenvalue.

Next we consider the case $|\Omega| < 1$ in the thermodynamic limit ($N \to \infty$). For this physical situation the result is that of Eq. (3.70). Now localization appears, but we have already learned that this limit does not allows efficient QST (see considerations below Eq. (3.46)). Disorder sums its effect with that of diffusion. On the other hand, in finite N limit, $\left(g\sqrt{N} \ll 1\right)$, the shift $\epsilon_k \to \epsilon_k - (\sigma^2/N) \sum_{k'} (\omega - \epsilon_{k'})^{-1}$ is always a real quantity, and localization does not appear. Then we can conclude that our system is robust with respect to weak disorder, considering those configurations which permit reliable QST.

3.5 Thermal effects on the QST protocol

The argument of this sections applies to the case where the chain is an array of quantum dots, and the impurity we are considering is one electron charge hopping from one site to another. For the sake of clarity, being the scope of this section the calculus of a decay rate, we write explicitly all physical parameters, such as $\hbar$, the tunneling amplitude w, and the lattice constant a.

We consider electron-phonon interaction extended to all the chain sites and study how thermal effects influence the spectrum of the tight binding model, described by

the Hamiltonian

$$H_S = \sum_k \epsilon_k c_k^\dagger c_k. \tag{3.73}$$

The bath is described in terms of harmonic oscillators:

$$H_B = \sum_{\mathbf{q}} \hbar\omega_{\mathbf{q}} a_{\mathbf{q}}^\dagger a_{\mathbf{q}}, \tag{3.74}$$

where $a_{\mathbf{q}}^\dagger$ ($a_{\mathbf{q}}$) creates (destroys) a phonon on the mode $\mathbf{q}$. As far as electron-phonon interaction is considered, a key role is represented by the coupling parameter which encloses the nature of the interaction.

Actually, we should consider the effect of phonons on the total Hamiltonian introduced in Eq. (3.17), describing our quantum bus, but, as in the case of disorder, in the limit of weak coupling, the effect of the interaction is to renormalize the eignevalues ϵ_k. Here, we expect that a macroscopic bath induces finite lifetimes for the system 's eignemodes, and we must compare these decay rates with the frequencies which allow QST in the bus.

First of all, according with the order of magnitude of tunneling in dot arrays, which is up to a few milli-electron-volts [65], only acoustic phonons near the Brillouin zone center $\mathbf{q} \sim 0$ are involved in the process. Electrons couple to longitudinal acoustic phonons through a deformation potential, and to longitudinal and transverse acoustic phonons through piezoelectric interaction [66]. However, piezoelectric interaction is essentially due to the lack of symmetry in the crystal, thus for materials such as Si, which has crystal inversion symmetry, it is not present. Then, we will limit ourselves to this context, already proposed as a solid state quantum information support [67], and consider only the deformation potential, which is

$$H_{ep} = D \sum_{\mathbf{q}} \left(\frac{\hbar}{2\rho_m V \omega_{\mathbf{q}}} \right)^{1/2} |\mathbf{q}| \rho(\mathbf{q}) (a_{\mathbf{q}} + a_{-\mathbf{q}}^\dagger), \tag{3.75}$$

where D is the deformation constant, ρ_m is the mass density of the material, V is the volume of the sample, $\omega_{\mathbf{q}} \simeq c\,|\mathbf{q}|$, c is the speed of sound, and $\rho(\mathbf{q})$ is the electron

density operator:

$$\rho(\mathbf{q}) = \rho(q_x) = \frac{1}{N}\sum_{k,k'} c_k^\dagger c_{k'} \sum_l e^{-iq_x l} e^{i(k-k')l}, \tag{3.76}$$

where the sum runs over all the chain sites, and q_x is the component of the wave vector along the chain direction.

Due the periodic boundary conditions of the chain, we consider q_x as a discrete quantity. This implies $\rho(q_x) = \sum_k c_{k+q_x}^\dagger c_k$.

Next, we study the time evolution of the mode $|k\rangle$, with the bath in equilibrium at a given temperature corresponding to $\beta = 1/KT$. The density matrix is

$$\rho\left(0\right) = \left|k\right\rangle \left\langle k\right| \otimes e^{-\beta H_B} = \sum_{\{n\}} e^{-\beta E\{n\}} c_k^\dagger \left|0,\{n\}\right\rangle \left\langle 0,\{n\}\right| c_k, \tag{3.77}$$

where $\{n\}$ is a label which runs over all possible phonon configurations. The time evolution will be given by

$$\rho\left(t\right) = \sum_{\{n\}} e^{-\beta E\{n\}} e^{-iHt/\hbar} c_k^\dagger \left|0,\{n\}\right\rangle \left\langle 0,\{n\}\right| c_k e^{iHt/\hbar}, \tag{3.78}$$

and the reduced density matrix, describing the chain alone is

$$\bar{\rho}\left(t\right) = \sum_{\{n\},\{m\}} e^{-\beta E\{n\}} \left\langle \{m\}\right| e^{-iHt/\hbar} c_k^\dagger \left|0,\{n\}\right\rangle \left\langle 0,\{n\}\right| c_k e^{iHt/\hbar} \left|\{m\}\right\rangle. \tag{3.79}$$

This quantity can be calculated in a second-order perturbation theory in $\lambda_{\mathbf{q}} = D\left(\hbar/2\rho_m V\omega_{\mathbf{q}}\right)^{1/2}|\mathbf{q}|$. Working in the ω-space, we have to consider

$$\begin{aligned}
\bar{\rho}\left(\omega,\omega'\right) &= c_k^\dagger \left|0\right\rangle \left\langle 0\right| c_k \frac{1}{\left(\omega-\epsilon_k\right)\left(\omega'-\epsilon_k\right)} + c_k^\dagger \left|0\right\rangle \left\langle 0\right| c_k \frac{1}{\mathcal{Z}} \sum_{\{n\},\{m\}} e^{-\beta E\{n\}} \\
&\times [\left\langle \{m\}\right| \frac{1}{\omega - H_0} H_{SB} \frac{1}{\omega - H_0} H_{SB} \frac{1}{\omega - H_0} c_k^\dagger \left|0,\{n\}\right\rangle \left\langle 0,\{n\}\right| c_k \frac{1}{\omega' - H_0} \left|\{m\}\right\rangle \\
&+ \left\langle \{m\}\right| \frac{1}{\omega - H_0} c_k^\dagger \left|0,\{n\}\right\rangle \left\langle 0,\{n\}\right| c_k \frac{1}{\omega' - H_0} H_{SB} \frac{1}{\omega' - H_0} H_{SB} \frac{1}{\omega' - H_0} \left|\{m\}\right\rangle],
\end{aligned} \tag{3.80}$$

where $c_k^\dagger \left|0\right\rangle \left\langle 0\right| c_k$ is the zero order contribution, $\mathcal{Z}$ is the partition function, and $H_0 = H_S + H_B$. It can be shown that other second-order terms do not contribute to

self-energy corrections, and will be neglected. After some algebraic manipulations we obtain

$$\begin{aligned}\bar{\rho}\left(\omega,\omega'\right) &= c_k^{\dagger}\left|0\right\rangle\left\langle 0\right|c_k\{\frac{1}{\left(\omega-\epsilon_k\right)\left(\omega'-\epsilon_k\right)}+\frac{1}{\mathcal{Z}}\sum_{\mathbf{q},n_{\mathbf{q}}}\lambda_{\mathbf{q}}^2 \\ &\times[\frac{e^{-\beta n_{\mathbf{q}}\hbar\omega_{\mathbf{q}}}}{\left(\omega-\epsilon_k\right)^2\left(\omega'-\epsilon_k\right)}\left(\frac{n_{\mathbf{q}}+1}{\omega-\hbar\omega_{\mathbf{q}}-\epsilon_{k-q_x}}+\frac{n_{\mathbf{q}}}{\omega+\hbar\omega_{\mathbf{q}}-\epsilon_{k+q_x}}\right) \\ &+\frac{e^{-\beta n_{\mathbf{q}}\hbar\omega_{\mathbf{q}}}}{\left(\omega-\epsilon_k\right)\left(\omega'-\epsilon_k\right)^2}\left(\frac{n_{\mathbf{q}}+1}{\omega'-\hbar\omega_{\mathbf{q}}-\epsilon_{k-q_x}}+\frac{n_{\mathbf{q}}}{\omega'+\hbar\omega_{\mathbf{q}}-\epsilon_{k+q_x}}\right)]\},\end{aligned} \tag{3.81}$$

or, performing the sum over $n_{\mathbf{q}}$,

$$\begin{aligned}&\bar{\rho}\left(\omega,\omega'\right)=c_k^{\dagger}\left|0\right\rangle\left\langle 0\right|c_k \\ &\times\left\{\frac{1}{\left(\omega-\epsilon_k\right)\left(\omega'-\epsilon_k\right)}+\left[\frac{1}{\left(\omega-\epsilon_k\right)^2\left(\omega'-\epsilon_k\right)}\Gamma_k\left(\omega\right)+\frac{1}{\left(\omega-\epsilon_k\right)\left(\omega'-\epsilon_k\right)^2}\Gamma_k\left(\omega'\right)\right]\right\},\end{aligned} \tag{3.82}$$

where Γ_ks are

$$\Gamma_k\left(\omega_i\right)=\sum_{\mathbf{q}}\lambda_{\mathbf{q}}^2\frac{1}{e^{\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}-e^{-\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}}\left(\frac{e^{\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}}{\omega_i-\hbar\omega_{\mathbf{q}}-\epsilon_{k-q_x}}+\frac{e^{-\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}}{\omega_i+\hbar\omega_{\mathbf{q}}-\epsilon_{k+q_x}}\right), \tag{3.83}$$

with $\omega_i=\omega,\omega'$. From Eq. (3.82) follows that $\bar{\rho}\left(\omega,\omega'\right)$ evolves as in absence of interaction, provided that ϵ_k is shifted in $\epsilon_k+\Gamma_k$. Than we interpret Γ_k as self-energy correction, and neglect all terms that are not suitable for this kind of resummation. Considering that phonons are usually very dense, we treat the sum as an integral, and write

$$\Gamma_k\left(\omega\right)=\frac{D^2\hbar}{2\rho_m cV}\sum_{q_x}\int d\tilde{q}d\Omega_{\mathbf{q}}\frac{\left|\mathbf{q}\right|}{e^{\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}-e^{-\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}}\left(\frac{e^{\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}}{\omega-c|\mathbf{q}|-\epsilon_{k-q_x}}+\frac{e^{-\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}}{\omega+c|\mathbf{q}|-\epsilon_{k+q_x}}\right), \tag{3.84}$$

where

$$\tilde{q}=\sqrt{|\mathbf{q}|^2-q_x^2}, \tag{3.85}$$

and Ω_q is the solid angle in q-space. The integral in $\tilde{q}$ gives, using

$$\lim_{\alpha\to 0}\frac{1}{x+i\alpha}\to P\left(\frac{1}{x}\right)-i\pi\delta\left(x\right),$$

and neglecting the small real correction deriving form the principal part,

$$\begin{aligned}\Gamma_k\left(\omega\right)&=i\frac{D^2 4\pi^2}{2\hbar^2\rho_m c^4 V}\\&\times\sum_{q_x}\frac{1}{e^{\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}-e^{-\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}}\{\left(\omega-\epsilon_{k-q_x}\right)^2 e^{\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}\theta\left(\omega-\epsilon_{k-q_x}\right)\theta\left[\left(\frac{\omega-\epsilon_{k-q_x}}{\hbar c}\right)^2-q_x^2\right]\\&+\left(\omega-\epsilon_{k+q_x}\right)^2 e^{-\frac{\beta\hbar\omega_{\mathbf{q}}}{2}}\theta\left(\epsilon_{k-q_x}+\omega\right)\theta\left[\left(\frac{\omega-\epsilon_{k+q_x}}{\hbar c}\right)^2-q_x^2\right]\}.\end{aligned}\tag{3.86}$$

Let us analyze which is the influence of Γ_ks on our quantum bus, in the case $g\ll w$. First, we assume the resonant condition $\Omega\equiv\epsilon_{\bar{k}}$. As described in Sec. 3.3.3, only the resonant mode is involved in the transmission, important frequencies are about $\epsilon_{\bar{k}}$, and then it is enough to calculate $\Gamma_{\bar{k}}\left(\epsilon_{\bar{k}}\right)$. Considering small values for q_x, $\epsilon_{\bar{k}}-\epsilon_{\bar{k}-q_x}\simeq -waq_x$, and $\epsilon_{\bar{k}}+\epsilon_{\bar{k}}\simeq waq_x$. At temperature $T=0$ we get

$$\Gamma_{\bar{k}}^{T=0}=i\frac{D^2\pi^2 w^2\sin^2\bar{k}a}{3\hbar^2 2\rho_m c^4 a}f\left(\bar{k}\right),\tag{3.87}$$

where $f\left(\bar{k}\right)$ is a number varying from 0 and 1 that measures the fraction of eigenmodes with energy smaller than $\epsilon_{\bar{k}}$, while for high temperatures

$$\Gamma_{\bar{k}}^{\beta}=i\frac{D^2 w\sin\bar{k}a}{\hbar^2\rho_m c^4 a}\frac{\pi}{\beta}f'\left(\bar{k}\right).\tag{3.88}$$

Let us estimate $\Gamma_{\bar{k}}$ in a concrete situation, e.g. when the quantum bus is an array of Si:P quantum dots with interdot distance which amounts to about 10nm [65, 67]. In this case one finds $\Gamma_{\bar{k}}^{T=0}\propto w^2$. Then, assuming $w\propto 10^{-3}eV$, we find a decoherence time of the order of $10^{-6}eV$, which implies that we can choose a value of $g/\sqrt{N}$ (the frequency of the QST protocol) smaller than w but larger than $\Gamma_{\bar{k}}$, and the protocol can work correctly. We can also assess that for finite temperatures up to about $10K$, coherent tunneling prevails against thermal noise.

The results are different when we consider $|\Omega| > w$. Now $\Gamma_k^{T=0}$ is similar to that obtained in resonance. The main difference is that w should be replaced by Ω. In this case the frequency of the QST protocol Λ_L can be very large and we expect damped oscillations also at zero temperature. However, so far we have not considered the Debye energy cut-off ω_D in the spectrum of phonons, that in Silicon is about $10^{-2}eV$. QST efficiency relies on the possibility of reaching for Ω values greater than ω_D.

We can conclude this section stating that QST for electrons can be achieved by means of a suitable choice of the system's parameters. Whereas in resonance this choice is perfectly compatible with the present technology, this is not completely obvious for values of Ω outside the band.

3.6 Conclusion

In this chapter we have discussed a reliable model for QST protocols [42]. After a preliminary discussion about the general problem of transferring a quantum state through a multi-mode channel, we have found a scheme that overcomes interference between modes, based on the interaction of external quantum systems with a chain, that acts merely as a bus. This model applies on a variety of physical scenarios. We have discussed various limits, finding those regimes that are actually favorable for our goal. Furthermore, we have also analyzed robustness of the bus considering a weakly disordered chain. Finally, we have analyzed the effects of a thermal environment in the physical situation of a quantum dot array.

Chapter 4

Conditional sign flip via teleportation

So far I have described possible implementations of quantum information protocols mainly based on solid state devices. Now we face optical implementation of quantum information protocols. First, in Sec. 4.1 I introduce the argument of linear optics quantum computation (LOQC) in general terms. In 4.2 a simple physical system, the beam splitter, is described. Then, Sec. 4.3 contains the description of the KLM protocol, which represents a milestone of LOQC. An original protocol to perform a two-qubit gate is presented in Sec. 4.4 and Sec. 4.5. In particular, Sec. 4.4 is devoted to the study of teleportation from an original point of view. Exploiting these concepts, one can formulate a proposal for a C-Sign gate (4.5). Conclusions are presented in Sec. 4.6.

4.1 Linear optics quantum computation

In the last decade, quantum optics represented a privileged sector where to realize peculiar schemes of quantum computation, such as quantum teleportation, optimal quantum cloning, entanglement purification, etc. The great advantage with respect to the others physical implementation [17, 69, 70] corresponds to the fact that photonic systems can be easily transferred from one place to another in the space, and moreover the weak interaction with the environment makes decoherence not so dangerous. They propagate very quickly, namely with velocity $v = c/n$ in a material with refractive index n, where c is the vacuum speed of light and typically $n = 1$ for transparent materials. Using fiber optics, photons can also be directed along arbitrary paths. Among many other advantages, such properties permit secure transmission of information over long distances, as we shall see in the next chapter [71, 72].

On the other hand, the robustness of photons with respect to interactions creates a serious obstacle to the realization of conditional gates essential for quantum computation (see Sec. 1.1) due to the large amount of resources required to create nonlinear coupling between qubits.

This scenario has been completely modified due the pioneering work of Knill, Laflamme, and Milburn [73], who proposed an efficient and fault tolerant lay-out of Quantum Information Processing (QIP) "designed" exclusively with linear optical components. Specifically, single photon sources, beam-splitters, phase-shifter and high efficiency detectors are required. Together with these instruments, KLM protocol requires the use of a number of photons bigger than those where the signal is encoded (ancilla photons) and postselection measurements over these auxiliary photons. The number of ancilla photons grows linearly with the number of operations requested from a generic circuit, keeping in this way the computational power that distinguishes QC from its classical analogous.

The realization of logic operations requires intrinsically the use of non-linear processes. Generally, non-linear coupling between single photons is not trivial to be achieved. To solve this obstacle KLM proposed to exploit the non-linearity associated to any measurement process. In fact, from a measure we learn about the photon whether or not it has been detected, independently from the applied field. Non-linearity induced by measurement is one of the relevant concepts of KLM scheme. In order to exploit this feature, one needs to use photon-number resolving detectors; moreover, since the "detection" of the vacuum state is also needed, detectors must have very high quantum efficiency (QE): the threshold value is 99%. The circuits used for implementing gates are usually probabilistic. One can see that N gates characterized by a probability p force us to repeat the operation p^{-N} times to have an acceptable result.

This feature apparently leads to an exponential grow up of the computational resource. It is shown that, over a threshold value for the success probability of a gate, resources follow a polynomial law, allowing QC to maintains its peculiar computational power respect than classical computer. The threshold of success of the gate is about to 99,99%.

4.2 The beam splitter

In this section we describe briefly the fundamental tool which will be used in the following to create a two-qubit gate, the beam splitter (BS). A BS can be represented as a linear operator which couples two input modes to two different output modes. In Fig. 4.1 we give a pictorial representation of the BS. The input-output relations between the field operators, in the case of a 50:50 BS (that is a BS with reflection and transmission characterized by the same amplitude) can be set as

$$a_1^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger + b_2^\dagger\right) \tag{4.1}$$

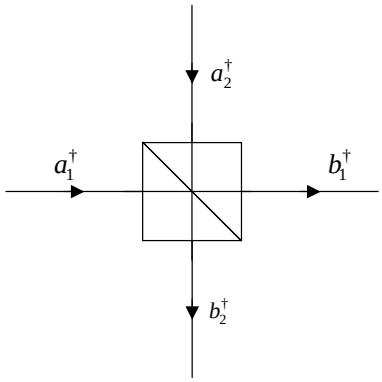

Figure 4.1. Pictorial representation of a beam splitter, which acts as a unitary transformation between input modes and output modes.

and

$$a_2^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger - b_2^\dagger\right). \tag{4.2}$$

Whenever a single photon is injected onto one of the input arms, the BS acts as an entangling machine. Indeed, introducing the beam-splitting operator $\widehat{BS}$, from Eqs. (5.3,5.4) follows that

$$\widehat{BS}\,|1_{a_1}0_{a_2}\rangle = \frac{1}{\sqrt{2}}\left(|1_{b_1}0_{b_2}\rangle + |0_{b_1}1_{b_2}\rangle\right), \tag{4.3}$$

$$\widehat{BS}\,|0_{a_1}1_{a_2}\rangle = \frac{1}{\sqrt{2}}\left(|1_{b_1}0_{b_2}\rangle - |0_{b_1}1_{b_2}\rangle\right), \tag{4.4}$$

that is, when the single photon is injected onto the mode a_1 the output state is a triplet one, while when the single photon is injected onto the mode a_2 we deal with a singlet state as output. It is worth noting that the phase convention introduced above is completely arbitrary, and a simple rotation in the space of the BS can generate different outputs. The action of the BS realizes one of one-qubit operations that are fundamental for quantum computation, the so-called Hadamard gate:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4.5}$$

All the consideration reported here can appear obvious, but they lie at the heart of the two-qubit gate that will be introduced in the next sections. Furthermore, chapter 5 will be largely based on such simple devices.

4.3 The KLM scheme

Let us describe in some details the idea of Knill, Laflamme and Milburn to implement a all-optical quantum computer. The authors adopt the "dual-rail" logic to encode qubits, i.e. a single photon over two spatial modes with the same polarization [74, 75]. Despite the lack of robustness of this encoding method with respect to the use of polarization, it allows a full-realization of a QC. Moreover, it is always possible to convert easily one representation in the other using only a polarizing beam splitter, PBS, and a half-wave plate oriented at 45°, that exchanges horizontal and vertical polarization.

The work is based on three main results:

1. the possibility of implementing a non-trivial two qubits gate employing only beam-splitters and phase shifter and non-linearity induced by detection of auxiliary photons;

2. the exploitation of a generalized teleportation protocol to enhance the success probability of the gate over the threshold bound for efficient computation;

3. the development of a code for qubits that ensures the operation robustness against possible imperfections of circuit elements, like photon losses, non-ideal detector, and phase decoherence.

To implement a scalable computation this scheme requires highly efficient photon-number-detector, QE $\geq 99\%$, very low loss short term photon storage and long state

preparation time in order to achieve the minimum accuracy required for reliable quantum computation.

Let us analyze in more details the first two results.

4.3.1 Two-qubit gate

Following [73], an essential ingredient for the realization of a non-deterministic two-qubit gate is the non-linear sign shift gate. This gate acts on a single bosonic mode iin the following way:

$$|\Psi\rangle_{in} = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle \rightarrow |\Psi\rangle_{out} = \alpha\,|0\rangle + \beta\,|1\rangle - \gamma\,|2\rangle\,. \tag{4.6}$$

The success probability of Knill, Laflamme and Milburn C-sign gate is equal to 1/16, because the NS gate works with $p = 1/4$. In spite of this probabilistic behaviour, the C-sign can be made near-deterministic adopting a generalized version of the "vacuum-single photon qubit" teleportation [76], a method that brings to a linear growth of resource and to an arbitrary enhancement of success probability (n auxiliary photons $\Longrightarrow p = 1 - 1/(n+1)$).

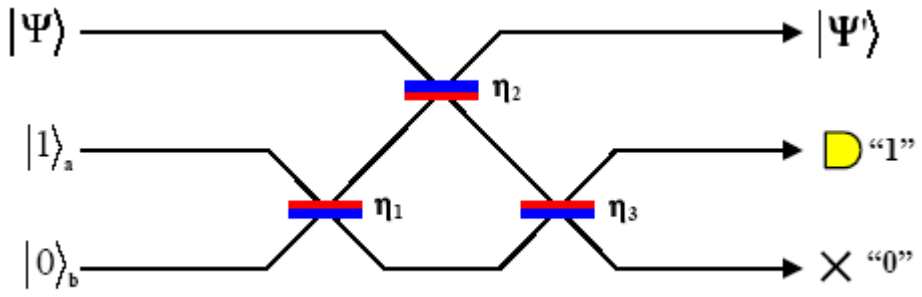

Figure 4.2. KLM Non linear sign gate.

The scheme provides two auxiliary modes, a and b (see Fig. 4.2). At the initial stage a single photon belongs on the mode a, while the mode b is unoccupied. The success of the gate is conditioned by the detection of an output photon in the mode a.

The beam-splitters used in this scheme are chosen in a way that the sign "-" of Eqs.(5.3,5.4) corresponds to reflection onto the blue surface.

Moreover the reflection coefficients, denoted in Fig. 4.2 by η_i, are chosen in order to achieve the "balancing" of the gate.

Let us consider the operation of the scheme:

- for $|\Psi\rangle = |0\rangle$ the probability amplitude C to have a photon on the output mode a is :

$$C = \sqrt{\eta_1\eta_2\eta_3} + \sqrt{(1-\eta_1)(1-\eta_3)}; \tag{4.7}$$

- for $|\Psi\rangle = |1\rangle$ the probability amplitude, C', to have a photon on the output mode a and no photon on the mode b is :

$$C' = (1-\eta_2)\sqrt{\eta_1\eta_3} - \sqrt{\eta_2}[\sqrt{\eta_1\eta_2\eta_3} + \sqrt{(1-\eta_1)(1-\eta_3)}], \tag{4.8}$$

or

$$C' = (1-\eta_2)\sqrt{\eta_1\eta_3} - C\sqrt{\eta_2}. \tag{4.9}$$

Setting $C = C'$, we have:

$$C = \frac{(1-\eta_2)\sqrt{\eta_1\eta_3}}{1+\sqrt{\eta_2}}; \tag{4.10}$$

- for $|\Psi\rangle = |2\rangle$, we require that the probability amplitude corresponding to 1 photon in mode a and 0 photons in mode b must be equal to $-C$, in order to realize the NS gate. We obtain:

$$\begin{aligned} -C &= -(1-\eta_2)\sqrt{\eta_1\eta_2\eta_3} - \sqrt{\eta_2}[(1-\eta_2)\sqrt{\eta_1\eta_3} - C\sqrt{\eta_2}] \\ &= \eta_2 C - 2(1-\eta_2)\sqrt{\eta_1\eta_2\eta_3}. \end{aligned} \tag{4.11}$$

From the preceding equation we obtain $\eta_2 = (\sqrt{2}-1)^2$, and choosing for η_1, η_3 the values that optimize C we finally derive: $\eta_1 = \eta_3 = 1/(4-2\sqrt{2})$, which implies $C = 0.5$. Then, the NS gate is deterministic and work with a probability equal to $p = C^2 = 1/4$. A simplified version of this gate has been formulated by T. Ralph *et al.* [77], achieving the value $p \simeq 0.227$.

In Ref. [73] the authors employ the NS gate to realize a probabilistic C-sign gate (the definition of the C-sign gate will be given in Sec. 4.6). Here we do not give details of the gate, which is very complex. It is enough to say that the success probability reaches the value 1/8.

After the work of KLM other schemes have been proposed to perform conditional operations. Specifically, it is worth mentioning the works of Pittman *et al.* [78, 79, 80], which use entangled ancilla states to perform a C-NOT gate with success probability $p = 1/4$. The original scheme proposed in Sec. 4.6 is strictly related to them.

4.3.2 Teleportation and KLM

The second main result of [73] consists in the use of teleportation protocol, as indicated in the seminal work of Gottesman and Chuang [81], that leads to an enhancement of the success probability of a gate, reducing the problems related to the implementation of the C-sign between two independent qubits to a remote state preparation problem. Due to the "dual-rail" encoding and to the use of only linear elements, the teleportation protocol employs the "vacuum-single photon" qubit encoding [76, 82]. This protocol achieves an efficiency that reaches 1/2. For this particular encoding we can perform the Bell measurement necessary to implement the teleportation in two different step [73]: a first measurement determines the parity p of the photon number over the two modes, a second one determines the sign s of the superposition.

Assume as input state on mode 1 the state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, if p is odd and s ="+" over mode 3 we obtain the state $\alpha|0\rangle + \beta|1\rangle$, corresponding to success of the protocol, if $s =$ " $-$ ", we have the state $\alpha|0\rangle - \beta|1\rangle$. Thus we can get the original state using a phase shifter. For even p in order to complete the protocol we must flip the vacuum state with the single photon state, and this cannot be achieved easily with linear optics. The realization of a C-sign gate "on-line" requires two distinct teleportation processes, so the success probability of the gate, starting from the "right" input state on the teleportation scheme, is $p = 1/4$. This value is well far from the threshold condition for efficient computation. Nevertheless it is possible, as enlightened in [73], to achieve arbitrary high probability adopting a generalized teleportation protocol where the usual Bell state is replaced by a larger entangled system spanning $2n$ bosonic modes, a n qubits state, expressed by:

$$|t_n\rangle = \sum_{j=00}^{n} |1\rangle^j |0\rangle^{n-j} |0\rangle^j |1\rangle^{n-j} \tag{4.12}$$

In this way the teleportation efficiency grows up to $(n+1)^{-1}$. Moreover using a simple code, that doubles the resource, this probability becomes $n^2 (n+1)^{-2}$.

The Bell measurement is replaced by a $(n+1)\,Dim$ discrete Fourier transform.

If $0 < k < n+1$ photons are detected, the teleported state will emerge on the $(n+k)$ (th) mode and the opportune transformation will be realized.

4.4 Heretical approach to quantum teleportation

Let us resume briefly the teleportation protocol. A quantum state $|\alpha_1\rangle = a|0_1\rangle + b|1_1\rangle$ is combined with a two-qubit maximally entangled Bell state $|\Psi_{23}\rangle$. A Bell measurement, performed on the qubits 1 and 2, causes the transfer on the third qubit of the superposition initially encoded on the first one, except for a unitary transformation determined by the result of the Bell measurement. From a formal

point of view, the teleportation is represented by a basis change in the combined Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$, plus a measurement. Usually the state $|\Psi_{23}\rangle$ is considered as fixed, but this is not a necessary prescription. In a more complete description, the global input state is written in terms of all possible Bell states, each of them with a probability amplitude u_i where $i = 0,z,x,y$ (the choice of symbols will appear clear in what follows), that we can use to perform the process: recalling that the Bell states are

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle \pm |11\rangle\right) \tag{4.13}$$

and

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}} \left(|10\rangle \pm |01\rangle\right), \tag{4.14}$$

we have

$$|\Phi\rangle = |\alpha\rangle_1 \left(u_0 \left|\Psi^+_{23}\right\rangle + u_z \left|\Psi^-_{23}\right\rangle + u_x \left|\Phi^+_{23}\right\rangle + u_y \left|\Phi^-_{23}\right\rangle\right). \tag{4.15}$$

After the basis change we obtain a new expression in terms of Bell states on 1 and 2:

$$\begin{aligned} |\Phi\rangle \;=\; & \sum_i \Big(\left|\Psi^+_{12}\right\rangle u_i a_{0i} \sigma_i |\alpha_3\rangle + \left|\Psi^-_{12}\right\rangle u_i a_{zi} \sigma_z \sigma_i |\alpha_3\rangle \\ & + \left|\Phi^+_{12}\right\rangle u_i a_{xi} \sigma_x \sigma_i |\alpha_3\rangle + \left|\Phi^-_{12}\right\rangle u_i a_{yi} \sigma_y \sigma_i |\alpha_3\rangle \Big), \end{aligned} \tag{4.16}$$

having introduced the Pauli matrices acting on the third qubit and

$$a_{ij} = \begin{pmatrix} 1 & -1 & 1 & i \\ 1 & -1 & -i & -1 \\ 1 & -i & 1 & 1 \\ -i & 1 & 1 & 1 \end{pmatrix}. \tag{4.17}$$

If a measurement is done by projection, e.g. on the the singlet state $\left|\Phi^-_{12}\right\rangle$, we obtain a different state of the third qubit according to the u_i selected. This result shows that teleportation acts as a controlled gate: the teleported state experiences

a unitary transformation determined by the Bell state used as an input. In the most general case both C-NOT and C-sign are contemplated respectively when u_0 and u_x or u_0 and u_z are non vanishing and by the establishment of a connection between the logic value of a qubit used as control and the suitable pair of Bell states $|\Psi_{23}\rangle$ selected. In particular, we found a simple model where this behaviour emerges giving rise to a C-sign gate. We stress that we are using teleportation in a very unusual way, fixing the Bell measurement result, and varying the input Bell state in a controlled way.

4.5 Conditional sign flip via teleportation

Next, we proceed to formulate a proposal for a feasible two-qubit gate (the C-Sign gate) following the KLM criteria. A conditional sign flip gate is a two-qubit gate: the target qubit experiences a sign change between its components $|0\rangle$ and $|1\rangle$ if and only if the control qubit is in the logic state $|1\rangle$. In the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ the unitary operator representing the gate is

$$U = |0\rangle\langle 0|^{(1)} \otimes I^{(2)} + |1\rangle\langle 1|^{(1)} \otimes \sigma_z^{(2)} \tag{4.18}$$

(I and σ_z are respectively the identity operator and one of Pauli matrices), and has the following matrix representation:

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{4.19}$$

As requested in [73] each qubit is realized on two spatial modes: the presence of the photon in the first (second) rail corresponds to the logic state $|1\rangle$ ($|0\rangle$). For the sake of clarity we shall utilize the second quantization language, using occupation numbers instead of logic values, writing $|01\rangle$ for $|0\rangle$ and $|10\rangle$ for $|1\rangle$.

4.5.1 Teleportation of a vacuum–one-photon qubit

The starting point of our description is the experimental realization of vacuum-one photon qubit teleportation [76, 82, 83], whose set-up is sketched in Fig. 4.3.

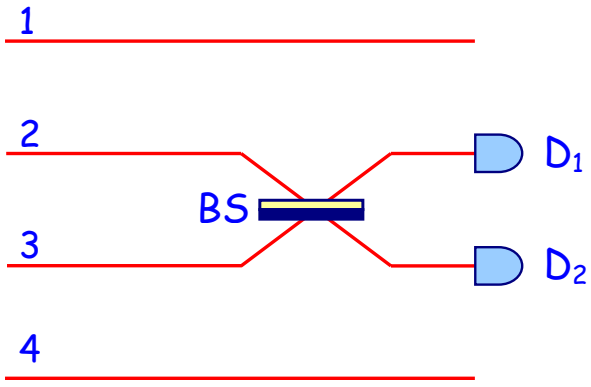

Figure 4.3. Teleportation of vacuum–one-photon quantum bit. Target and ancilla qubits are each defined by a single photon occupying two optical modes. When detector D_1 records a single photon, the state in modes 1-4 reproduces the initial state of the target. In particular, the coherence between modes 1-2 of the target can be transferred to a coherence between modes 1-4.

The modes 1 and 2 define an entangled single-photon state (say a singlet state):

$$|\Psi_{12}\rangle = \frac{1}{\sqrt{2}}\left(|1_1 0_2\rangle - |0_1 1_2\rangle\right), \tag{4.20}$$

while an unknown state is realized onto the modes 3 and 4:

$$|\Psi_{34}\rangle = \alpha\,|1_3 0_4\rangle + \beta\,|0_3 1_4\rangle \tag{4.21}$$

A BS mixes the modes 2 and 3 giving for the overall state

$$\begin{aligned} |\Psi\rangle \;=\; & \frac{\alpha}{2}\left(|1_1 1_2 0_3 0_4\rangle - |1_1 0_2 1_3 0_4\rangle - |0_1 2_2 0_3 0_4\rangle + |0_1 0_2 2_3 0_4\rangle\right) \\ & + \frac{\beta}{2}\left(\sqrt{2}\,|1_1 0_2 0_3 1_4\rangle - |0_1 1_2 0_3 1_4\rangle - |0_1 0_2 1_3 1_4\rangle\right), \end{aligned} \tag{4.22}$$

or

$$\begin{aligned} |\Psi\rangle \;=\; & -\frac{1}{2}\left(\alpha\,|1_1 0_4\rangle + \beta\,|0_1 1_4\rangle\right)|1_2 0_3\rangle + \frac{1}{2}\left(\alpha\,|1_1 0_4\rangle - \beta\,|0_1 1_4\rangle\right)|0_2 1_3\rangle \\ & + \frac{\beta}{\sqrt{2}}\,|1_1 0_2 0_3 1_4\rangle - \frac{\alpha}{2}\left(|0_1 2_2 0_3 0_4\rangle - |0_1 0_2 2_3 0_4\rangle\right). \end{aligned} \tag{4.23}$$

The prior result has the following interpretation. Whenever one and only one photon is detected by one of the detectors, the system realizes a teleportation from the modes 1 and 2 to the modes 1 and 4. As in the general version of teleportation, a deterministic unitary rotation is necessary when the photon is detected by the detector D_2. On the other hand, in the case of detection of zero photons or two photons the operation fails. This occurrence fixes the efficiency to 1/2. The preceding result is also suitable to be read in terms of entanglement swapping [83].

4.5.2 Destructive C-sign gate

The machine introduced in the previous paragraph is the building block to realize a conditional gate, as depicted in Fig. 4.4. In agreement with the general definition of the C-sign gate, we define a target qubit and a control qubit, each of them being defined over two spatial modes. The rails of the control qubit are the input arms of a 50% beam splitter (BS_1) that acts as an Hadamard gate (see Eq. (4.5)). Then, if the input photon is in the state $|01\rangle$, the output state is an entangled singlet state, while if it is in the state $|10\rangle$ we deal with a triplet one on the output arms. The entangled states created in such a way are used to perform teleportation.

One of spatial modes outgoing from BS_1 is mixed on a second 50% beam splitter (BS_2) with one of spatial modes of the target qubit. With reference to Fig. 4.4, we denote with 1 and 2 the modes associated to the control qubit, with $1'$ and $2'$ the output modes of BS_1 and with 3 and 4 the modes corresponding to the target qubit.

Let us consider first the case in which the control qubit is in the state $|1_1 0_2\rangle$. Due to the action of the Hadamard gate the state after the photon has impinged BS_1 is $1/\sqrt{2}\,(|0_{1'}1_{2'}\rangle + |1_{1'}0_{2'}\rangle)$. This is a triplet entangled state realized over the output spatial modes of BS_1.

If the target qubit is in the arbitrary superposition $\alpha\,|0_3 1_4\rangle + \beta\,|1_3 0_4\rangle$ the whole

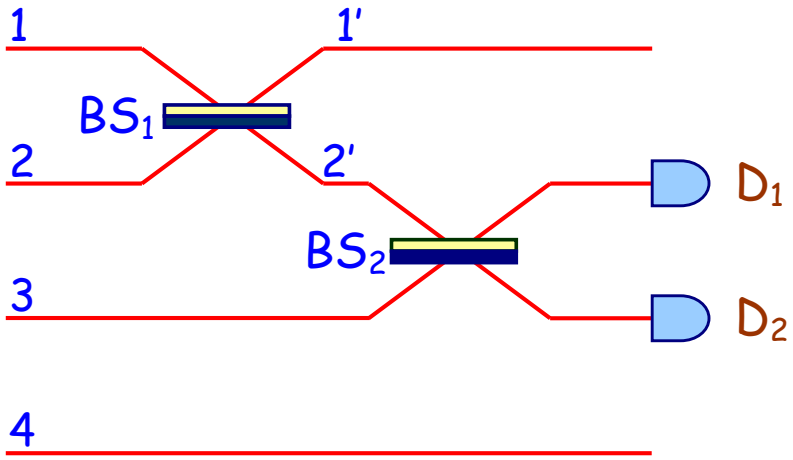

Figure 4.4. Destructive conditional sign flip gate: the modes 1 and 2 correspond to the control qubit, while the modes 3 and 4 correspond to the target qubit. The beam splitter BS_1 acts as an Hadamard gate on the control qubit and BS_2 is used to perform quantum teleportation.

state is

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(\alpha\,|0_{1'}1_{2'}0_3 1_4\rangle + \beta\,|0_{1'}1_{2'}1_3 0_4\rangle + \alpha\,|1_{1'}0_{2'}0_3 1_4\rangle + \beta\,|1_{1'}0_{2'}1_3 0_4\rangle\right) \quad (4.24)$$

The portion of this state corresponding to the spatial modes $2'$ and 3 is conveniently rewritten in terms of Bell states $|\Phi^{\pm}\rangle = 1/\sqrt{2}\,(|00\rangle \pm |11\rangle)$ and $|\Psi^{\pm}\rangle = 1/\sqrt{2}\,(|10\rangle \pm |01\rangle)$. After this substitution we have

$$\begin{aligned} |\Psi\rangle \;=\; & \frac{1}{2}\Big[\left|\Psi^{+}_{2'3}\right\rangle\left(\alpha\,|0_{1'}1_4\rangle + \beta\,|1_{1'}0_4\rangle\right) + \left|\Psi^{-}_{2'3}\right\rangle\left(\alpha\,|0_{1'}1_4\rangle - \beta\,|1_{1'}0_4\rangle\right) \\ & + \left|\Phi^{+}_{2'3}\right\rangle\left(\alpha\,|1_{1'}1_4\rangle + \beta\,|0_{1'}0_4\rangle\right) + \left|\Phi^{-}_{2'3}\right\rangle\left(\alpha\,|1_{1'}1_4\rangle - \beta\,|0_{1'}0_4\rangle\right)\Big] \end{aligned} \quad (4.25)$$

Our idea is to perform a projective measurement over the modes $2'$ and 3 by selecting only those events corresponding to the state $\left|\Psi^{-}_{2'3}\right\rangle$ as result. The measurement is performed using these modes as the input arms of BS_2. The state $\left|\Psi^{-}_{2'3}\right\rangle$ corresponds to the detection of one and only one photon on the detector D_1 and to the absence of counts on the second detector D_2. As a result, the state emerging on the spatial modes $1'$ and 4 is $\alpha\,|0_{1'}1_4\rangle - \beta\,|1_{1'}0_4\rangle$. We observe that an entanglement swapping has been realized together with a sign flip with respect to the incoming target state.

Next, we study the situation corresponding to a control qubit in the state $|0_1 1_2\rangle$. In such a situation the Hadamard gate creates a singlet entangled state on the output modes of BS_1: $1/\sqrt{2}\,(|0_{1'}1_{2'}\rangle - |1_{1'}0_{2'}\rangle)$. Then Eq. 4.25 has to be opportunely modified. Limiting our interest to the term associated with the singlet as output result, now we have $\left|\Psi_{2'3}^{-}\right\rangle\,(\alpha\,|0_{1'}1_4\rangle + \beta\,|1_{1'}0_4\rangle)$. Thus, we observe again an entanglement swapping, but the difference with the former situation is that no sign flip arises from the process.

The previous results can be synthesized stating that the target qubit, initially encoded using the modes 3 and 4, is transferred on $1'$ and 4 with a sign change conditional to the logic state of the control qubit, as required from the definition of the C-sign gate. The gate is deterministic: it does not work with a success probability equal to 1, but we know whether it works correctly. In our case the probability is 1/4, determined by the postselection procedure selecting one of four Bell states, and it can increased up to 1/2 accepting single counts on D_2, with an adjunctive single qubit rotation. If both singlet and triplet state are accepted we deal with the so-called active teleportation [82].

Unluckily, the control qubit is destroyed by the projection and the gate above illustrated is not complete. To make the scheme useful for quantum computation a method to restore the control state has to be introduced.

4.5.3 Nondestructive C-sign gate

To overcome the previous obstacle we use the technique of quantum encoding. From the "no cloning theorem" [84] we learn that a physical machine able to copy an arbitrary quantum state in a blank state cannot be realized. However, the theorem does not exclude the possibility of copying two selected orthogonal states and this is the working principle of a quantum encoder. Roughly speaking, the conversion $(\alpha\,|0\rangle + \beta\,|1\rangle) \rightarrow (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\alpha\,|0\rangle + \beta\,|1\rangle)$ is forbidden while $(\alpha\,|0\rangle + \beta\,|1\rangle) \rightarrow$

$(\alpha\,|0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle)$ is (at least in a probabilistic way) allowed leaving α and β out of consideration.

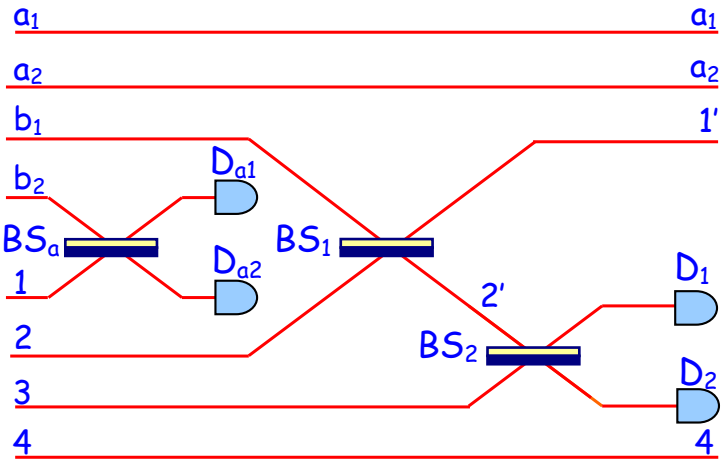

Figure 4.5. Nondestructive conditional sign flip gate: the modes a_1, a_2, b_1 and b_2 represent the quantum encoder, control and target qubit are yet implemented respectively on the modes 1 and 2 and 3 and 4 . The auxiliary beam splitter BS_a and the auxiliary detectors D_{a_1} and D_{a_2} are used to "double" the control qubit in an entangled state on a_1, a_2, b_1 and 2. BS_1 and BS_2 perform the conditional gate and the output is represented by the control qubit on the modes $a_1$and a_2 and the (modified by the gate) target qubit on the modes $1'$and 4.

A quantum encoder operating on polarization qubits is described in [80, 85]. It applies also in our case due to the existence of converters from polarization to dual rail and vice versa that are easily realizable using a polarizing beam splitter and a $\lambda/2$ wave plate. On the other hand, we will show that a quantum encoder working only with photon number qubits is feasible using non polarizing beam splitters. The scheme is depicted in Fig. 4.5. The control qubit $(\alpha_1\,|01\rangle + \alpha_2\,|10\rangle)$ we want to copy is defined on the modes 1 and 2, while modes a_1, a_2, b_1, and b_2 correspond to two ancilla qubits previously prepared in the maximally entangled state $1/\sqrt{2}\,(|0_{a_1}1_{a_2}0_{b_1}1_{b_2}\rangle - |1_{a_1}0_{a_2}1_{b_1}0_{b_2}\rangle)$. The modes b_2 and 1 are mixed on a beam splitter (BS_a) and a projective measurement analogous to that one described in Sec. 4.5.2 takes place selecting only the singlet state $\left|\Psi^-_{b_2 1}\right\rangle = 1/\sqrt{2}\,(|0_{b_2}1_1\rangle - |1_{b_2}0_1\rangle)$.

The projection is performed measuring one and only one photon on D_{a_1} and zero photons on D_{a_2}. As a result, it remains $1/\sqrt{2}\,(\alpha_1\,|0_{a_1}1_{a_2}0_{b_1}1_2\rangle + \alpha_2\,|1_{a_1}0_{a_2}1_{b_1}0_2\rangle)$. Thus, we have realized the quantum encoding operation, apart from a swapping from mode 1 to b_1. This gate is probabilistic being conditioned from the output of the Bell measurement. The success probability is 1/4 and again it reaches 1/2 if also $\left|\Psi^+_{b_21}\right\rangle = 1/\sqrt{2}\,(|0_{b_2}1_1\rangle + |1_{b_2}0_1\rangle)$ is accepted via a classically feed-forwarded one qubit rotation. Notice that a qubit can be encoded also on a string of n qubits simply using a generalized maximally entangled state $1/\sqrt{2}\,(|0101.....01\rangle - |1010.....10\rangle)$ and performing the projection measurement mixing one of the $2n$ modes with one mode of the incoming qubit.

Let us return to our main problem. We want to build a gate that transforms a two qubit state, defined on four spatial modes, in accordance with the operator U introduced in Eq. 4.19:

$$\begin{aligned} &U\,(\alpha_1\,|0_1 1_2\rangle + \alpha_2\,|1_1 0_2\rangle) \otimes (\alpha_3\,|0_3 1_4\rangle + \alpha_4\,|1_3 0_4\rangle) = \\ &\alpha_1\alpha_3\,|0_1 1_2 0_3 1_4\rangle + \alpha_1\alpha_4\,|0_1 1_2 1_3 0_4\rangle + \alpha_2\alpha_3\,|1_1 0_2 0_3 1_4\rangle - \alpha_2\alpha_4\,|1_1 0_2 1_3 0_4\rangle \end{aligned} \tag{4.26}$$

The control state is doubled via the quantum encoder above introduced and, under the probabilistic condition relied to the postselection process, we deal with the initialized three qubit state

$$|\Psi\rangle = (\alpha_1\,|0_{a_1}1_{a_2}0_{b_1}1_2\rangle + \alpha_2\,|1_{a_1}0_{a_2}1_{b_1}0_2\rangle)\,(\alpha_3\,|0_3 1_4\rangle + \alpha_4\,|1_3 0_4\rangle) \tag{4.27}$$

The procedure described in Sec. 4.5.2 can now start: the modes b_1 and 2 are rearranged in $1'$ and $2'$ via the BS_1, the modes $2'$ and 3 are mixed on BS_2, the postselection measurement on $\left|\Psi^-_{2'3}\right\rangle$ is performed, and as a result of the complete set of operations we find that U creates the state $\alpha_1\alpha_3\,|0_{a_1}1_{a_2}0_{1'}1_4\rangle + \alpha_1\alpha_4\,|0_{a_1}1_{a_2}1_{1'}0_4\rangle + \alpha_2\alpha_3\,|1_{a_1}0_{a_2}0_{1'}1_4\rangle - \alpha_2\alpha_4\,|1_{a_1}0_{a_2}1_{1'}0_4\rangle$, in perfect agreement with the definition of the C-sign gate. Furthermore, the scheme realizes a teleported gate, as outlined in [81].

Due to the nondeterministic nature of the destructive gate and the quantum encoder, the nondestructive C-sign flip can reach 1/4 as overall efficiency.

4.6 Conclusions

We have proposed a method to realize a probabilistic C-sign flip gate for number state qubits based only on few linear optics elements, specifically three balanced beam splitters, two single photon sources for target and control qubits, photodetectors, postselection measurements, and entangled ancilla photons, which can be created via single-photon sources [86]. The maximum success probability is 1/4. In the original proposal contained in [73] the C-sign gate was achieved via two nonlinear sign shift combined with two beam splitters. The network created in such a scheme was very intricate, and the simplification arising from the idea previously illustrated is remarkable. To achieve the gate, a four fold coincidences measurement is required, fully available with the present technology.

Chapter 5

Quantum key distribution with single-photon entangled states

In this chapter I will present an original scheme to create a quantum key distribution [87]. In Sec.5.1 I will introduce the concept of quantum cryptography, together with some protocol which is particularly important for historical reasons. Then, in Sec. 5.2 the original model is introduced and discussed in detail. Conclusions are presented in Sec. 5.3.

5.1 Quantum cryptography

The first suggestion about quantum cryptography, or, more correctly, Quantum Key Distribution (QKD) is due to Wiesner [88], whereas the concretization derives from the work of Bennett&Brassard in 1984 and is known with the acronym BB84 [71]. Quantum Key Distribution arises from the idea of using the laws of quantum mechanics to perform secure communication. In particular, QKD exploits two theorems deriving from Heisenberg uncertainty principle: i) the no-cloning theorem [84] states that it not possible to realize a perfect copy of an unknown quantum state; ii) the

Lo-Chau lemma [89] states that it is not possible to measure an unknown quantum state without perturbing it.

A brief introduction to key distribution can be formulated in the following way.

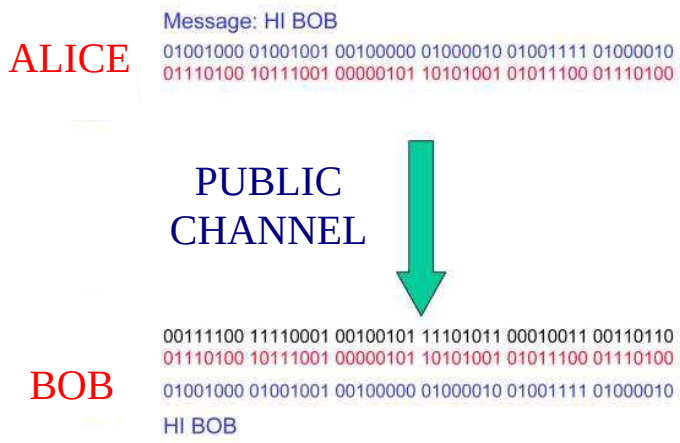

Figure 5.1. Secure communication via quantum key distribution. Alice wants to send a message (blue string)to Bob. Alice and Bob share a secret key (red string). The black string is the sum $\bigoplus 2$ of key and message, and is what Alice transmits using the public channel. Bob accomplishes the same operation (sum $\bigoplus 2$, or, equivalently, difference $\bigoplus 2$) and gets the message. The sequence of bits which is transmitted on the public channel has no relation with the message, and its knowledge is useless without knowing the key.

The usual way to describe the process is to introduce a sender (Alice) and a receiver (Bob), who are trying to exchange a private message in a secure way using a public channel. A key is a string of bits which is shared by Alice and Bob, and which Alice uses to encrypt the message and Bob uses to decrypt it. Indeed, she sends on the public channel the sum of the message itself and the key, as depicted schematically in Fig. 5.1. QKD involves the way to create a shared key whose secrecy is built up using quantum mechanics..

In the following we give a description of the most important QKD protocols [90].

5.1.1 The BB84 protocol

Let us consider a two-level system (for the sake of concreteness we will refer to a spin 1/2).

The protocol uses four quantum states that constitute two orthogonal bases, for example, the states $|\uparrow\rangle$, $|\downarrow\rangle$, $|\leftarrow\rangle$, and $|\longrightarrow\rangle$. $|\uparrow\rangle$ and $|\downarrow\rangle$ are eigenstates of S_z, $|\leftarrow\rangle$ and $|\longrightarrow\rangle$ are eigenstates of S_x. For instance, one can assume that $|\uparrow\rangle$ and $|\leftarrow\rangle$ correspond to the classical bit "0", while $|\downarrow\rangle$ and $|\longrightarrow\rangle$ correspond to "1". In the first phase of the protocol, Alice sends spins to Bob by choosing randomly each time one of four states. Then, Bob, using a random-number generator independent from that of Alice, measures the incoming spins in one of the two bases. As a result, whenever the basis chosen is the same, Alice and Bon get perfectly correlated results. On the other hand, if the bases are different, they get uncorrelated results. The way to discard these latter unwanted data is to use a classical channel together with the quantum one. The classical channel is assumed to be public, but it cannot be altered by any adversary (usually called Eve). For each bit Bob announces publicly in which basis he measured the corresponding qubit, without announcing its result. Alice then reveals only whether or not the state in which she encoded that qubit is compatible with the basis announced by Bob. Then, they keep only the results corresponding to the same choice of basis, and share the so called sifted key.

Let us now consider the security of the above ideal protocol against Eve who intercepts a qubit propagating from Alice to Bob. Obviously, Bob must receive the qubit. The no-cloning theorem does not allow to copy the qubit. Then, Eve cannot simply keep the qubit but she must study some eavesdropping strategy. The simplest attack is the so-called intercept-resend strategy: Eve measures each qubit in one of the two bases, like Bob. Then, she re-sends to Bob the qubit emerging from her apparatus in the state corresponding to her measurement result. In about half of the cases, Eve will choose the basis compatible with the state encoded by Alice.

In these cases she re-sends a spin in the correct state, and Alice and Bob will not notice her presence. On the other hand, in the remaining half of the cases, Eve uses the basis incompatible with the state prepared by Alice. This necessarily happens, since Eve has no information about Alice's random-number generator (randomness is fundamental). In these cases the qubits sent out by Eve are in states with an overlap of 1/2 with the correct states. A control routine can be introduced at the end of the bit exchange. Alice and Bob select arbitrarily a given number of bits and compare their operations using the public channel. In this way they discover Eve's intervention in about half of the cases corresponding to her bad basis choice. The measure of Eve'influence on the key is the quantum bit error rate (QBER). In the case of the BB84 protocol it amounts to 1/4 of the number of bit intercepted by Eve. If Alice and Bob find a number of errors largest that a threshold value, which can be fixed considering unavoidable effects due to noise and losses in the channel, they discover Eve and abort the transmission.

5.1.2 The B92 protocol

This scheme [91] differs from the BB84 scheme, since it shows that two non-orthogonal states are sufficient create a secure key. The states Alice can select randomly are $|\uparrow\rangle$ and $|\longrightarrow\rangle$. Bob realizes a POVM measurement [1] using the projectors $P_\uparrow = I - |\uparrow\rangle\langle\uparrow|$ or $P_\rightarrow = I - |\longrightarrow\rangle\langle\longrightarrow|$. What happens is that $P_\uparrow|\uparrow\rangle = 0$, $P_\rightarrow|\longrightarrow\rangle = 0$, $\langle\longrightarrow|P_\uparrow|\longrightarrow\rangle = 1 - |\langle\longrightarrow|\uparrow\rangle|^2$, $\langle\uparrow|P_\uparrow|\uparrow\rangle = 1 - |\langle\longrightarrow|\uparrow\rangle|^2$. The key is built as follows. Each time Bob obtained a finite value from his apparatus, he know that if he measured $P_\uparrow$, then Alice prepared $|\longrightarrow\rangle$, and if he measured $P_\rightarrow$, then Alice prepared $|\uparrow\rangle$. Then, it is sufficient that Bob publicly tells Alice in which cases he found a finite result without announcing which measurement he made. All others runs will be discarded. The presence of Eve could cause events where, e.g., Bob find a result different from zero even in cases where Alice sends $|\uparrow\rangle$ and he is

measuring $P_{\uparrow}$, or Alice sends $|\longrightarrow\rangle$ and he is measuring $P_{\longrightarrow}$. A control routine can reveal easily the presence of the eavesdropper in the channel, as in the previous case by selecting a random subset of data and verifying the consistency of results with the premises.

5.1.3 The EPR protocol

The model described in this section has been introduced by A. Ekert [72], following a suggestion of D. Deutsch [92]. In this case the quantum channel carrying two qubits from Alice to Bob is substituted by a channel carrying two qubits from a common source, one qubit being addressed to Alice the other one being addressed to Bob. The two qubits are prepared in the singlet state

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\,,\downarrow\rangle - |\downarrow\,,\uparrow\rangle\right), \tag{5.1}$$

which is invariant under rotations,

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\,,\longrightarrow\rangle - |\longrightarrow\,,\uparrow\rangle\right). \tag{5.2}$$

Alice and Bob measure their respective qubits both selecting in random way among two orthogonal bases, as in the BB84 case. Obviously, whenever the basis selected by Alice is the same selected by Bob, their respective results are perfectly anti-correlated. Then, either of them can know the state obtained by the other, and a key can be obtained. Those data corresponding to a different basis choice are discarded. In his paper Ekert suggested that the security of this two-qubit protocol can be connected to the Bell's inequality, which shows that quantum mechanics exhibits correlations that cannot be reproduced by any local theory [93]. Some time ago, it has been shown by Bennett, Brassard, and Mermin [94] that there is complete equivalence between the EPR scheme and the BB84 scheme.

5.2 Exploiting single-photon entanglement to generate a quantum key distribution

In the previous section we described a number of protocols to create a QKD without considering any physical system in a specific way. Although in principle the polarization of photons is a natural candidate, in long distance communication through optical fibers birefringence effects advice against the use of polarization. Then, schemes using the phase-coding technique, i.e. schemes where the degree of freedom used to define the bits is the phase inside some quantum state [95, 96, 97, 98], are very useful for practical purposes.

Here we propose a new method of phase encoding based on vacuum-one photon entangled states, which involves a complete symmetry between Alice and Bob, and is designed for stable transmission [87]. A very different proposal for quantum cryptography which uses also single-particle entanglement appears in Ref. [99]. The scheme is depicted in Fig. 5.2. Alice wants to create a key and to share it with Bob. She uses a single photon source [100, 101] which injects the photon either on the mode a_1 or on the mode a_2. The modes a_1 and a_2 are mixed in a beam splitter (BS_a) and then the single photon is entangled on the two output modes a_1' and a_2'. In terms of field operators, the BS_a action on the input-output modes is represented by

$$\hat{a}_1^\dagger = \frac{1}{\sqrt{2}}\left(\hat{a}_1'^\dagger + \hat{a}_2'^\dagger\right) \tag{5.3}$$

and

$$\hat{a}_2^\dagger = \frac{1}{\sqrt{2}}\left(\hat{a}_1'^\dagger - \hat{a}_2'^\dagger\right). \tag{5.4}$$

($\hat{a}_i^\dagger$ creates a photon on the mode a_i) Thus, the output state is $2^{-1/2}\left(|01\rangle + |10\rangle\right)$ if the photon is put in the mode a_1 or $2^{-1/2}\left(|01\rangle - |10\rangle\right)$ if the photon is put in the mode a_2. These two possible choices represent the logic values (the bit) which Alice wants to add in the QKD. Therefore, the bit is encoded in the phase of the entangled

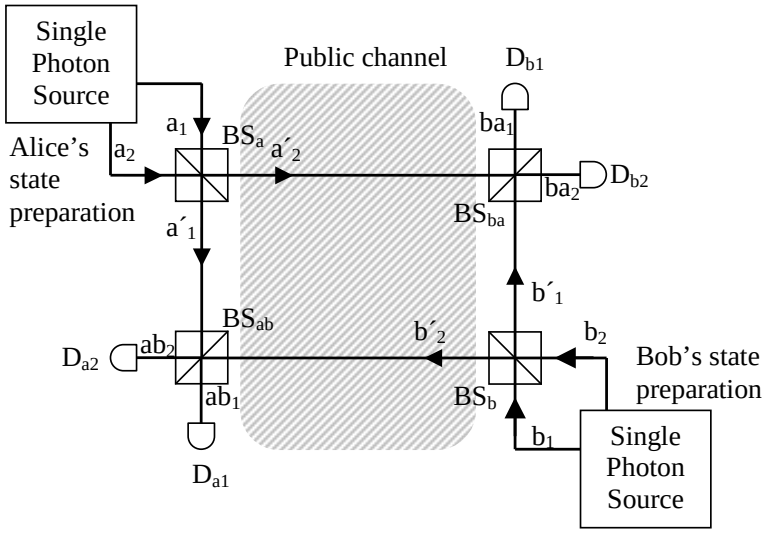

Figure 5.2. Scheme for QKD using two single photon entangled states. The shaded area represents the public channel and is the region where eavesdropping can take place. Alice (left side) and Bob (right side) use the respective single photon sources to create two entangled states, encoding the bit on the phase, on the output modes of BS_a and BS_b. Each of them stores one mode in a secure area and sends the other mode to the counterpart. The protocol is concluded via the recombination on the beam splitters BS_{ab} and BS_{ba} and the statement of Alice (the scheme works also exchanging the roles) of which detectors (D_{a1} or D_{a2}) has counted one photon. Comparing this information with his result (click on D_{b1} or D_{b2}), Bob acquires the secret information.

state emerging from BS_a which we conveniently rewrite as $2^{-1/2}\left(|01\rangle + n\,|10\rangle\right)$ with $n = -1{,}1$ ($n = 1$ will correspond to the logic value 1, $n = -1$ will correspond to the logic value 0).

Bob, being far apart, realizes the same operation through his own apparatus and creates the state $2^{-1/2}\left(|01\rangle + m\,|10\rangle\right)$ (again, $m = -1{,}1$) on the modes b'_1 and b'_2. Obviously, n and m are completely uncorrelated.

Afterwards, Alice (Bob) stores the mode a'_1 (b'_1) and sends to Bob (Alice) the mode a'_2 (b'_2). Each of them has a second beam splitter (BS_{ab} and BS_{ba}) which is used to mix the mode previously stored with the mode received from the counterpart.

The initial state is

$$|\phi\rangle = \frac{1}{2}\left(\left|0_{a'_1}1_{a'_2}\right\rangle + n\left|1_{a'_1}0_{a'_2}\right\rangle\right)\left(\left|0_{b'_1}1_{b'_2}\right\rangle + m\left|1_{b'_1}0_{b'_2}\right\rangle\right). \tag{5.5}$$

Because of the unitary operation associated to BS_{ab} and BS_{ba}, which consists of field mode relations analogous to Eqs. (5.3) and (5.4), the state $|\phi\rangle$ becomes

$$\begin{aligned} |\phi\rangle \;=\; & \frac{1}{2\sqrt{2}}[m\left(|0_{ab_1}0_{ab_2}2_{ba_1}0_{ba_2}\rangle - |0_{ab_1}0_{ab_2}0_{ba_1}2_{ba_2}\rangle\right) \\ & + n\left(|2_{ab_1}0_{ab_2}0_{ba_1}0_{ba_2}\rangle - |0_{ab_1}2_{ab_2}0_{ba_1}0_{ba_2}\rangle\right) \\ & + (mn-1)\left(|0_{ab_1}1_{ab_2}1_{ba_1}0_{ba_2}\rangle + |1_{ab_1}0_{ab_2}0_{ba_1}1_{ba_2}\rangle\right) \\ & + (mn+1)\left(|0_{ab_1}1_{ab_2}0_{ba_1}1_{ba_2}\rangle + |1_{ab_1}0_{ab_2}1_{ba_1}0_{ba_2}\rangle\right)]. \end{aligned} \tag{5.6}$$

The protocol provides a measure realized both by Alice and Bob on the output modes of BS_{ab} and BS_{ba}. The scheme works if and only if one and only one photon is detected by Alice and one and only one photon is detected by Bob. Thus, the terms corresponding to two photons entering in one beam splitter and zero photons entering in the other beam splitter do not contribute, fixing to 1/2 the efficiency of the model.

Here we note that, in order to observe quantum interference on BS_{ab} and BS_{ba}, and this is exactly the situation from which Eq. (5.6) is derived, the wavepackets impinging the input arms of the beam splitters are required to be completely

indistinguishable [106]. To create such a situation the stored modes have to be opportunely delayed.

Let us suppose that Alice measures one photon on the mode ab_1. The state corresponding to this result is

$$|\phi\rangle = \frac{1}{2}[(mn+1)\,|1_{ab_1}0_{ab_2}1_{ba_1}0_{ba_2}\rangle + (mn-1)\,|1_{ab_1}0_{ab_2}0_{ba_1}1_{ba_2}\rangle]. \qquad (5.7)$$

As a consequence, Bob will detect his photon on the mode ba_1 if $m = n$ or on the mode ba_2 if $m = -n$. If Alice had counted "1" on the mode ab_2 the role of Bob's detectors would change with respect to the relation between m and n.

Then, Alice sends on the public channel her result to Bob, who, comparing the two results, is able to identify the value of n to add to the key. Due to the complete randomness of the output Alice's result, there is no connection between the information sent on the public channel and n. We assume that Alice and Bob perform the measurements in time coincidence. The public statement of which detector has counted 1 photon can take place after the entire key has been realized, as usual in QKD schemes, in analogy with basis reconciliation in the BB84.

Analyzing the scheme, one can state that the bit exchange is realized via entanglement swapping [102] from the modes a'_1, a'_2 and b'_1, b'_2 to the modes ab_1, ab_2 and ba_1, ba_2, as already suggested in the framework of quantum cryptography [103, 104]. The scheme described is in some aspect related to a cryptographic system recently realized [105]: also in that system both Alice and Bob create and exchange the key. The main differences concern the encrypting method (the polarization of photons) and a time hierarchy between Alice's and Bob's operations. As we shall later, this aspect will appear significant in the security of the scheme.

As in any QKD scheme, we need to consider the possibility that an eavesdropper (Eve) is trying to gain information, or simply to disturb the transmission in order to create errors in the reception.

Then, a control procedure has to be introduced. The simple idea is as follows: for

a random subset of bits, during the public discussion, Alice can claim both which detector has recorded the photon and the value of n encoded, giving to Bob the possibility to verify that the global state was not affected by external interactions.

5.2.1 Analysis of security and efficiency

Apart from limitations on QKD arising from experimental imperfections regarding generation, transmission and detection of qubits [107], we shall focus our attention on some simple attack strategy by some external eavesdropper.

First we describe the possibility of an attack only aimed to create errors in the key. If the disturbance consists in the subtraction of one photon the protocol automatically fails and there are no effects on the QKD creation. Better, Eve can act modifying the phase of the photons traveling in the public channel by an amount between 0 to π. In such a circumstance the control procedure is able to detect the interference: if the phase change is π the role of detector pairs with respect to m and n is completely inverted, and when Alice announces both the result and n, Bob immediately discovers Eve's action. More significant is the case of phase change equal to $\pi/2$: now just about in 50% of cases the action induces an error, and it's possible that when Alice launches the control routine Bob does not note the introduction of a third part. However, after ν control steps, the probability that Eve is not revealed is $(1/2)^{\nu}$ and can be arbitrarily reduced. In the case of phase variation less than $\pi/2$ the number of control routines to get a given confidence level increases, but the probability that Eve's action influences the key decreases.

Let us consider the case that Eve wants actually to get the key. Since the secret is encoded in the phase of an entangled state, and one of the components of the state is not accessible to anyone but Alice, there is no way to get information acting only on the public mode. Formally, this feature is expressed stating that the reduced density matrix of a single mode is diagonal and corresponds to a one-qubit maximally mixed

state. The simplest method Eve can use is the intercept/resend strategy using the same setup as Bob. Naturally, Eve does not know neither n nor m and has to create a different one-photon entangled state $2^{-1/2}\left(|01\rangle + p\,|10\rangle\right)$ $(p = -1{,}1)$, to mix her state with Alice's state and to wait from Alice announcement about the measurement result to conclude the operation. As in the regular procedure between Alice and Bob, the scheme fails in half number of cases, while in the remaining cases Eve acquires the bit. The quantum bit error rate (QBER) introduced by Eve in the sifted key (here represented by all bit exchanges with one photon detected by Alice and one photon detected by Bob) is 1/2, due to lack of correlation between n and p, while the amount of information gained by Eve is 1/2 per bit. Thus, comparing our model with the BB84, we conclude that, while Eve gets the same amount of information, she induces a QBER which is twice, and this feature strongly improves the robustness of the system against these attacks.

On the other hand, even when the eavesdropping action is performed, Bob needs to receive a mode from Alice. This aspect involves the resending strategy that Eve can choice. Eve used one photon to copy Bob's operation, and whichever is the number of photon sent to Bob (0,1, a combination of 0 and 1) the total number of photon revealed by Alice and Bob is no longer 2, but depends on the measurement process. Hence, by checking the numbers of contemporary clicks, Alice and Bob discover the presence of an eavesdropping action and abort the transmission. Moreover, even if the total photon number is 2, by the control routine above mentioned, Eve can be detected, due to the complete absence of correlation between n,m,p. One can argue that the eavesdropper can first find n and then send to Bob the correct state $2^{-1/2}\left(|01\rangle + n\,|10\rangle\right)$, but Alice's announcement happens after Bob measure, so that the use of coincidence measurements guarantees against this kind of action.

A more detailed analysis of eavesdropping influence on the counting rate can be formulated as follows. At the time of her own measurement, Eve learns how many

photons Alice will count. Let us suppose that she is so able (Eve is a quantum devil) first to perform the measurement and successively to choice the resending strategy. The following situations are possible: (i) Eve knows that Alice will measure two photons: in such a case the best choice she can made is to send nothing to Bob; (ii) Alice measures zero photons: now the choice to minimize the error is to send ever one photon to Bob; (iii) Alice measures one photon: now the resending strategy does not matter. As a result, eavesdropping modifies the number of detected photons in 1/2 of cases.

Therefore, the control about the counting rate represents a powerful method to reveal eavesdropping to add to the control routine. Actually, in order to exploit this feature, a multi-photon resolution is needed, and this not yet fully available in the present laboratory technology, although some important step has been made [108, 109].

Naturally, Eve can use an alternative strategy. She can create in any circumstance two entangled states to share with Alice and Bob, and, moreover, she can prepare other fake photons to send in order to enforce both Alice and Bob to count ever one photon. The cost to pay for this strategy is the following: due the probabilistic nature of projections, Alice and Bob expect to measure one photon just in 1/2 of cases; then Eve should simulate such behaviour leaking a big amount of information. Thus, this strategy is not convenient.

Another simple eavesdropping strategy is the so called beam splitting attack. Let us suppose that a coherent, weak source of photons, is used instead of a single photon source. Then, with a probability small but finite, the source can inject two (or more) photons. In BB84 schemes, the two photons contain the same information. Then, Eve can subtract one of them and, after the public discussion, perform the measurement selecting the right basis. In such a way she acquires the bit without introducing any kind of noise. Let us analyze what happens in our case, when, for

example, Alice injects two photons onto BS_a. The initial state is

$$|\phi\rangle = \frac{1}{2\sqrt{2}} \left(\left| 0_{a'_1} 2_{a'_2} \right\rangle + \left| 2_{a'_1} 0_{a'_2} \right\rangle + n \left| 1_{a'_1} 1_{a'_2} \right\rangle \right) \left(\left| 0_{b'_1} 1_{b'_2} \right\rangle + m \left| 1_{b'_1} 0_{b'_2} \right\rangle \right). \tag{5.8}$$

A simple observation to do is that Eve should be able to act on the state $\left(\left| 0_{a'_1} 2_{a'_2} \right\rangle + \left| 2_{a'_1} 0_{a'_2} \right\rangle + n \left| 1_{a'_1} 1_{a'_2} \right\rangle \right)$, with the idea of factorizing it in the tensor product $\left(\left| 0_{a'_1} 1_{a'_2} \right\rangle + n \left| 1_{a'_1} 0_{a'_2} \right\rangle \right) \left(\left| 0_{a'_1} 1_{a'_2} \right\rangle + n \left| 1_{a'_1} 0_{a'_2} \right\rangle \right)$, and to keep one copy. The global nonlocality and the inaccessibility of the mode a'_1 forbid this kind of eavesdropping strategy. Obviously, also the protocol fails due to the number of photons. What matters is that the security of the scheme is robust with respect to that situation.

Let us come back to analyze the differences between our proposal and the QKD realized by Degiovanni *et al.* [105]. In that case there is a time ordering between the encoding operations of sender and receiver: that is, Alice create a secrete state, Bob acts on that state, and then resends it to Alice. Therefore, an eavesdropper can extract some information by monitoring the state before and after Bob's action. In our case we assume that Alice and Bob perform all operations in coincidence. Therefore, all the information traveling on the public channel is not useful.

On the other hand, the presence of two senders and two receivers makes our scheme vulnerable versus a subtle strategy: Eve can short-circuit both Alice and Bob creating two Mach-Zehnder interferometers. In such a case the two speakers are separated and each single measurement result depends only, in a deterministic way, by the initial state created by the respective speaker. Thus, Eve has only to wait for the public communication to perfectly eavesdrop the bit without introducing noise. Against this kind of attack, we are helped by the control method introduced by Degiovanni *et al.*. Actually, checking the correlation between, for instance, the mode which Alice stores and the mode which she send to Bob, it is possible to reveal Eve's presence in 1/2 of cases.

The theoretical efficiency E of the scheme can be evaluated following the criteria

introduced in Ref. [110]:

$$E = \frac{b_s}{q_t + b_t}, \tag{5.9}$$

where q_t is the number of quantum bit exchanged, b_t is the number of classical bit exchanged, and b_s is the number of secret bits added to the key. In our case, considering the "single shot" efficiency, and the fact that both Bob and Alice add one bit, one finds $q_t = 2$, $b_t = 1$ and $b_s = 1$, from which follows $E = 1/3$. If the same criterion is applied to Ref. [98], avoiding the use of active switches, that are not suitable for long distance fiber communication, we get $E = 1/6$. In the case of BB84 protocols the maximum efficiency that can be reached is $E = 1/4$. Thus, our proposal seems to give some advantage. Actually, one should consider some unavoidable effect that could lower the practical efficiency of the scheme. For instance, our proposal requires the contemporary detection of two photons. Thus, the success probability scales with the square of detection efficiency, in contrast with the usual situation, where just one detection is needed.

5.3 Conclusions

To summarize, we have introduced a new method to create a random QKD based on a mechanism of bit exchange between sender and receiver. The secret is encoded in the phase of a single photon entangled state. Although the encoding is realized only through two orthogonal states, as in the Goldenberg-Vaidman protocol [111], quantum mechanics guarantees that no information is extracted acting just on a subsystem, and only the product between Alice's and Bob's states allows to extract the key element. The security of the scheme against simple eavesdropping techniques, as intercepting/resending strategy and beam splitting attack, has been analyzed. Finally, a comparison with other phase encoding based schemes has been performed, showing the advantages of our proposal if addressed to long distance

optical fiber transmission. The scheme is completely symmetric with respect to the role of Alice and Bob, and is suitable for information exchange in a sort of quantum dialogue. Probably, the main obstacle towards a possible realization of the proposed protocol is represented by the difficulty to achieve photon number resolution, which enhances the security of the protocol itself.

Summary and outlook

The contents of the present dissertation arise from my experience as a Ph. D. student, and embody many of the topics I encountered during last three years. Two main arguments have been the subject of my work: i) methods of statistical mechanics and many-body theory applied to quantum information processes (chapters 2 and 3); ii) theoretical design of all-optical quantum information schemes (chapters 4 and 5).

In chapter 1 I introduced some basic concepts (such as quantum teleportation) which appear a lot of times throughout the thesis, in order to simplify the development of the subsequent chapters.

The first chapter containing original result is chapter 2, where I developed a scheme to perform quantum teleportation through an array of double quantum dots [13, 14]. The interest of this protocol can be found considering that the robustness of the quantum channel with respect to the interaction with an external environment is enhanced as the channel length increases and the system experiences a phase transition, at least considering, for the bath, the zero temperature limit. The significance of this result originates from the fact decoherence represents the main obstacle towards the realization of a scalable quantum computer. It should be interesting to analyze finite temperature effects and to design a real experimental layout. I would cite that the experimental implementation of this teleportation protocol is the main subject of a research project submitted within the Sixth Framework Programme by

the group of I. Ostrovskii (Lviv University).

In chapter 3 I considered the problem of transferring quantum information inside a mesoscopic device from a more general point of view [42]. To this end I introduced a model of separated quantum systems coupled through the interaction with a chain that acts as a channel. The generality of this model is found in the fact that there are different physical systems which appear as possible candidates: quantum dots, Josephson junctions, nanoelectromechanical oscillators, optical cavities. It has been shown that, whenever the energy of the two system lies outside the spectrum of the chain, or whenever it matches with one of the eigenmodes of the channel (in this case the spectrum must be discrete), the systems, that can be far each other, undergo coherent Rabi-like oscillations. Furthermore, it has been shown that such structure is robust with respect to the presence of weak imperfections in the chain. Finally a finite temperature analysis has been performed for the case of quantum dots. It has been shown that coherent oscillations persist in the case of resonance within the discrete spectrum, and that when the energy of the two system lies outside the spectrum of the chain what matter is the ratio between this energy the Debye energy of the host material.

Chapter 4 opens the optical part of the thesis. I presented a scheme to realize a non-deterministic two-photon gate exploiting a modified version of the teleportation protocol [68]. This model falls inside the so-called linear optics quantum computation, introduced by Knill, Laflamme, and Milburn, who have shown that scalable networks of logic gates can be built using linear optics. The importance of the scheme presented here is due to the fact that it reaches the maximum of efficiency allowed by theory, and is suitable for experimental implementation, being strictly connected to teleportation protocols already realized. Recently, new approaches to linear optics quantum computation are emerging, considering the use of cluster states or linked states. The approach to teleportation presented here could be useful

also in these cases.

In chapter 5 I described an original scheme to realize a quantum cryptography protocol. Quantum cryptography is, beyond any doubt, the most advanced field of quantum information, having already achieved a commercial development. Despite the advances in this sector, long distance communication suffers various technical limits, such as birefringence effects in optical fibers. The aim of the protocol introduced in this thesis is to design a resilient scheme, being the information encoded in the phase of a quantum state, and being the efficiency higher than similar proposal. The originality of this scheme is based on the use of single-photon entanglement as a resource. I knew in a private communication with XianMin Jin, one of the members of the Quantum Physics and Information Laboratory, Department of Modern Physics, University of Science Technology of China, that they are working on the experimental realization of this QKD protocol.

For reasons that appear obvious, transferring photons in the space is easy, and thus they are natural candidates for the implementation of quantum communication protocols. In fact, many optical experimental implementation of quantum information protocols have been realized, such as teleportation, quantum cryptography, optimal quantum cloning, purification, dense coding. The state of the art is different when considering solid state devices. In this case the amount of interactions with the environment limits the feasibility of experiments. One of the motivations of this thesis is to suggest ways to make advances in this sector exploiting the knowledge of optical quantum information. In this sense, the scheme for a conditional gate proposed in the fourth chapter, being based on manipulations of number states, could be extended to the macroscopic qubit of double-quantum-dot pairs introduced in chapter 2, observing that the nearly degenerate ground state is used both for transferring information and performing the unitary rotation associated to a beam splitter, and that zero temperature decoherence decreases as the size increases.

There are some other arguments that I studied in this period. One of them, concerning quantum communication through a spin chain, has been presented in appendix B. Further, I would mention a teleportation protocol on a quantum-dot chain, which differentiates from that presented in chapter 2, published as a preprint [112]. That work has a starting point which is an oversimplification that weakens the content of the paper. I would mention also the attempt to study a quantum state transfer protocol through the use of the Jordan-Wigner transformations.

At the very end, I would repeat my acknowledgments towards Prof. F. de Pasquale and S. Paganelli. I worked in continuous contact with them day after day, and all the results presented in this dissertation are outgrowth of the common investigations.

Appendix A

In Sec. 3.3 we have introduced the kernel

$$\Lambda_d(\omega) = \frac{g^2}{N}\sum_k \frac{e^{ikd}}{\omega - \epsilon_k}, \tag{A-1}$$

stating that

$$\Lambda_d(\omega) = \frac{g^2}{(\omega^2-1)^{1/2}}\frac{K_d(\omega) + K_{N-d}(\omega)}{1 - K_N(\omega)}. \tag{A-2}$$

Here we give the explicit derivation. First of all, one can observe that the sum is realized on a symmetric range. Than $\Lambda_d(\omega) = \Lambda_{-d}(\omega)$. Let us write

$$\Lambda_d(\omega) = \frac{g^2}{N}\sum_k f_k(\omega), \tag{A-3}$$

where

$$f_k(\omega) = \frac{e^{ikd}}{\omega - \epsilon_k} \tag{A-4}$$

is a periodic function of k, which admits to be represented by means of its Fourier series

$$f_k(\omega) = \sum_{n=-\infty}^{\infty} f_n(\omega)\, e^{-ink}. \tag{A-5}$$

The coefficients are

$$f_n(\omega) = \frac{1}{2\pi}\int_0^{2\pi} f_k(\omega)\, e^{ink} dk \tag{A-6}$$

or

$$f_n(\omega) = \frac{1}{2\pi}\int_0^{2\pi} \frac{e^{ik(d+n)}}{\omega - \epsilon_k} dk. \tag{A-7}$$

Coming back to $\Lambda_d(\omega)$, we have

$$\Lambda_d(\omega) = g^2 \sum_{n=-\infty}^{\infty} \left(\frac{1}{N} \sum_{k=0}^{\frac{2\pi N}{(N-1)}} e^{-ink} \right) \frac{1}{2\pi} \int_0^{2\pi} \frac{e^{ik'(d+n)}}{\omega - \epsilon_{k'}} dk'. \tag{A-8}$$

Since

$$\frac{1}{N} \sum_{k=0}^{\frac{2\pi N}{(N-1)}} e^{-ink} = \sum_{l=-\infty}^{\infty} \delta_{n,Nl}, \tag{A-9}$$

the result is

$$\Lambda_d(\omega) = g^2 \sum_{l=-\infty}^{\infty} I_{d+Nl}(\omega), \tag{A-10}$$

where

$$I_{d+Nl}(\omega) = \frac{1}{2\pi} \int_0^{2\pi} \frac{e^{ik(d+Nl)}}{\omega - \epsilon_k} dk. \tag{A-11}$$

The sum is now divided separating the terms with $n > 0$ from those with $n < 0$:

$$\Lambda_d(\omega) = g^2 \sum_{l=-\infty}^{-1} I_{d+Nl}(\omega) + g^2 \sum_{l=0}^{\infty} I_{d+Nl}(\omega). \tag{A-12}$$

The first sum is manipulated by exchanging l with $-l$, and by exploiting the dependence on the absolute value of the argument:

$$\Lambda_d(\omega) = g^2 \sum_{l=1}^{\infty} I_{Nl-d}(\omega) + g^2 \sum_{l=0}^{\infty} I_{d+Nl}(\omega). \tag{A-13}$$

Again,

$$\Lambda_d(\omega) = g^2 \sum_{l=0}^{\infty} I_{Nl-d}(\omega) - g^2 I_{-d}(\omega) + g^2 \sum_{l=0}^{\infty} I_{d+Nl}(\omega). \tag{A-14}$$

The integral $I_r(\omega)$ is calculated in the complex space as follows. First of all, we change integration variable through the introduction of $z = e^{ik}$, which implies, assuming $\epsilon_k = -\cos k$,

$$I_r(\omega) = \frac{-i}{2\pi} \oint \frac{z^{r-1}}{\omega + \frac{1}{2}(z + z^{-1})} dz, \tag{A-15}$$

or

$$I_r(\omega) = \frac{-i}{\pi} \oint \frac{z^r}{z^2 + 2\omega z + 1} dz. \tag{A-16}$$

The poles are in

$$z_{\pm} = -\omega \pm \left(\omega^2 - 1\right)^{1/2}. \tag{A-17}$$

Let us consider the case $|\omega| > 1$. Being the integration area restricted to the unit circle about the origin, just the pole z_+ falls inside this region. This implies

$$I_r(\omega) = \frac{K_r(\omega)}{(\omega^2 - 1)^{1/2}}, \tag{A-18}$$

where $K_r(\omega) = [z_+(\omega)]^r$. The same result is obtained in the case $|\omega| < 1$, provided that ω has a non vanishing imaginary part. Then we have

$$\Lambda_d(\omega) = \frac{g^2}{(\omega^2 - 1)^{1/2}} \left\{ \sum_{l=0}^{\infty} \left[K_{Nl-d}(\omega) + K_{Nl+d}(\omega) \right] - K_{-d}(\omega) \right\}. \tag{A-19}$$

Since $|z_+(\omega)| < 1$, we can treat the sum as a geometric series, finally getting

$$\Lambda_d(\omega) = \frac{g^2}{(\omega^2 - 1)^{1/2}} \frac{K_d(\omega) + K_{N-d}(\omega)}{1 - K_N(\omega)}, \tag{A-20}$$

QED.

In the case of infinity of sites ($N \to \infty$), $K_N(\omega) = K_{N-d}(\omega) = 0$, and

$$\Lambda_d(\omega) = \frac{g^2}{(\omega^2 - 1)^{1/2}} K_d(\omega). \tag{A-21}$$

Appendix B

Transferring entanglement in a spin chain exploiting redundance

In this appendix I describe a work whose results have not been published. The physics I present has some interesting aspects, but the quality of the results is probably not high enough. Since a Ph. D. thesis should contain (almost) all the work carried out, I decided to propose this argument in a separate form.

I report a study about the possibility of encoding redundant entangled states to transfer them in a quantum chain described by a XY Hamiltonian (see Eq. (3.1)). Roughly speaking, we can think to create a tripartite W state, defined as

$$|W\rangle = \frac{1}{\sqrt{3}} \left(|\downarrow\uparrow\uparrow\rangle + |\uparrow\downarrow\uparrow\rangle + |\uparrow\uparrow\downarrow\rangle \right), \tag{B-1}$$

which evolves following the laws studied in Sec. 3.1, and to look for a bipartite entangled state in two sites different from those used for the encoding operation.

Labeling with l,m and n the encoding sites, the initial state is

$$|\Psi\left(t=0\right)\rangle = \frac{1}{\sqrt{3}} \left(|\downarrow\uparrow\uparrow\rangle + |\uparrow\downarrow\uparrow\rangle + |\uparrow\uparrow\downarrow\rangle \right)_{l,m,n} |\uparrow\uparrow \ldots \uparrow\uparrow\rangle \equiv \frac{1}{\sqrt{3}} \left(|l\rangle + |m\rangle + |n\rangle \right), \tag{B-2}$$

or, in terms of modes, defined in Eq. (3.5),

$$|\Psi\left(t=0\right)\rangle = \frac{1}{\sqrt{3}} \frac{1}{\sqrt{N}} \sum_{q} \left(e^{iql} + e^{iqm} + e^{iqn} \right) |q\rangle . \tag{B-3}$$

Then, defining $\epsilon_q = -2w\cos q$, the time evolution is given as

$$|\Psi(t)\rangle = \frac{1}{\sqrt{3}}\frac{1}{\sqrt{N}}\sum_q \left(e^{iql} + e^{iqm} + e^{iqn}\right) e^{i\epsilon_q t}\,|q\rangle\,, \tag{B-4}$$

which can be rewritten in terms of sites

$$|\Psi(t)\rangle = \frac{1}{\sqrt{3}}\frac{1}{N}\sum_{q,r} \left(e^{iq(l-r)} + e^{iq(m-r)} + e^{iq(n-r)}\right) e^{i\epsilon_q t}\,|r\rangle\,. \tag{B-5}$$

Assuming $N \to \infty$, this state is given in terms of Bessel function:

$$|\Psi(t)\rangle = \frac{1}{\sqrt{3}}\sum_r \left(e^{i\frac{\pi}{2}(l-r)}J_{l-r}(2wt) + e^{i\frac{\pi}{2}(m-r)}J_{m-r}(2wt) + e^{i\frac{\pi}{2}(n-r)}J_{n-r}(2wt)\right)|r\rangle\,. \tag{B-6}$$

At this stage, the calculus of the reduced density matrix is easy. Various quantities can be analyzed. As a first question, one can analyze how much rapidly the state diffuses from the sites l,m and n, and compare this result with degradation of a Bell (bipartite) entangled state. In Fig. B1 we plot the Fidelity (defined in Sec. 3.1) both for W states and for Bell state, observing that W states are more resilient.

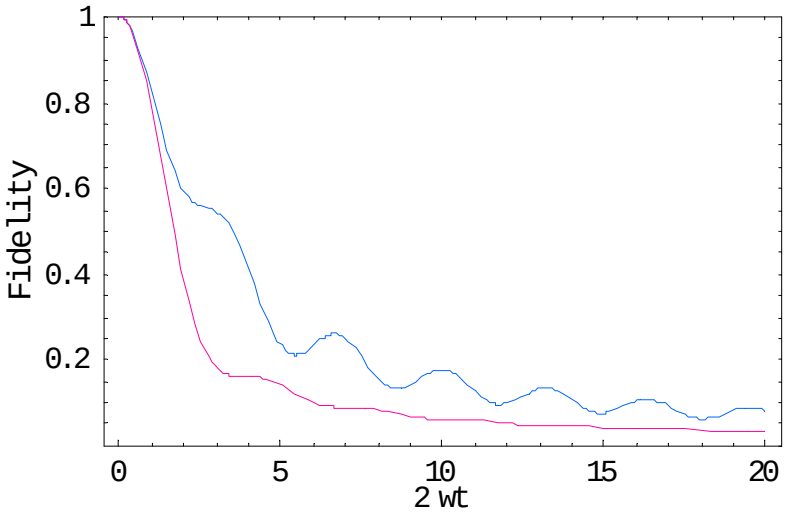

Figure B-1. Time evolution for the fidelity of W state (blue line) and Bell state (red line). The concurrence is measured on the encoding sites in both cases.

Next, we can observe the same quantities on sites which are separated from the initial ones. In Fig. B2 we measured the fidelity at distance $n = 4$ from the encoding sites. Now we start from zero both for W states and Bell states. The maximum value reached is about the same for all the states, but W states seem to preserve their entanglement for a much long time.

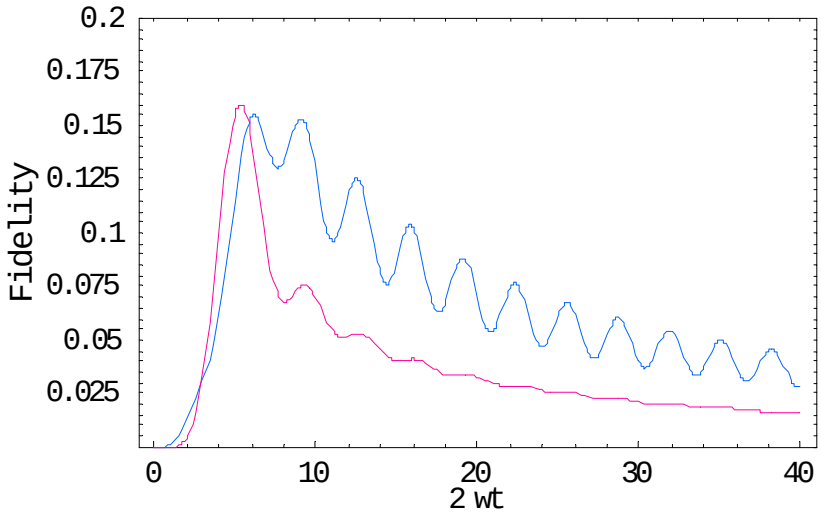

Figure B-2. Time evolution for the fidelity of W state (blue line) and Bell state (red line) measured at a distance of 4 sites from the origin.

Starting from W states, one can observe also bipartite entanglement evolving in the chain (tracing out all the sites but 2), and compare this degree of entanglement with that obtained starting from Bell states. In Fig. B3 we show the concurrence obtained considering the evolution of a W state, from the sites 0,1,2 sites 4,5, and compare it with the concurrence measured on the sites 4,5 derived from a Bell state on the sites 0,1. In this case the advantage deriving from a redundant encoding appears very small.

This kind of work could be extended considering M-partite W states. Traces of enhancement appear, but the difficulty of controlling a higher number of encoding sites balances negatively these (weak) advantages.

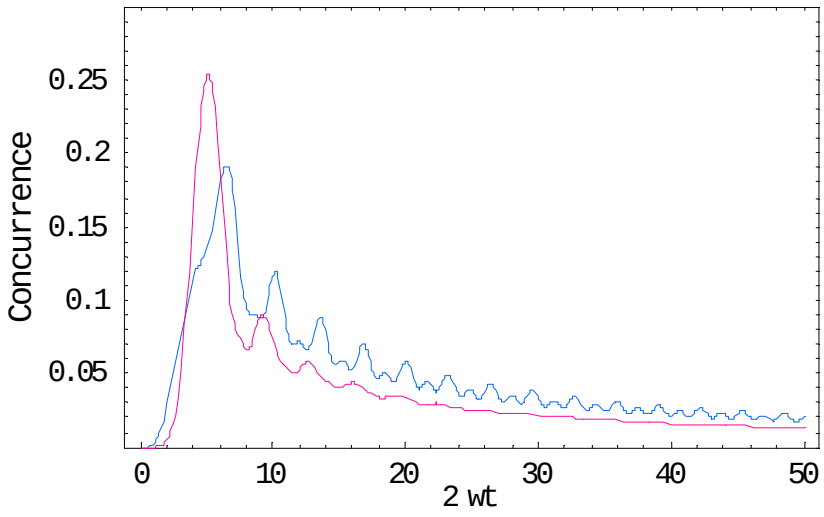

Figure B-3. Time evolution for the concurrence of W state (blue line) and Bell state (red line) measured at a distance of 4 sites from the origin.

Bibliography

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2000).

[2] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982); Found. Phys, **16**, 507 (1986).

[3] P. W. Shor, SIAM J. Comp **26**, 1984 (1997).

[4] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[5] D. P. DiVincenzo, Fort. Phys. **48**, 771 (2000).

[6] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[7] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[8] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[10] W. H. Zurek, Rev. Mod. Phys. **75** 715 (2003).

[11] D. Giulini, E. Joos, C. Kiefer, J. Kupsch, I. O. Stamatescu and H. D. Zeh *Decoherence and the appearence of a Classical World in Quantum Theory* (Springer, Berlin) (1996).

[12] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[13] F. de Pasquale, G. Giorgi, and S. Paganelli, Phys. Rev. A **71**, 042304 (2005).

[14] F. de Pasquale, G. Giorgi, and S. Paganelli, Phys. Rev. Lett. **93**, 120502 (2005).

[15] S. Tarucha, D. G. Austing, T. Honda, R. J. van der Hage, and L. P. Kouwenhoven, Phys. Rev. Lett. **77**, 3613 (1996).

[16] T. H. Oosterkamp, T. Fujisawa, W. G. Van Der Wiel, K. Ishibashi, R. V. Hijman, S. Tarucha, and L. P. Kouwenhoven, Nature (London) **395**, 873 (1998).

[17] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).

[18] T. Hayashi, T. Fujisawa, H. D. Cheong, Y. H. Jeong, and Y. Hirayama, Phys. Rev. Lett. **91**, 226804 (2003).

[19] J. R. Petta, A. C. Johnson, C. M. Marcus, M. P. Hanson, A. C. Gossard, Phys. Rev. Lett. **93**, 186802 (2004).

[20] E. Lieb, T. Schultz and D. Mattis, Ann. Phys. (N.Y.) **16**, 407 (1961).

[21] P. Pfeuty, Ann. Phys (N.Y.) **57**, 79 (1970).

[22] S. Sachdev, *Quantum Phase Transitions*, Cambridge University Press, Cambridge (1999).

[23] S. Fujita, *Introduction to Non-Equilibrium Statistical Mechanics* (Saunders, Philadelphia, 1968).

[24] T. Brandes and T. Vorrath, Phys. Rev. B **66**, 075341 (2002).

[25] L. Fedichkin and A. Fedorov, Phys. Rev. A **69** 032311 (2004).

[26] A. J. Leggett, S. Chakravarty, A. T. Dorsey, M. P. A. Fisher, A. Garg, and W. Zwerger, Rev. Mod. Phys. **59**, 1 (1987).

[27] A. M. Childs, E. Farhi and J. Preskill, Phys. Rev. A **65**, 012322 (2002).

[28] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[29] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).

[30] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).

[31] M. A. Nielsen, E. Knill and R. Laflamme, Nature (London) **396**, 52 (1998).

[32] M. Riebe et al., Nature (London) **429**, 734 (2004).

[33] D. Barrett, et al. Nature (London) **429**, 737 (2004).

[34] J. H. Reina and N. F. Johnson, Phys. Rev. A **63**, 012303 (2001).

[35] O. Sauret, D. Feinberg and T. Martin, Eur. Phys. J. B **32**, 545 (2003); ibid., Phys. Rev. B **69**, 035332 (2004).

[36] A. Messiah, *Quantum Mechanics, Vol II* (North-Holand, Amsterdam, 1961).

[37] A. M. Childs et al., Phys. Rev. A **66**, 032314 (2002).

[38] G.Brassard, S. L. Braunstein, and R. Cleve, Physica D, **120**, 43 (1998).

[39] E. DelRe, B. Crosignani, and P. Di Porto, Phys. Rev. Lett. **84**, 2989 (2000).

[40] L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999).

[41] N. Lutkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[42] F. de Pasquale, G. Giorgi, and S. Paganelli, quant-ph/0505097.

[43] S. Bose, Phys. Rev. Lett. **91**, 207901 (2003).

[44] T. J. Osborne and N. Linden, Phys. Rev. A **69**, 052315 (2004).

[45] S. M. Giampaolo, F. Illuminati, A. Di Lisi, and S. De Siena, quant-ph/0503107.

[46] V. Subrahmanyam, Phys. Rev. A **69**, 034304 (2004).

[47] A. Romito, R. Fazio, and C. Bruder, Phys. Rev. B **71**, 100501(R) (2005).

[48] J. Preskill, http://www.theory.caltech.edu/people/preskill/ph229/.

[49] J. Eisert, M. B. Plenio, S. Bose, and J. Hartley, Phys. Rev. Lett. **93**, 190402 (2004).

[50] D. Burgarth and S. Bose, Phys. Rev. A **71**, 052315 (2005).

[51] M. Christandl, N. Datta, A. Ekert and A. J. Landahl, Phys. Rev. Lett. **92**, 187902 (2004).

[52] M. Christandl, N. Datta, T. C. Dorlas, A.Ekert, A. Kay, and A. J. Landahl, Phys. Rev. A **71**, 032312 (2005).

[53] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997).

[54] M. B Plenio and F. L Semião, New J. Phys. **7**,73 (2005).

[55] A. Wojcik, T. Luczak, P. Kurzynski, A. Grudka, T. Gdala, M. Bednarska, Phys. Rev. A **72**, 034303 (2005).

[56] U. Fano, Nuovo Cimento **12**, 156 (1935).

[57] U. Fano, Phys. Rev. **124**, 1866 (1961).

[58] P. W. Anderson, Phys. Rev. **109**, 1492 (1958).

[59] P. W. Anderson, Phys. Rev. **124**, 41 (1961).

[60] T.M. Stace, C. H.W. Barnes, and G. J. Milburn, Phys. Rev. Lett. **93**, 126804 (2004).

[61] N. C. van der Vaart, M. P. de Ruyter van Steveninck, L. P. Kouwenhoven, A. T. Johnson, Y. V. Nazarov, and C. J. P. M. Harmans, Phys. Rev. Lett. **73**, 320 (1994).

[62] G. Kirczenow, A. S. Sachrajda, Y. Feng, R. P. Taylor, L. Henning, J. Wang, P. Zawadzki, and P. T. Coleridge, Phys. Rev. Lett. **72**, 2069 (1994).

[63] A. Wallraff, D. I. Schuster, A. Blais, L. Frunzio, R.- S. Huang, J. Majer, S. Kumar, S. M. Girvin, R. J. Schoelkopf, Nature (London) **431**, 162 (2004).

[64] B. Kramer and A. MacKinnon, Rep. Prog. Phys. **56**, 1469 (1993).

[65] X. Hu, B. Koiller, and S. D. Sarma, Phys. Rev. B **71**, 235332 (2005).

[66] G.D. Mahan, *Many-Particle Physics* (Plenum, New York, 1981).

[67] S. R. Schofield, N. J. Curson, M. Y. Simmons, F. J. Rueß, T. Hallam, L. Oberbeck, and R. G. Clark, Phys. Rev. Lett. **91**, 136104 (2003).

[68] G. Giorgi, F. de Pasquale, and S. Paganelli, Phys. Rev. A **70**, 022319 (2004).

[69] Y. Nakamura, Y. Pashkin and J. S.Tsai, Nature (London) **398**, 786 (1999).

[70] L. Vandersypen, M. Steffen, G. Breyta, C. Yannoni, R. Cleve and I. L. Chuang, Nature (London) **414**, 883 (2001).

[71] C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175-179.

[72] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[73] E. Knill, R. Laflamme and G.J. Milburn, Nature (London) **409**, 46 (2001).

[74] G. Giorgi, P. Mataloni and F. De Martini, Phys. Rev. Lett. **90**, 027902 (2003).

[75] I. L. Chuang and Y. Yamamoto, Phys. Rev. Lett. **76**, 4281 (1996).

[76] E. Lombardi, F. Sciarrino, S. Popescu, and F. De Martini, *Phys. Rev. Lett.* **88**, 070402 (2002).

[77] Ralph, White, Munro, Milburn, *Phys. Rev. A* **65**, 012314 (2001).

[78] T.B. Pittman, B.C. Jacobs and J.D. Franson, *Phys. Rev. A* **66**, 052305 (2002).

[79] T.B. Pittman, M.J. Fitch, B.C. Jacobs and J.D. Franson, quant-ph/0303095 (2003).

[80] T.B. Pittman, B.C. Jacobs, and J.D. Franson, *Phys. Rev. A* **64**, 062311 (2001).

[81] D Gottesman, I. L. Chuang, *Nature* **402**, 390(1999).

[82] S. Giacomini, F. Sciarrino, E. Lombardi and F. De Martini, *Phys. Rev. A* **66**, 030302 (R) (2002).

[83] F. Sciarrino, E. Lombardi, G. Milani, and F. De Martini, *Phys. Rev. A* **66**, 024309 (2002).

[84] W.K. Wooters and W.H. Zurek, Nature (London) **299**, 802 (1982).

[85] T. B. Pittman, B. C. Jacobs and J. D. Franson, Phys. Rev. A **69**, 042306 (2004).

[86] D. Fattal, E. Diamanti, K. Inoue, and Y. Yamamoto, Phys. Rev. Lett. **92**, 037904 (2004).

[87] G. Giorgi, Phys. Rev. A **71**, 064303 (2005).

[88] S. Wiesner, "Conjugate Coding", manuscript 1970 ca; subsequently published in SIGACT NEWS 15:1, 78 (1983).

[89] H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).

[90] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145-195 (2002).

[91] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[92] D. Deutsch, Proc. R. Soc. Lond. A **420**, 97 (1985).

[93] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, (Cambridge University Press, Cambridge, 1987).

[94] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[95] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).

[96] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).

[97] R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47**, 533 (2000).

[98] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).

[99] J.-W. Lee, E. K. Lee, Y. W. Chung, H.-W. Lee, and J. Kim, Phys Rev. A **68**, 012324 (2003).

[100] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, Phys. Rev. Lett. **86**, 1502 (2001).

[101] J. McKeever, A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich, and H. J. Kimble, Science **303**, 1992 (2004).

[102] J. W. Pan, D. Bouwmeester, H.Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[103] A. Cabello, Phys Rev. A **61**, 052312 (2000).

[104] D. Song, Phys Rev. A **69**, 034301 (2004).

[105] I. P. Degiovanni, I. R. Berchera, S. Castelletto, M. L. Rastello, F. A. Bovino, A. M. Colla, and G. Castagnoli, Phys. Rev. A **69**, 032310 (2004).

[106] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).

[107] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[108] J. Řeháček, Z. Hradil, O. Haderka, J. Peřina, Jr., and M. Hamar, Phys. Rev. A **67**, 061801(R) (2003).

[109] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, Phys. Rev. A **68**, 043814 (2003).

[110] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).

[111] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).

[112] F. de Pasquale, G. Giorgi, and S. Paganelli, cond-mat/0407152.