UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

Quantum walks in cryptography and finite-temperature topological phase transitions

Chrysoula Vlachou

Supervisor: Doctor Paulo Alexandre Carreira Mateus
Co-Supervisor: Doctor Nikola Paunković

Thesis approved in public session to obtain the PhD Degree
Physics

Jury final classification: Pass with Distinction

2018

TÉCNICO LISBOA

UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

Quantum walks in cryptography and finite-temperature topological phase transitions

Chrysoula Vlachou

Supervisor: Doctor Paulo Alexandre Carreira Mateus
Co-Supervisor: Doctor Nikola Paunković

Thesis approved in public session to obtain the PhD Degree in Physics

Jury final classification: Pass with Distinction

Jury

Chairperson: Doctor José Luís Rodrigues Júlio Martins, Instituto Superior Técnico da Universidade de Lisboa

Members of the Comittee:

Doctor Armando Humberto Moreira Nolasco Pinto, Universidade de Aveiro

Doctor Pedro Domingos Santos do Sacramento, Instituto Superior Técnico da Universidade de Lisboa

Doctor Miguel António da Nova Araújo, Escola de Ciências e Tecnologia da Universidade de Évora

Doctor Nikola Paunković, Instituto de Telecomunicações, Lisboa

Funding Institution: Fundação para a Ciência e a Tecnologia (FCT)

2018

Abstract

Quantum cryptography is a field of study that utilizes the properties of quantum physics to develop cryptographic primitives that are beyond the reach of classical cryptography. Its main objective is to improve existing classical implementations and to introduce new cryptographic methods that can withstand the power of quantum computers. While much of the research in this field has focused on quantum key distribution (QKD), there have been important advances in the understanding and development of other two-party primitives such as quantum oblivious transfer (QOT). QOT protocols, having a similar structure to QKD protocols, allow for quantum-safe computation. However, the conditions under which QOT is fully quantum-safe are still under intense scrutiny. The thesis begins by surveying the work done on the concept of oblivious transfer within theoretical quantum cryptography, highlighting proposed protocols and their security requirements, discussing impossibility results, and examining quantum security models in which QOT security can be proven.

The most significant application of oblivious transfer (OT) is in the realm of secure multiparty computation (SMC). This technology has the potential to revolutionize fields such as data analysis and computation by enabling multiple parties to compute virtually any function while maintaining the privacy of their inputs. However, the security and efficiency of SMC protocols are heavily dependent on the security and efficiency of OT. To address this, the thesis conducts a detailed comparison of the complexity of quantum oblivious transfer based on oblivious keys and two of the fastest classical OT protocols. This comparison provides insight into the potential benefits and limitations of using quantum techniques in SMC.

Building on the theoretical comparison of quantum and classical approaches to oblivious transfer, the thesis integrates and compares both within an SMC system for genomic analysis. The proposed system utilizes quantum cryptographic protocols to compute a phylogenetic tree from a set of private genome sequences. This system significantly improves the privacy and security of the computation by incorporating three quantum cryptographic protocols that provide enhanced security against quantum computer attacks. The system adapts several distance-based methods, such as the Unweighted Pair

Group Method with Arithmetic mean (UPGMA), Neighbour-Joining (NJ), and Fitch-Margoliash (FM), into a private setting where the sequences owned by each party are not disclosed to other members. The performance and privacy guarantees of the system are evaluated theoretically through a complexity analysis and a security proof. Additionally, the thesis provides an extensive explanation of the implementation details and cryptographic protocols used. The implementation of quantum-assisted secure phylogenetic tree computation is based on the Libscapi implementation of the Yao protocol, the PHYLIP library, and simulated keys of two quantum systems: quantum oblivious key distribution and quantum key distribution. The implementation is benchmarked against a classical-only solution, and the results indicate that both approaches have similar execution times, with the only difference being the time overhead taken by the oblivious key management system of the quantum-assisted approach.

Finally, the thesis presents the first quantum protocol for oblivious linear evaluation. Oblivious linear evaluation is a generalization of oblivious transfer, where two distrustful parties, Alice and Bob, obliviously compute a linear function, $f(x) = ax + b$, without revealing their inputs to each other. Alice inputs the function coefficients, a and b, and Bob inputs the function input, x. The output, $f(x)$, is only delivered by Bob. This primitive is essential for arithmetic-based secure multiparty computation protocols from a structural and security point of view. In the classical setting, it is known that oblivious linear evaluation can be generated based on oblivious transfer, and quantum counterparts of these protocols can, in principle, be constructed as straightforward extensions based on quantum oblivious transfer. However, the thesis presents a novel quantum protocol for oblivious linear evaluation that does not rely on quantum oblivious transfer. The protocol is first presented for the semi-honest setting and then extended to the dishonest setting using a commit-and-open strategy. The protocol uses high-dimensional quantum states to compute the linear function obliviously, $f(x)$, on Galois fields of prime dimension, $GF(d) \cong \mathbb{Z}_d$, or prime-power dimension, $GF(d^M)$. The protocol utilizes a complete set of mutually unbiased bases in prime-power dimension Hilbert spaces and their linear behavior upon the Heisenberg-Weyl operators. The protocol is also generalized to achieve vector oblivious linear evaluation, which increases efficiency by generating several instances of oblivious linear evaluation. The security of the protocol is proven in the framework of quantum universal composability.

Key-words: quantum cryptography, quantum oblivious transfer, quantum oblivious linear evaluation, secure multiparty computation, UC security.

Resumo

A criptografia quântica é o campo da criptografia que explora as propriedades quânticas da matéria. Geralmente, visa desenvolver primitivas fora do alcance da criptografia clássica e melhorar as implementações clássicas existentes. Embora grande parte do trabalho neste campo se foque na distribuição de chaves quânticas (*quantum key distribution*, QKD), também têm existido desenvolvimentos cruciais para a compreensão e desenvolvimento de outras primitivas criptográficas, como a transferência oblívia quântica (*quantum oblivious transfer*, QOT). Pode-se mostrar a semelhança entre a estrutura de aplicação das primitivas QKD e QOT. Assim como os protocolos QKD permitem comunicação com segurança quântica, os protocolos QOT permitem computação com segurança quântica. No entanto, as condições sobre as quais o QOT é totalmente seguro têm sido sujeitas a um intenso estudo. Nesta tese, começamos por fazer um levantamento do trabalho desenvolvido em torno do conceito de OT dentro da criptografia quântica teórica. Aqui concentramo-nos em alguns protocolos propostos e nos seus requisitos de segurança. Revisitamos os resultados de impossibilidade desta primitiva e discutimos vários modelos quânticos de segurança sob os quais é possível provar a segurança do QOT.

A aplicação mais famosa do OT está no domínio da computação multipartidária segura (*secure multiparty computation*, SMC). Esta tecnologia tem o potencial de ser disruptiva nas áreas de análise e computação de dados. Esta permite que vários participantes calculem um certa função, preservando a privacidade dos seus dados. No entanto, a maior parte da segurança e eficiência dos protocolos SMC dependem da segurança e eficiência do OT. Por esta razão, fazemos uma comparação detalhada entre a complexidade da QOT baseada em chaves oblívias e dois dos protocolos OT clássicos mais rápidos.

Seguindo a comparação teórica entre OT quântico e clássico, integramos e comparamos ambas as abordagens dentro de um sistema SMC baseado na análise de sequências genéticas. Em resumo, propomos um sistema SMC auxiliado por protocolos criptográficos quânticos com o objectivo de computar uma árvore filogenética a partir de um conjunto de sequências genéticas privadas. Este sistema melhora significativamente a privacidade e a segurança da computação graças a três protocolos criptográficos quânticos que fornecem segurança aprimorada contra ataques de computadores quânticos. Este sistema adapta

vários métodos baseados em distância (Unweighted Pair Group Method with Arithmetic mean, Neighbour-Joining, Fitch-Margoliash) num ambiente privado onde as sequências de cada participante não são divulgadas aos demais membros presentes no protocolo. Avaliamos teoricamente as garantias de desempenho e privacidade do sistema através de uma análise de complexidade e prova de segurança, e fornecemos uma extensa explicação dos detalhes de implementação e protocolos criptográficos. Implementamos este sistema com base na implementação Libscapi do protocolo de Yao, na biblioteca PHYLIP e em chaves simuladas de dois sistemas quânticos: distribuição de chaves oblívias quânticas e distribuição de chaves quânticas. Comparamos esta implementação com uma solução somente clássica e concluímos que ambas as abordagens apresentam tempos de execução semelhantes. A única diferença entre os dois sistemas é a sobrecarga de tempo tomada pelo sistema de gestão de chaves oblívias da abordagem quântica.

Finalmente, apresentamos o primeiro protocolo quântico de avaliação linear oblívia (*oblivious linear evaluation*, OLE). O OLE é uma generalização do OT, em que dois participantes calculam de forma oblívia uma função linear, $f(x) = ax + b$. Ou seja, cada participante fornece os seus dados de forma privada, a fim de calcular o resultado $f(x)$ que se torna conhecido por apenas um deles. Do ponto de vista estrutural e de segurança, o OLE é fundamental para protocolos SMC baseados em circuitos aritméticos. No caso clássico, sabe-se que o OLE pode ser gerado com base no OT, e as contrapartes quânticas desses protocolos podem, em princípio, ser construídas como extensões directas baseadas em QOT. Aqui, apresentamos o primeiro, protocolo quântico OLE que não depende de QOT. Começamos apresentando um protocolo semi-honesto e depois estendemo-lo para o cenário desonesto através de uma estratégia *commit-and-open*. O nosso protocolo usa estados quânticos para calcular a função linear, $f(x)$, em corpos de Galois de dimensão prima, $GF(d) \cong \mathbb{Z}_d$, ou dimensão de potência prima, $GF(d^M)$. Estas construções utilizam a existência de um conjunto completo de *mutually unbiased bases* em espaços de Hilbert de dimensão de potência prima e o seu comportamento linear sobre os operadores de Heisenberg-Weyl. Também generalizamos o nosso protocolo para obter uma versão vectorial do OLE, onde são geradas várias instâncias de OLE, tornando o protocolo mais eficiente. Provamos que os protocolos têm segurança estática no âmbito da composição universal quântica.

Palavras-chave: criptografia quântica, transferência oblívia quântica, avaliação linear oblívia quântica, computação multipartidária segura, segurança UC.

Acknowledgments

I am deeply grateful to my advisors, Paulo Mateus and Armando Nolasco Pinto, for their guidance and support throughout the course of this research. Their expertise and insight have been invaluable in shaping the direction and outcome of this thesis.

I am also grateful for the valuable contributions of my colleagues, who have provided me with valuable insights and knowledge throughout this research. Special recognition goes to Chrysoula Vlachou for her stimulating discussions and Pedro Branco for his expertise on the UC framework and other crypto-related topics. Their guidance and support have been instrumental in shaping this research and making this journey a success.

I would like to extend my appreciation to my friends Francisco Gomes, Gonçalo Santos, José Reis and Tomás Lobão, who have been a constant source of support and encouragement throughout my research journey. As the Latin saying goes, "Veræ amicitiæ sempiternæ sunt" (Cicero, "De Amicitia"). I also want to express my deep gratitude to my family, particularly my wife Teresinha and my children Henrique and Helena, for their unwavering love and support. This thesis is dedicated to them.

I acknowledge Fundação para a Ciência e a Tecnologia (FCT, Portugal) for its support through the PhD grant SFRH/BD/144806/2019 in the context of the Doctoral Program in the Information Security (IS). I also acknowledge support from the project QuantaGenomics funded within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101017733, and with funding organisations, The Foundation for Science and Technology – FCT (QuantERA/0001/2021), Agence Nationale de la Recherche - ANR, and State Research Agency – AEI; and in part by AIT—Austrian Institute of Technology GmbH and 37 Further Beneficiaries of OpenQKD (Project number 857156, Action QuGenome).

Contents

List of Figures

List of Tables

List of Abbreviations

AES – Advanced encryption standard.

ALSZ13 – OT extension protocol developed by Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner [**?**].

API – Application programming interface.

BB84 – Quantum key distribution protocol developed by Charles Bennet and Gilles Brassard in 1984 [**?**].

BBCS – Quantum oblivious transfer protocol developed by Bennet, Brassard, Crépeau and Skubiszewska [**?**].

BCJL – Quantum bit commitment protocol developed by Brassard, Crépeau, Jozsa and Langlois [**?**].

BGW – Secure multiparty computation protocol developed by Ben-Or, Goldwasser and Wigderson [**?**].

BM – Oblivious transfer protocol developed by Bellare and Micali [**?**].

BMR – Secure multiparty computation protocol developed by Beaver, Micali and Rogaway [**?**].

BQS – Bounded-quantum-storage model.

BQS-UC – Bounded-quantum-storage universal composability model.

CBMC-GC – C Bounded model checker - Garbled Circuit.

CCD – Secure multiparty computation protocol developed by Chaum, Crépeau and Damgárd [**?**].

COM – Commitment.

CP – Completely positive map.

CPTP – Completely positive trace preserving map.

CPU – Central processing unit.

CRS – Common reference string.

CSRNG – Cryptographically secure pseudorandom number generator.

DI – Device independent.

EGL – Even, Goldreich, Lempel.

F84 – Evolutionary distance developed by Felsenstein.

FSA – Faked-state attacks.

GDPR – General data protection regulation.

GISAID – Global initiative on sharing avian influenza data.

GMW – Secure multiparty computation protocol developed by Goldreich, Micali and Wigderson [**?**].

GWAS – Genome-wide association studies.

HyCC – Compilation of hybrid protocols developed in [**?**].

JC – Jukes-Cantor.

K2P – Kimura 2-parameter.

KOS15 – OT extension protocol developed by Keller, Orsini and Scholl [**?**].

LAN – Local area network.

LD – LogDet.

LWE – Learning with errors.

M-LWE – Module learning with errors.

MDI – Measurement device independent.

MMH – Multi-linear modular hashing.

MUB – Mutually unbiased bases.

NP – Oblivious transfer protocol developed by Naor and Pinkas [**?**].

NQS – Noisy quantum storage model.

NTRU – Number theory research unit.

OKM – Oblivious key management system.

OLE – Oblivious linear evaluation.

OT – Oblivious transfer.

PDQ – Private database queries.

PET – Privacy-enhancing technologies.

PHYLIP – Phylogeny inference package.

POVM – Positive operator-valued measure.

PRG – Pseudorandom generator.

QBC – Quantum bit commitment.

QKD – Quantum key distribution.

QOKD – Quantum oblivious key distribution.

QOLE – Quantum oblivious linear evaluation.

QOT – Quantum oblivious transfer.

QRNG – Quantum random number generator.

quantum-UC – Quantum universal composability model.

RNG – Random number generator.

RSA – Public-key cryptosystem developed by Rivest, Shamir and Adleman [**?**].

RWOLE – Random weak oblivious linear evaluation.

SARS-CoV-2 – Severe acute respiratory syndrome coronavirus 2.

SHA – Secure hash algorithm.

SMC – Secure multiparty computation.

THA – Trojan-horse attack.

UC – Universal composability model.

UPGMA – Unweighted pair group method with arithmetic mean.

VM – Virtual machine.

VOLE – Vector oblivious linear evaluation.

WOLE – Weak oblivious linear evaluation.

WSE – Weak string erasure.

Chapter 1

Introduction

1.1 Motivation

Since the invention of writing, the need for secret communication resulted in the development of cryptography – the art of "hidden communication". It started by using simple symbols as code words and evolved to the stage where the security is based on various mathematical hardness assumptions: the widely used RSA-based cryptographic system[**?**] relies on the conjecture that factoring large numbers is not feasible using standard computers, while the alternative lattice-based public-key cryptographic system[**?**] is based on the assumed difficulty of the so-called "shortest and closest vector problems" (also related to the well known $P \neq NP$ conjecture[**?**]). With the advent of quantum computation, and in particular after the discovery of the celebrated Shor's algorithm for the efficient factoring of prime numbers[**?**], the security of numerous cryptographic systems currently in use became jeopardised, and as a consequence the need for new cryptographic systems resilient to quantum adversaries arose. The above mentioned lattice-based cryptographic system is resilient to quantum adversaries that execute Shor's algorithm, as its security is not based on the factoring problem; nevertheless, it does rely on another mathematical assumption, thus it is just computationally secure. In this context, the idea of quantum cryptography was born. The security of the communication, rather than relying on mathematical/ computational hardness assumptions, is now based on the laws of quantum mechanics, i.e, quantum cryptographic protocols are unconditionally secure (information-theoretic security). The only classical encryption scheme which is known to be unconditionally secure is the one-time pad, however the key management is a very hard task. The major advantage of quantum cryptography is that it is not only unconditionally secure, but also the key management is easy. Quantum cryptography was first considered by Wiesner in the late sixties and early seventies, who introduced the notions of quantum multiplexing and money (this work, though, was only published a decade later

in 1983 [**?**]), and further developed in 1984 by Bennet and Brassard [**?**] in their famous Quantum Key Distribution (QKD) BB84 protocol. Subsequently, Shor and Preskill [**?**] and independently Mayers [**?**] showed that the BB84 protocol is unconditionally secure. Since then, quantum cryptography has been among the hottest subjects of research and the intense investigation has yielded so far impressive results. Several QKD experiments over long distances have been reported [**?** **?** **?** **?** **?**], and QKD is already commercial.[1] Furthermore, the recent successful launch of a satellite [**?**] paved the way for intercontinental QKD [**?**].

In the first part of this thesis (Chapters 2 and 3), we present our work on quantum cryptography. In particular, we propose a new secure quantum public-key cryptosystem, as an alternative to the currently used classical public-key cryptosystems, whose security can be seriously compromised by adversaries with potential access to a quantum computer. Moreover, we design three novel QKD protocols and study their security properties. This way, we stay in tune with the current advances in QKD, which is widely considered as the most secure and practical instance of quantum cryptography, so far.

The cryptographic protocols that we propose (public-key cryptosystem and key distribution) have a common feature. They are all based on quantum walks (QWs), the quantum counterpart of classical random walks. A classical random walk describes the behaviour of a "walker" over a path who, at each step, can choose to follow one of the possible directions with a certain *a priori* fixed probability. It was shown to be very useful in computer science (sampling massive online graphs, image segmentation, estimating the size of the World Wide Web, wireless networking, etc.), physics (modelling the Brownian motion, studying polymers, etc.), and many other fields of research (financial economics, medicine and biology, psychology, etc.). One may study several properties of classical random walks, such as the probability of returning to the original position after a certain number of steps, the characteristics of the probability distribution of the positions at each step, etc...

QWs were introduced in 1993 [**?**], as the quantum analogue of classical random walks and since then, they have been playing a prominent role in quantum computation. Unlike the classical case, in which the state of the walker is described by a probability distribution over the allowed positions, in the quantum scenario the state of the walker is given by a superposition of positions. One can study different types of QWs, determined by their time evolution (discrete- vs continuous-time) and the topology of the underlying positions space (walks on the line, lattice, circle, graphs, etc.). They are a very successful tool in algorithmic theory, since they provide polynomial and exponential speedups over classical

[1]Currently there are three companies offering commercial QKD systems: ID Quantique (Geneva), MagiQ Technologies, Inc. (New York) and QuintessenceLabs (Australia).

computations for several problems [? ? ? ?]. They have also been proven to be very useful in search problems [? ? ? ?]. Moreover, they are an important computational primitive, since they permit universal quantum computation [? ? ?].

Recently, the use of QWs for cryptographic purposes has been also suggested. For instance, in [?], Rohde *et al.*, proposed a limited form of quantum homomorphic encryption using multi-particle QWs. In their protocol, a server could manipulate data sent by a client in such a way that the server has limited information on the client's data, while the client has limited information on the server's computation. Also, Yan *et al* presented a new method to generate keys for image encryption using QWs [?]. To the best of our knowledge, our work is the first attempt to use QWs for the encryption of messages and key distribution and perhaps its most important contribution is that it introduces this exciting possibility, which may spur new research in both cryptography and the study of QWs. By themselves, QWs exhibit many fascinating properties which, as we show, translate to interesting properties of quantum cryptographic protocols.

An issue with significant impact on both classical and quantum cryptography is the absence of long-term stable quantum memories. The design of quantum memories, in which a large amount of quantum states should be stored for a long time and processed, is a hard task, since decoherence effects, due to thermal noise and imperfections of the system, inevitably occur.[2] This is a huge challenge towards the construction of operational and scalable quantum computers. Therefore, the classical cryptosystems that are vulnerable to quantum adversaries remain secure as long as a large-scale quantum computer does not exist. On the other hand, the security of quantum cryptosystems depends also on the existence or absence of long-term stable quantum memories, as we will now explain. In general, the security proofs of quantum cryptographic protocols assume all-powerful adversaries who are able to reliably store quantum states for as long as they wish [?]. Their security, thus, will not be compromised by a future technological development of stable quantum memories. However, for practical mid-term applications of quantum cryptography, it is sufficient to consider adversaries with access to more realistic noisy and/ or bounded quantum memories. Along these lines, there have been proposed several cryptographic protocols, whose security is studied with respect to the memory resources that an adversary could possess [? ? ? ? ? ? ?].

In search of stable quantum memories that would, in turn, permit the realisation of large-scale quantum computers, researchers from different areas have focused their attention in trying to find physical systems able to preserve the coherence of quantum states for timescales much longer than the timescale of logical operations. Topologically ordered

[2]During the completion of this thesis, we became aware of two very impressive and promising recent results. In [?], the experimental demonstration of the simultaneous storing of 665 quantum states for more than $50\mu s$ was reported and in [?] the storing of a qubit for 8 hours was achieved.

many-body systems are among the best candidates to fulfil this requirement. These systems have attracted a lot of interest during the last few decades, as they possess some unique "exotic" properties [**?** **?** **?**], which have potentially many applications in various emerging fields such as spintronics, photonics and – as already mentioned – quantum computing. There are two main reasons for which topological systems are very promising for designing stable quantum memories and for performing fault-tolerant quantum computation. First, because their degenerate ground states cannot be distinguished by local observables. This local indistinguishability of quantum information implies that the effects due to local noise can be reversible. Furthermore, it has been shown that the topological order is robust against weak local perturbations on the Hamiltonian at zero temperature [**?** **?** **?**]. These two properties, though, do not solve the problem of decoherence due to thermal noise, which is always present, as maintaining a many-body system at zero temperature for a long time is practically unfeasible. For this purpose, a lot of studies have been concentrated on the behaviour of topological order at finite temperatures. As a result, there have been stated several no-go theorems, that rule out some specific types of many-body lattice Hamiltonians with topological features, which definitely fail to maintain coherence at finite temperatures [**?**]. In parallel, several new physical models have been proposed, whose properties permit the protection of quantum information in thermal environments (for a complete and detailed review, see [**?**]). Most of these models can be decomposed into simpler ones which exhibit topological behaviour and they are based on the seminal toric code [**?**], a landmark in quantum error correction and the topological quantum computing paradigm.

In the second part of this thesis (Chapters 4, 5 and 6), we present our work on the behaviour of topological order at finite temperatures. In particular, we probe the robustness of the topological features with respect to temperature for paradigmatic models of topological systems, by means of the study of the corresponding phase transitions in and out of equilibrium. This way, we aim to contribute to the current effort of fully understanding the properties of topological systems, which are significant for the future design of stable quantum memories and subsequently large-scale quantum computers, with important implications in classical and quantum cryptography.

In the following sections of this chapter, we present general, brief introductions to all the aforementioned topics, thus putting into a more concrete context the work developed in this thesis.

1.2 Public-key cryptography

Public-key cryptography (also called asymmetric cryptography) refers to cryptographic systems that use pairs of public and private (or secret) keys. The public keys, as their name suggests, are known and they are shared among all the users involved in a certain communication protocol, while the corresponding private keys are only known to the owner. Public-key cryptosystems can be used for message encryption or for authentication. To illustrate how they work, let us consider the following examples:

- *Message encryption*
  Suppose that two parties Alice (A) and Bob (B) want to exchange a message. A uses her private key to generate her public key, which she sends over a public channel to B. B uses this public key to encrypt his message and sends it to A. Upon receiving it, A uses her private key to decrypt B's message. It is straightforward to understand that the security of the communication protocol depends on the secrecy of the private key, since anyone can encrypt using the public key, but only one can decrypt using the private key.

- *Authentication*
  Suppose that B received an encrypted message by A and wants to verify that it was actually her who sent it. A has signed the message with her private key and B can use the associated public key to verify that it was A, i.e., the owner of the private key, who sent the message.

The security of most public-key cryptosystems relies on the so-called trapdoor one-way functions.

Definition 1. *(Honest function)*
A function $f : \mathbb{N} \to \mathbb{N}$ is called honest if $|f(x)|$ and $|x|$ are polynomially related, i. e., there exists a k such that for all $x \in \mathbb{N}$:

$$|f(x)| \leq |x|^k + k$$

and

$$|x| \leq |f(x)|^k + k.$$

Definition 2. *(One-way function)*
An honest function $f : \{0,1\}^* \to \{0,1\}^*$ is called one-way if it is injective and the following two conditions hold:
1)(Easy to compute): There exists a polynomial time algorithm $\mathcal{A}$, such that on input x, $\mathcal{A}$ outputs $f(x)$ (i.e. $\mathcal{A}(x) = f(x)$).

2)(Hard to invert): For every probabilistic polynomial time algorithm $\mathcal{A}'$, every polynomial poly and all sufficiently large $n = length(x)$:

$$Pr[f(\mathcal{A}'(f(x))) = f(x)] < 1/poly(n).$$

If we include the extra requirement that the function becomes easy to invert given some extra information called the trapdoor information, then the function is called a *trapdoor one-way function.*

Public-key cryptosystems take advantage of these properties of one-way functions to ensure security of the communication. In particular, they provide the legitimate users A and B with a mathematical problem which is easy to solve, while any eavesdropper E, attempting to intercept, needs to solve a computationally very hard problem. There exist several computationally hard mathematical problems, which are good candidates for one-way functions, such as the integer factorisation problem and the discrete logarithm problem, upon which most of the practical cryptosystems that we use nowadays are based. Nevertheless, a rigorous proof for the existence of one-way functions is missing; such a proof would also imply the solution of the famous open problem $P \neq NP$ [**?**]. Practically, this means that the security of all current cryptosystems based on mathematical hardness assumptions can be threatened by adversaries who might possess advanced algorithms and hardware. Such an example is the celebrated Shor's quantum algorithm for the efficient factoring of prime numbers [**?**]. It was proposed in 1997 by Peter Shor and it solves in polynomial time the integer factoring and the discrete logarithm problem. Hence, when quantum computers will be available, an adversary that possesses one will be able to crack almost all practical public-key cryptosystems (such as RSA, Diffie-Hellman, ElGamal etc). Consequently, the need for public-key cryptosystems secure against attacks by adversaries with quantum computers arose. In a first attempt to address this problem, the authors in [**?**] extend the model of public-key cryptosystems to quantum public-key cryptosystems. They define quantum trapdoor one-way functions, as the counterpart of trapdoor one-way functions in the case of quantum Turing machines and assuming their existence they define quantum public-key cryptographic systems, in analogy to the classical case. Later, in [**?**] a concrete quantum public-key cryptographic system was presented, whose security is based on the indistinguishability of quantum states and more recently, Nikolopoulos [**?** **?**] proposed a secure public-key encryption scheme based on single-qubit rotations.

1.3 Quantum key distribution

A QKD scheme is a protocol between two parties A and B that can perform quantum operations with the purpose of establishing a common classical string (their shared key), which afterwards they can use to communicate privately in a pre-agreed encryption scheme (such as a one-time-pad). Therefore, it is required that any third party, that might be eavesdropping, is not able to extract information about the key, thus compromising the privacy of the communication. The eavesdropper is usually called Eve (E). Bennett and Brassard [**?**] in 1984, and Ekert [**?**] in 1991, proposed the first QKD protocols, upon which most of the discrete variables QKD protocols are based. Since then a lot of modifications and improvements have been proposed in order to achieve unconditionally secure and practical QKD schemes, by taking advantage of the laws of quantum mechanics [**?** **?** **?** **?**].

QKD protocols can be divided in two categories: the prepare-and-measure (PM) protocols and the entanglement-based (EB) protocols. In the former, the key is obtained by performing measurements on the quantum states that the parties exchange (ideally these states are pure), while in the latter, the parties share entangled states and they obtain the key by performing local measurements on their part of the entangled pair (these reduced states are mixed). In both kinds, some authenticated classical communication between the parties is also required for establishing the shared key. The aforementioned BB84 [**?**] and E91 [**?**] protocols are the first, simplest and most illustrative representatives of PM and EB protocols, respectively. The security of these protocols is based on physical laws (as opposite to computational hardness assumptions for the current classical cryptosystems), specifically on principles and properties of quantum mechanics, such as the Heisenberg uncertainty principle, the non-cloning theorem [**?**], the monogamy of entanglement [**?**], as well as the violation of Bell's inequalities [**?** **?**]. In 1992, Bennet, Brassard and Mermin [**?**] showed that the security analysis of a simpler EB protocol similar to the E91, could be reduced to the security analysis of the BB84 protocol, thus creating a whole new context in quantum cryptography. Since then, the relationship between the presence of entanglement (and specifically the ability of the involved parties to certify or distil entanglement) and the security of QKD protocols has been thoroughly investigated [**?** **?** **?** **?**].

In this context, a quite common technique, when it comes to proving security of PM QKD protocols, is to consider an equivalent EB protocol and prove its security. Security of the latter implies security of the former. The proofs of security for EB protocols are widely based on various entropy inequalities that have been proposed [**?** **?** **?** **?** **?** **?** **?**], and they provide bounds on the maximum information that an eavesdropper E can extract, depending on her attacks. These entropy bounds are then used to calculate the

key rate that the parties A and B can securely obtain [**?** **?**].

In order to calculate the aforementioned entropy bounds one considers the probability distributions that result from the measurements that A and B perform on the pairs of the entangled states that they share, followed by error-correction and other post-processing techniques that they might choose to use. The statistics that A and B obtain depend crucially on the measurement devices that they possess; since they share entanglement their measurement data should be correlated, and if not, the parties conclude that their measurement devices cannot be trusted. This happens either because E is interfering in the communication and introduces disturbance or because the measurement devices themselves are not properly working. If the measurement devices are not working properly, E can use that to her advantage, thus compromising the security of the protocol. To overcome this problem, a whole new area of QKD has been created, the so-called device-independent QKD [**?** **?** **?** **?**]. In this framework, the measurement devices of A and B are not trusted – they are rather considered as black boxes that generate probability distributions, which do not necessarily result from measuring pairs of entangled states; they might even be classical probability distributions that E is providing. Therefore, A and B have an extra task to certify the presence of entanglement, i.e., to make sure that their measurement data truly come from the entangled states that they assume to share. The correlations are tested through the violation of various Bell-type inequalities, depending on the dimension of the systems exchanged, the kind of the entangled states and the type of measurements they assume [**?** **?** **?**]. We should note though that dealing with a device-independent scenario is much more complicated not only theoretically but also during the evaluation of the respective figures of merit. For this reason, the trusted device protocols have not been abandoned, as they are quite easier to deal with in practice. On the same time the technological progress promises higher trust in the devices in the future. An intermediate scenario exists, the so-called semi-device-independent QKD, in which one of the parties does not trust his device – let's say B – while the other – let's say A – does. In this case, the probability distribution of B is assumed to be classical, while A's probability distribution is assumed to come from a quantum state, resulting in a joint probability distribution of a so-called classical-quantum state. In this case, the correlations are tested through the violation of the respective steering inequalities [**?** **?** **?** **?** **?** **?** **?** **?**]. Consequently, these three different levels of trust to the devices are connected and can be studied along with three basic features that characterise the entanglement properties of quantum states, namely their separability, locality and steerability, respectively. Here, we should also stress that the aforementioned equivalence between PM and EB protocols does not in general hold if the devices are not trusted. However, under specific assumptions about the devices we can have this equivalence in

the device-independent case [**?**].

Besides the problem of untrusted devices, there is another related issue that should be resolved if we really want to speak about unconditionally secure QKD protocols [**?**], and that is the randomness problem. Most of QKD protocols assume that the parties have access to some source of randomness and this assumption is crucial when it comes to proving security. As an example, one can consider the BB84 protocol, where A and B randomly choose the preparation and measurement bases, respectively, and this assumption ensures the security of the protocol. However, it is practically very hard to have perfect randomness sources, and E can use this to her advantage. Therefore, the parties should be able to check how good their randomness sources are for the requirements of the protocol they want to execute; in other words, they should be able to certify randomness, such that E's possible interference does not compromise the security of the protocol. On the same time, a lot of effort has been put in order to find ways that would enable access to more randomness. These issues of randomness certification and generation has been addressed in numerous studies [**? ? ? ? ? ?**].

We conclude this section by mentioning that it has been shown in several studies [**? ? ? ? ? ?**] that when the parties exchange higher dimensional systems (qudits instead of qubits), the respective QKD protocols can tolerate more noise than the 2-dimensional ones, thus opening a new direction in both the theoretical and practical investigation of QKD. Due to the high dimension of their positions space, the use of QWs in QKD seems to be a very promising option, as we will show in Chapter 3.

1.4 One-dimensional discrete-time quantum walks

In the work presented in this thesis, we consider dicrete-time QWs (DTQWs) on the line and on the circle. In this section we will introduce and briefly describe some of their basic properties. In a DTQW on the infinite line, we consider the movement of a walker along discrete positions on it, labeled by $i \in \mathbb{Z}$. At each step the particle coherently moves to the left and to the right, depending on the state of an internal degree of freedom, the so-called coin state. The Hilbert space of the QW H_{qw} is the tensor product of the position Hilbert space H_p and the coin Hilbert space H_c, $H_{qw} = H_p \otimes H_c$. The position Hilbert space is $H_p = \text{span}\{|i\rangle, i \in \mathbb{Z}\}$, and the coin Hilbert space H_c is spanned by the two possible coin states $|R\rangle, |L\rangle$ corresponding to heads and tails. The letters R and L stand for right and left according to which side the walker is moving, when the coin shows heads or tails, respectively. A single step of the walk is given by the unitary evolution operator

$$\hat{U}_{qw} = \hat{S} \cdot (\hat{I}_p \otimes \hat{U}_c),$$

where $\hat{I}_p$ is the identity operator in H_p, $\hat{U}_c$ is a rotation in H_c and $\hat{S}$ is the so-called shift operator, given by

$$\hat{S} = \sum_{i \in \mathbb{Z}} |i+1\rangle \langle i| \otimes |R\rangle \langle R| + |i-1\rangle \langle i| \otimes |L\rangle \langle L| ,$$

and coherently moves the walker one position to the right and to the left on the line, depending on its coin state.
The general expression for $\hat{U}_c$ is:

$$\hat{U}_c = \hat{U}_c(\theta, \xi, \zeta) = \begin{bmatrix} e^{i\xi}\cos\theta & e^{i\zeta}\sin\theta \\ -e^{-i\zeta}\sin\theta & e^{-i\xi}\cos\theta \end{bmatrix}. \tag{1.1}$$

1.4.1 Shift operator on the circle

In the case of a DTQW on the circle, the walker hops along discrete positions on it. To simulate such a walk, one could either identify the positions $-P$ and P of a line, or connect the two, thus altering the corresponding shift operator. In the former, the circle has an even number of positions ($2P$), while in the latter it has an odd number of positions ($2P+1$).

In both cases, we can relabel the positions Hilbert space to be $\mathcal{H}_p = \{|i\rangle : i \in \{0, \ldots, P-1\}\}$, and write the shift operator on the circle with P positions as

$$\begin{aligned} \hat{S} &= \sum_{i=0}^{P-1} \Big(|i+1 \,(\mathrm{mod}\ P)\rangle \langle i| \otimes |R\rangle \langle R| + |i-1 \,(\mathrm{mod}\ P)\rangle \langle i| \otimes |L\rangle \langle L| \Big) \\ &= \hat{T}_1 \otimes |R\rangle \langle R| + \hat{T}_{-1} \otimes |L\rangle \langle L| , \end{aligned} \tag{1.2}$$

where

$$\hat{T}_x = \sum_{i=0}^{P-1} |i + x \,(\mathrm{mod}\ P)\rangle \langle i| \tag{1.3}$$

is the translation operator for x positions.

1.5 Free-fermion systems exhibiting non-trivial topological order

Topological phases of matter are a subject of active research during the last decades, as they constitute a whole new paradigm in condensed matter physics. Since the seminal

paper of Haldane [**?**], where the anomalous Hall insulator was discovered, there has been an intense investigation of these "exotic" phases of matter [**? ? ? ?**]. In contrast to the well-studied "standard" quantum phases of matter, described by local order parameters (see for example Anderson's classification [**?**]), the ground states of topological systems are characterised by global order parameters, which are called topological invariants, and they have the same value throughout the same topological phase. If a phase is topologically trivial, then the value of the associated invariant is 0. Examples of such invariants are the Chern numbers [**?**], the Berry geometric phase [**?**], and non-local string parameters [**?**] (cf. [**?**]). Free-fermion systems that describe insulators and superconductors with an energy gap can exhibit topological features, as long as their Hamiltonians possess some of the following symmetries, namely time-reversal (TRS), particle-hole (PHS) and chiral symmetry (CS). The respective topological phases can be classified according to these symmetries and the dimension of the system [**? ?**].

Due to the discrete nature of the topological invariants, Hamiltonians of gapped systems in different topological phases cannot be smoothly transformed from one into the other unless passing through a gap-vanishing region of criticality. In other words, for a topological phase transition (PT) to occur, the energy gap has to close. Topological PTs are quite different from the "standard" quantum PTs [**?**], which are traditionally described by the Landau theory [**?**]. According to the Landau theory, a quantum PT occurs when we adiabatically change a parameter of the system around a region of criticality at temperature zero, thus breaking a local symmetry of the system. On the other hand, when it comes to topological PTs, there is no symmetry breaking; the symmetries of the system are rather preserved.

At zero-temperature, the critical behaviour of systems featuring topological order is accompanied by the existence of edge states at the boundary between two distinct topological phases. These edge states are symmetry-protected, i.e., they are robust against perturbations of the Hamiltonian that preserve the respective symmetries, and their presence is predicted by the bulk-to-boundary correspondence principle [**? ?**].

In addition to the standard local symmetry breaking and the aforementioned global topological order parameters, several information-theoretic quantities were used to study PTs in general, such as entanglement measures [**? ? ? ?**] and the fidelity [**? ? ? ? ? ? ? ?**]. Whenever there is a PT, the state of the system changes significantly and the fidelity, as a measure of the distinguishability between two quantum states, signals out this change. In [**?**] the authors analysed the intimate connection between the pure-state fidelity and the Berry phase, showing that the fidelity-induced Riemannian metric and the Berry curvature are the real and imaginary part, respectively, of the so-called quantum geometric tensor and thus, they provide a universal framework for the study of quantum

PTs.

A question that naturally arises is whether there is any kind of topological order at finite temperatures and which could be the appropriate quantities ("topological order parameters") to describe possible PTs. In the context of systems in thermal equilibrium, several different approaches have been used to tackle this problem [**?** **?** **?** **?** **?** **?**] and various types of mixed-state generalisations of geometric phases [**?** **?**] were used to infer topological phase transitions of systems at finite temperature (for the pure-state case of the Berry phase, see [**?** **?**]). The most promising one is based on the work of Uhlmann [**?**], who extended the notion of geometrical phases from pure states to density matrices. The concept of the Uhlmann holonomy, and certain quantities that can be derived from it, were used to infer PTs at finite temperatures [**?** **?** **?** **?** **?** **?**]. There exist several proposals for the observation of the Uhlmann geometric phase [**?** **?**] and experimental demonstrations have been reported in [**?** **?**]. Nevertheless, the physical meaning of these quantities and their relevance to the observable properties of the corresponding systems stay as an interesting open question [**?** **?** **?**]. On the other hand, the fidelity is, through the Bures metric [**?**], closely related to the Uhlmann connection. Therefore, both the fidelity and the Uhlmann connection can be used to infer the possibility of PTs, as shown in [**?**] for the case of the BCS superconductivity.

1.6 The fidelity, the Uhlmann connection and their use in the study of phase transitions of systems in equilibrium

In Chapters 4 and 5, we present our study of PTs at finite temperatures for topological systems in equilibrium, where we will use the well-established fidelity approach, as well as a quantity associated to the Uhlmann connection (along the lines of [**?**]). In this section we provide a general overview of the fidelity and its relationship with the Uhlmann connection, and how they can be used in order to infer the existence of PTs at finite temperatures.

We start by considering the classical fidelity between two probability distributions. Given the probability distributions $\{p_x\}_{x\in L}$ and $\{q_x\}_{x\in L}$ of two random variables X and Y, respectively, ranging over the same set $L = \{1, 2, \cdots, n\}$, the classical fidelity is defined as

$$F(p_x, q_x) = \sum_{x\in L} \sqrt{p_x q_x}.$$

It is a distinguishability measure for classical information, as it describes how "close" the

two distributions are. Geometrically, it is the inner product between two (normalised) vectors $(\sqrt{p_1}, \cdots, \sqrt{p_n})$ and $(\sqrt{q_1}, \cdots, \sqrt{q_n})$ in the Euclidean space.

We now proceed to introduce the quantum analog of classical fidelity, the fidelity between two quantum states ρ_1 and ρ_2. One way to do so is to take into account that each time we measure an observable, let's say $\hat{O}$, with respect to two quantum states ρ_1 and ρ_2, we end up with two classical probability distributions $\{p_x^{\hat{O}}\}_{x\in L}$ and $\{q_x^{\hat{O}}\}_{x\in L}$, respectively, for which we can calculate the classical fidelity $F(p_x^{\hat{O}}, q_x^{\hat{O}})$. It has been shown that the quantum fidelity given as

$$F(\rho_1, \rho_2) = \mathrm{tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}},$$

is always smaller or equal than the classical fidelity between the two respective probability distributions

$$F(\rho_1, \rho_2) \leq F(p_x^{\hat{O}}, q_x^{\hat{O}}).$$

The equality is achieved for a specific positive-operator valued measurement (POVM) associated to a so-called optimal observable for the two states, see [**?**].

In analogy to the classical case, $F(\rho_1, \rho_2)$ is associated to the distance between ρ_1 and ρ_2, thus it is a measure of their distinguishability. Nevertheless, we should stress that fidelity itself is not a distance, however it can be associated to the Bures distance in the space of density matrices, as follows:

$$d_B(\rho_1, \rho_2) = \sqrt{2(1 - F(\rho_1, \rho_2))},$$

with $d_B(\rho_1, \rho_2)$ being the Bures distance. The fidelity takes its minimum value $F(\rho_1, \rho_2) = 0$, when the two states are completely distinguishable and this corresponds to the maximum value of the Bures distance $d_B(\rho_1, \rho_2) = 1$. On the other hand, the Bures distance is minimum $d_B(\rho_1, \rho_2) = 0$, when the fidelity achieves its maximum value $F(\rho_1, \rho_2) = 1$, which means that the states ρ_1 and ρ_2 are completely indistinguishable.

A few basic properties of the fidelity are the following:

1. Fidelity is symmetric with respect to its arguments: $F(\rho_1, \rho_2) = F(\rho_2, \rho_1)$.

2. Fidelity is invariant under unitary transformations: $F(U\rho_1 U^\dagger, U\rho_2 U^\dagger) = F(\rho_1, \rho_2)$.

In the special case that one of the two states is pure, for example if $\rho_2 = |\psi\rangle\langle\psi|$, the fidelity is $F(|\psi\rangle, \rho_1) = \sqrt{\langle\psi|\rho_1|\psi|\psi|\rho_1|\psi\rangle}$. Furthermore, for two pure states $|\psi\rangle$ and $|\phi\rangle$: $F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi|\psi|\phi\rangle|$, which is exactly the overlap between the two states.

We proceed by showing the relationship between the fidelity and the Uhlmann connection. The set of mixed states is convex but not linear in general, i.e., for any two

mixed states ρ_1 and ρ_2 and scalars λ_1 and λ_2 the linear combination $\lambda_1\rho_1 + \lambda_2\rho_2$ is not necessarily a mixed state. Nevertheless, a convex combination of ρ_1 and ρ_2 is a mixed state, i.e, for $\lambda_1, \lambda_2 \geq 0$ and $\lambda_1 + \lambda_2 = 1$, the linear combination $\lambda_1\rho_1 + \lambda_2\rho_2$ belongs in the set of mixed states. This feature of non-linearity imposes significant restrictions when it comes to perform a geometric study. On the other hand, we do not have this issue in the case of pure states, since a pure state $\rho = |\psi\rangle\langle\psi|$, can be treated as a projection on the subspace spanned by $|\psi\rangle$, therefore inheriting the geometric properties of the Hilbert space. Notice the $U(1)-$ gauge freedom; $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ correspond to the same state $\rho = |\psi\rangle\langle\psi|$.

To overcome this restrictions, one can introduce the concept of the purification of a mixed state, that is any mixed state in a certain Hilbert space can be seen as the reduced state of a pure state in a different (larger) Hilbert space. Specifically, let us assume that we have a mixed state ρ represented by the corresponding density matrix acting on a finite-dimensional Hilbert space H_1. Then we can always consider a second Hilbert space H_2 and a pure state $|\Psi\rangle \in H_1 \otimes H_2$, such that

$$\rho = \mathrm{tr}_2(|\Psi\rangle\langle\Psi|).$$

The state $|\Psi\rangle$ is called a purification of ρ. We should stress that for a state ρ one can find in general more than one purifications. Nevertheless, there is a choice of purification of particular interest, the one that reveals the relationship between the fidelity and the Uhlmann connection. This purification belongs in the so-called Hilbert-Schmidt space:

Definition 3. *(Hilbert-Schmidt space)*
Given a finite-dimensional Hilbert space H, the corresponding Hilbert-Schmidt space is the tensor product $H \otimes H^*$, where H^* is the dual of H. This space is equipped with the respective Hilbert-Schmidt inner product, which for $w_1, w_2 \in H \otimes H^*$ is defined as

$$\langle w_1, w_2\rangle = \mathrm{tr}\Big(w_1^\dagger w_2\Big).$$

Any mixed state $\rho \in H$ can be purified by means of $w \in H \otimes H^*$ as $\rho = ww^\dagger$, where w is called the amplitude of ρ in this case. Notice that there is a $U(n)-$ gauge freedom in the choice of the amplitude, analogously to the $U(1)-$ gauge freedom in the case of pure states; w and wU with U being unitary correspond to the same state $\rho = ww^\dagger$. The choice of the Hilbert-Schmidt space is quite special, since there is no space smaller than $H \otimes H^*$ where we can purify ρ, while choosing a larger space is not necessary because the purified density matrices will always belong in a subspace isomorphic to the Hilbert-Schmidt space [**?**]. In what follows, we describe how a particular choice of the amplitude reveals the relationship between the fidelity and the Uhlmann connection.

Two amplitudes w_1 and w_2, such that $\rho_1 = w_1 w_1^\dagger$ and $\rho_2 = w_2 w_2^\dagger$, are said to be parallel in the Uhlmann sense if they minimise the distance induced by the Hilbert-Schmidt inner product $\langle w_2, w_1\rangle = \mathrm{tr}\Big(w_2^\dagger w_1\Big)$:

$$||w_2 - w_1||^2 = \mathrm{tr}(w_2 - w_1)^\dagger (w_2 - w_1) = 2(1 - \mathrm{Re}\langle w_2, w_1\rangle).$$

Minimising $||w_2 - w_1||^2$ is equivalent to maximising $\mathrm{Re}\langle w_2, w_1\rangle$:

$$\mathrm{Re}\langle w_2, w_1\rangle \leq |\langle w_2, w_1\rangle| = |\,\mathrm{tr}\Big(w_2^\dagger w_1\Big)|.$$

Considering the polar decompositions $w_i = \sqrt{\rho_i} U_i, i \in \{1, 2\}$, where the U_i's are unitary matrices, the above inequality becomes

$$\mathrm{Re}\langle w_2, w_1\rangle \leq |\,\mathrm{tr}\Big(U_2^\dagger \sqrt{\rho_2}\sqrt{\rho_1} U_1\Big)|.$$

Using the polar decomposition $\sqrt{\rho_2}\sqrt{\rho_1} = |\sqrt{\rho_2}\sqrt{\rho_1}|V$, with V unitary, and the cyclic property of the trace, we obtain

$$\mathrm{Re}\langle w_2, w_1\rangle \leq |\,\mathrm{tr}\Big(|\sqrt{\rho_2}\sqrt{\rho_1}| V U_1 U_2^\dagger\Big)|.$$

The Cauchy-Schwarz inequality implies

$$\mathrm{Re}\langle w_2, w_1\rangle \leq \mathrm{tr}\,|\sqrt{\rho_2}\sqrt{\rho_1}|,$$

with the equality holding for $V U_1 U_2^\dagger = I$, where I is the identity. Finally, we can write $|\sqrt{\rho_2}\sqrt{\rho_1}| = \sqrt{(\sqrt{\rho_2}\sqrt{\rho_1})^\dagger (\sqrt{\rho_2}\sqrt{\rho_1})}$ and get

$$\mathrm{Re}\langle w_2, w_1\rangle \leq \mathrm{tr}\,\sqrt{(\sqrt{\rho_1}\rho_2\sqrt{\rho_1})} = F(\rho_1, \rho_2),$$

which shows the relationship between the fidelity and the Uhlmann connection, as characterised by V, the so-called Uhlmann factor (associated to the choice of gauge for the amplitudes).

To illustrate this relationship better, let us consider the Uhlmann parallel transport condition. Suppose that $\rho(t)$ is a closed curve of density matrices parametrised by $t \in [0, 1]$. Then, given an initial state $\rho(0)$ and the corresponding amplitude $w(0)$, the Uhlmann parallel transport condition, taken for an infinitesimal time period δt, yields a unique curve in the space of amplitudes (called the horizontal lift), along which $w(t)$ and $w(t + \delta t)$ are parallel, $\forall t$. The length of the curve in the space of amplitudes – with respect to the metric induced by the Hilbert-Schmidt inner product – is equal to

the length of the corresponding curve in the space of density matrices – with respect to the Bures metric. The respective Bures distance is given in terms of the fidelity as $d_B(\rho_1, \rho_2) = \sqrt{2(1 - F(\rho_1, \rho_2))}$.

Finally, we present how we can apply the above concepts in the study of PTs. Consider two close points t and $t + \delta t$ in the parameter space and the respective states $\rho(t)$ and $\rho(t+\delta t)$ in the space of density matrices. If the two states belong to the same phase, they almost commute, hence $V \approx I$ and $\sqrt{\rho(t+\delta t)}\sqrt{\rho(t)} \approx |\sqrt{\rho(t+\delta t)}\sqrt{\rho(t)}|$. Moreover, since they are almost indistinguishable, $F(\rho(t), \rho(t + \delta t)) \approx 1$. On the other hand, if $\rho(t)$ and $\rho(t + \delta t)$ belong to different phases, they must be significantly different, thus their fidelity must be smaller than one [**?**]. The difference between the two states can be in their spectra or their eigenbases. In the case of the latter, we also have non-trivial $V \neq I$ [**?**].

To quantify the difference between the Uhlmann factor V and the identity, we will use the following quantity, as defined in [**?**]:

$$\Delta(\rho(t), \rho(t + \delta t)) := F(\rho(t), \rho(t + \delta t)) - \mathrm{tr}\Big(\sqrt{\rho(t + \delta t)}\sqrt{\rho(t)}\Big). \tag{1.4}$$

For $\rho(t)$ and $\rho(t + \delta t)$ from the same phase, $F(\rho(t), \rho(t + \delta t)) = \mathrm{tr}\Big(\sqrt{\rho(t + \delta t)}\sqrt{\rho(t)}\Big) \approx 1$, therefore $\Delta(\rho(t), \rho(t + \delta t)) \approx 0$, while for $\rho(t)$ and $\rho(t + \delta t)$ from different phases, $F(\rho(t), \rho(t + \delta t)) \neq 1$ and in the case the Uhlmann factor is also non-trivial, we have $\Delta(\rho(t), \rho(t + \delta t)) \neq 0$.

Summarising the above, the departure of fidelity from 1 and the departure of Δ from 0 are signalling the PT points.

1.7 Phase transitions of systems out of equilibrium

The real time evolution of closed quantum systems out of equilibrium has some surprising similarities with thermal PTs, as noticed by Heyl, Polkovnikov and Kehrein [**?**]. They coined the term Dynamical Quantum PTs (DQPTs) to describe the non-analytic behaviour of certain dynamical observables after a sudden quench in one of the parameters of the Hamiltonian. Since then, the study of DQPTs became an active field of research and a lot of progress has been achieved in comparing and connecting them to the equilibrium PTs [**? ? ? ? ? ? ? ? ?**]. Along those lines, there exist several studies of DQPTs for systems featuring non-trivial topological properties [**? ? ? ? ? ? ?**]. DQPTs have been experimentally observed in systems of trapped ions [**?**] and systems of cold atoms in optical lattices, that both exhibit topological features [**?**]. The figure of merit in the study of DQPTs is the Loschmidt Echo (LE) and its derivatives, which have been

extensively used in the analysis of quantum criticality [? ? ? ? ?] and quantum quenches [?]. At finite temperature, generalisations of the zero-temperature LE were proposed, based on the mixed-state Uhlmann fidelity [? ?], and the interferometric mixed-state geometric phase [? ?]. For alternative approaches to finite-temperature DPTs, see [? ?]. As already stressed, the fidelity has been employed numerous times in the study of PTs [? ? ? ? ?], while the interferometric mixed-state geometric phase was introduced in [?]. The two quantities are in general different and it comes as no surprise that they give different predictions for the finite temperature behaviour of systems with topological order [?]: the fidelity LE does not show DPTs at finite temperatures, while the interferometric LE indicates their persistence. In Chapter 6 we study DPTs of topological systems and clarify what their fate at finite temperature truly is, and which of the two opposite predictions better captures their many-body nature.

1.8 Structure of the thesis

The work presented this thesis led to the publication of five papers; four of the them are already published in peer-reviewed journals and one is submitted to a peer-reviewed journal and is currently under review (it is also available as a preprint in arXiv):

- C. Vlachou, J. Rodrigues, P. Mateus, N. Paunković, and A. Souto, Quantum walk public-key cryptographic system, International Journal of Quantum Information, 13(7):1550050, 2015.
- C. Vlachou, W. Krawec, P. Mateus, N. Paunković, and A. Souto, Quantum key distribution with quantum walks, arXiv:1710.07979, (2017).
- B. Mera, C. Vlachou, N. Paunković, and V. R. Vieira, Uhlmann connection in fermionic systems undergoing phase transitions, Phys. Rev. Lett., 119:015702, 2017.
- B. Mera, C. Vlachou, N. Paunković, and V. R. Vieira, Boltzmann-Gibbs states in topological quantum walks and associated many-body systems: fidelity and Uhlmann parallel transport analysis of phase transitions, Journal of Physics A: Mathematical and Theoretical, 50(36):365302, 2017.
- B. Mera, C. Vlachou, N. Paunković, V. R. Vieira, and O. Viyuela, Dynamical phase transitions at finite temperature from fidelity and interferometric Loschmidt echo induced metrics, Phys. Rev. B, 97:094110, 2018.

The thesis begins with the Introduction in Chapter 1, which puts the developed work into context. In Part I of the thesis, which includes Chapters 2 and 3, we present our

work on the applications of QWs in cryptography. In particular, in Chapter 2 we propose a quantum public-key cryptosystem in which the public key is generated by performing a QW. We show that the protocol is secure and we analyse the complexity of the public-key generation and the encryption/ decryption procedures. In Chapter 3, we take advantage of the properties of QWs to design new secure QKD schemes. In particular, we propose three new QKD protocols; a two-way protocol, a one-way protocol of the BB84 type, and a semi-quantum protocol. We prove the security of the first two and the robustness against eavesdropping of the third. For all the aforementioned QKD protocols, we describe in detail the quantum memory requirements for all the parties (legitimate and eavesdropper).

In Part II of the thesis, which includes Chapters 4, 5 and 6, we present our study of PTs at finite temperatures for systems in and out of equilibrium that exhibit non-trivial topological features. In particular, in Chapter 4 we study the behaviour of the fidelity and the Uhlmann connection in systems of fermions undergoing PTs, both topologically trivial and non-trivial. By means of this approach, we show the absence of thermally driven PTs in the case of topological insulators and superconductors. Furthermore, by studying their edge states, we confirm the results obtained by the fidelity and the Uhlmann connection study, that is the gradual disappearance of the topological features at finite temperatures. We also clarify what is the relevant parameter space associated with the Uhlmann connection so that it signals the existence of topological order in mixed states. Among others, we studied the behaviour with respect to temperature of the Majorana modes (edge states of topological superconductors) which are basic constituents for achieving quantum memories [**?** **?** **?** **?**]. In Chapter 5, we consider QW protocols that are known to simulate topological phases and the respective quantum PTs [**?** **?**] for chiral symmetric Hamiltonians, in order to investigate whether the topological order of these systems at zero temperature is also maintained at finite temperatures. Using the same approach as in Chapter 4, we conclude that no temperature-driven PTs occur, i.e., the topological behaviour is washed out gradually as temperature increases. However, we find finite-temperature parameter-driven PTs. In Chapter 6, we move to topological systems out-of-equilibrium and we study finite-temperature DQPTs by means of the fidelity and the interferometric LE induced metrics. When generalising the associated dynamical susceptibilities – which coincide at zero temperature – at finite temperatures one finds that they behave very differently: using the fidelity LE, the zero temperature DQPTs are gradually washed away with temperature, while the interferometric counterpart exhibits finite-temperature DPTs. We analyse the physical differences between the two, and argue which is the more suitable quantity to study, when it comes to perform relevant experiments in topological many-body systems.

Finally, in Chapter 7 we summarise all the above and present our conclusions.

Part I

Applications of Quantum Walks in Cryptography

Chapter 2

A public-key cryptographic system based on quantum walks

In this chapter, we present a quantum public-key cryptographic system, in which the public keys are states generated by means of a QW, while the secret key consists of: (i) the QW operator, (ii) the number of steps that the walk is performed and (iii) the starting position and coin of the QW. In the next section we present the protocol and prove its correctness, while in the following Sections 2.2 and 2.3, we prove its security and efficiency. Finally, in the last section we summarise our results and point out some possible directions for future work.

*The work presented in this chapter corresponds to the work published in [**?**].

2.1 Public-key encryption based on discrete-time quantum walks

For our public-key cryptographic system we will consider DTQWs on a circle, as presented in Section 1.4 of the introductory Chapter 1. To generate the public key, we use a discrete number of possible walks $\hat{U}_k = \hat{S}[\hat{I} \otimes \hat{U}_c(\theta_k, \xi_k, \zeta_k)]$, with $\theta_k = \xi_k = \zeta_k = k\frac{2\pi}{d}$, $k \in \mathcal{I} = \{1, 2, \ldots, d\}$ and $d \in \mathbb{N}$, given by the standard shift and coin operations $\hat{U}_c(\theta_k, \xi_k, \zeta_k)$, presented in Section 1.4.

Protocol 1 (Public-key encryption scheme)**.**

Inputs for the protocol

- *Message to transfer:*
  $m \in \{0, \ldots, 2^n - 1\}$*, i.e., a message of at most* n *bits;*
- *Secret key* $SK = (\hat{U}_k, t, l, s)$ *where:*
  $\hat{U}_k$ *with* $k \in \mathcal{I} = \{1, 2, \ldots, d\}$, $t \in \mathcal{T} = \{t_0, \ldots, t_{max}\} \subset \mathbb{N}$, $l \in \{0, \ldots, 2^n - 1\}$ *and* $s \in \{L, R\}$.

Public-key generation

- *A chooses uniformly at random* $l \in \{0, \ldots, 2^n - 1\}$ *and* $s \in \{L, R\}$*, and generates the initial state* $|l\rangle |s\rangle$*;*
- *Then she chooses, also uniformly at random, the walk* $\hat{U}_k = \hat{S}(\hat{I}_p \otimes \hat{U}_c)$ *and the number of steps* $t \in \mathcal{T}$*;*
- *Finally, she generates the public key:*

$$|\psi_{PK}\rangle = \hat{U}_k^t |l\rangle |s\rangle = \left[\hat{S}(\hat{I}_p \otimes \hat{U}_c)\right]^t |l\rangle |s\rangle . \tag{2.1}$$

Message Encryption

- *B obtains A's public key* $|\psi_{PK}\rangle$*;*
- *He encrypts* m *by applying a spatial translation to obtain:*

$$|\psi(m)\rangle = (\hat{T}_m \otimes \hat{I}_c) |\psi_{PK}\rangle ; \tag{2.2}$$

- *B sends* $|\psi(m)\rangle$ *to A.*

Message Decryption

- *A applies* $\hat{U}_k^{-t}$ *to the state* $|\psi(m)\rangle$*;*

- *She performs the measurement*

$$\hat{M} = \sum_i |i\rangle \langle i| \otimes \hat{I}_c \tag{2.3}$$

and obtains the result m'. The message sent by B is $m = m' - l \pmod N$.

2.1.1 Correctness of the protocol

Proposition 1. *The above protocol is correct, that means that if A and B follow it, and no third party intervenes during its execution, at the end of the decryption phase A recovers the message sent by B with probability* 1.

Proof. The correctness of the protocol when both parties follow the prescribed steps is a direct consequence of the fact that the QW $\hat{U}_k^t$ commutes with any translation $\hat{T}_m$ (see the following Lemma 1). Thus, the state of the system before the final step of the decryption phase (measurement), is:

$$\begin{aligned} |\psi_f\rangle &= \hat{U}_k^{-t} |\psi(m)\rangle \\ &= \hat{U}_k^{-t} (\hat{T}_m \otimes \hat{I}_c) \hat{U}_k^t |l\rangle |s\rangle \\ &= (\hat{T}_m \otimes \hat{I}_c) |l\rangle |s\rangle \\ &= |l + m \,(\mathrm{mod}\ N)\rangle |s\rangle . \end{aligned} \tag{2.4}$$

Hence, upon measuring $\hat{M}$ and obtaining $m' = l + m \,(\mathrm{mod}\ N)$, the last modular operation performed in the last step of the *Message Decryption* reveals that the decrypted message is indeed m. □

Below, we prove that $\hat{U}_k^t$ and $(\hat{T}_m \otimes \hat{I}_c)$ commute.

Lemma 1. *Let $N \geq 2^n$ where n is a fixed integer. Let $\hat{U}_k^t$ be a QW from Protocol 1 and let $\hat{T}_m$ denote the translation operator for m positions modulo N. Then $\hat{U}_k^t$ and $(\hat{T}_m \otimes \hat{I}_c)$ commute.*

Proof. Notice that the action of any $\hat{U}_k$ used in Protocol 1 can be written as:

$$\hat{U}_k |l\rangle |s\rangle = \alpha_{L(s)} |l-1\rangle |L\rangle + \alpha_{R(s)} |l+1\rangle |R\rangle , \tag{2.5}$$

where $|L\rangle$ and $|R\rangle$ are the orthogonal coin states and $\alpha_{L/R(s)}$ is the probability amplitude to find the walker in position $l-1$ or $l+1$, depending on its spin. Notice also that $\hat{T}_m$ is defined as:

$$\hat{T}_m \left| l \right\rangle = \left| l + m \,(\mathrm{mod}\ N) \right\rangle . \tag{2.6}$$

Then, for any element of the form $\left| l \right\rangle \left| s \right\rangle$ we have:

$$\begin{aligned} (\hat{T}_m \otimes \hat{I}_c)\hat{U}_k \left| l \right\rangle \left| s \right\rangle &= (\hat{T}_m \otimes \hat{I}_c)[\alpha_{L(s)} \left| l-1 \right\rangle \left| L \right\rangle + \alpha_{R(s)} \left| l+1 \right\rangle \left| R \right\rangle] \\ &= \alpha_{L(s)} \left| l - 1 + m \,(\mathrm{mod}\ N) \right\rangle \left| L \right\rangle \\ &\quad + \alpha_{R(s)} \left| l + 1 + m \,(\mathrm{mod}\ N) \right\rangle \left| R \right\rangle . \end{aligned} \tag{2.7}$$

On the other hand, we also have:

$$\begin{aligned} \hat{U}_k(\hat{T}_m \otimes \hat{I}_c) \left| l \right\rangle \left| s \right\rangle &= \hat{U}_k \left| l + m \,(\mathrm{mod}\ N) \right\rangle \left| s \right\rangle \\ &= \alpha_{L(s)} \left| l - 1 + m \,(\mathrm{mod}\ N) \right\rangle \left| L \right\rangle \\ &\quad + \alpha_{R(s)} \left| l + 1 + m \,(\mathrm{mod}\ N) \right\rangle \left| R \right\rangle . \end{aligned} \tag{2.8}$$

□

Observe that this lemma can be extended to more general shift operations, which allow for jumps across two or more positions, or even leave the position state unchanged, depending on the coin state.

2.2 Security of the protocol

The protocol consists of two phases. In the first, A sends a public key $\left| \psi_{PK} \right\rangle$ to B. In the second, upon encrypting the message m, B sends back to A the state $\left| \psi(m) \right\rangle$. Therefore, one has to show the security of the secret key during the first phase and the security of the message during the second phase.

Our proof of security is based on Holevo's Theorem, that bounds the amount of classical information that an eavesdropper can retrieve from a given quantum mixed state by means of a POVM measurement.

Let us denote by $\hat{\rho}_{PK}$ the mixed state of the public key, as perceived by E, who does not know *a priori* the secret key SK chosen by A. Even if E were to know $\hat{U}_k$ and t, $\hat{\rho}_{PK}$ is completely mixed:

$$
\begin{aligned}
\hat{\rho}_{PK} &= \hat{U}_k^t \left[\frac{1}{2^{n+1}} \sum_{l=0}^{2^n-1} \sum_{s\in\{L,R\}} |l\rangle \langle l| \otimes |s\rangle \langle s| \right] (\hat{U}_k^t)^\dagger \\
&= \hat{U}_k^t \left(\frac{1}{2^{n+1}} \hat{I}_p \otimes \hat{I}_c \right) (\hat{U}_k^t)^\dagger \qquad (2.9) \\
&= \frac{1}{2^{n+1}} (\hat{I}_p \otimes \hat{I}_c) \hat{U}_k^t (\hat{U}_k^t)^\dagger \qquad (2.10) \\
&= \frac{1}{2^{n+1}} \hat{I}_p \otimes \hat{I}_c.
\end{aligned}
$$

Assuming that E performs a measurement on $\hat{\rho}_{PK}$, Holevo's Theorem implies that the mutual information $I(SK, E)$ between the secret key SK and her inference is bounded from above by the Von Neumann entropy of this state:

$$
I(SK, E) \leq S(\hat{\rho}_{PK}) = -\operatorname{tr}(\hat{\rho}_{PK} \log \hat{\rho}_{PK}) = n + 1. \qquad (2.11)
$$

To conclude that the protocol is secure we have to show that the mutual information is very small compared to the Shannon entropy of the secret key. Indeed, the Shannon entropy of the secret key depends on the probability to choose $\hat{U}_k, t, l$ and s. In the following we denote by p_k the probability to choose $\hat{U}_k$ from the set $\left\{ \hat{U}_k | k \in \mathcal{I} = \{1, 2, \ldots, d\} \right\}$, by p_t the probability to run the walk for t steps, with $t \in \mathcal{T} = \{t_0, \ldots, t_{max}\}$, and by $p_{l,s}$ the probability to choose l from $\{0, 1, \ldots, 2^n - 1\}$ and s from $\{L, R\}$ in order to generate the initial state $|l\rangle |s\rangle$. Since these choices are random and independent, the probability of a certain secret key SK is given by:

$$
p_{SK} = p_k \; p_t \; p_{l,s} = \frac{1}{d \; |\mathcal{T}| \; 2^{n+1}}, \qquad (2.12)
$$

where $|\mathcal{T}|$ is the cardinality of $\mathcal{T}$.

The above probability distributions are uniform, so the Shannon entropy of the secret key is:

$$
\begin{aligned}
H(p_{SK}) &= -\sum_{k\in\mathcal{I}} \sum_{t\in\mathcal{T}} \sum_{l=0}^{2^n-1} \sum_{s\in\{L,R\}} p_k \; p_t \; p_{l,s} \log_2(p_k \; p_t \; p_{l,s}) \\
&= \log_2(d \; |\mathcal{T}| \; 2^{n+1}) \\
&= \log_2(d \; |\mathcal{T}|) + n + 1. \qquad (2.13)
\end{aligned}
$$

Thus, we have:

$$
I(SK, E) \leq S(\hat{\rho}_{PK}) < H(p_{SK}), \qquad (2.14)
$$

since $\log_2(d\,|\mathcal{T}|) >> 1$. With the appropriate choice of $|\mathcal{T}|$ and d, e.g., $|\mathcal{T}|, \log d \approx poly(n)$, for sufficiently large n, the Shannon entropy of the secret key has a polynomial overhead over the von Neumann entropy of the public key as seen by E,

$$H(p_{SK}) - S(\hat{\rho}_{PK}) = \log_2(d\,|\mathcal{T}|) \approx poly(n). \tag{2.15}$$

This way, upon obtaining the maximal possible information about the secret key, given by $S(\hat{\rho}_{PK})$, E's uncertainty (in the number of bits) of the SK is still polynomial in n, i.e., the number of keys consistent with the information she has is exponential in n. We note that the choice of $d \approx \exp(n)$

secures the secrecy of the encrypted message, while $|\mathcal{T}| \approx poly(n)$ was chosen to maintain the protocol's efficiency, discussed in the next section.

Notice that d could be exponential on n, since in the protocol we only need to provide information to specify the walk (in fact, $\log(d)$ bits). However, in order for the protocol to be efficient as we discuss in the next section, $|\mathcal{T}|$ must be polynomial on n.

For the rest of this section we will discuss the security of the message m during the second phase of the protocol, when B sends the encrypted message $|\psi(m)\rangle = (\hat{T}_m \otimes \hat{I}_c)\,|\psi_{PK}\rangle$ to A. Without knowing the secret key, the state perceived by E is still a complete mixture:

$$\begin{aligned} \hat{\rho}_E &= (\hat{T}_m \otimes \hat{I}_c)\left(\frac{1}{2^{n+1}}\hat{I}_p \otimes \hat{I}_c\right)(\hat{T}_m \otimes \hat{I}_c)^\dagger = \\ &= \frac{1}{2^{n+1}}(\hat{T}_m \otimes \hat{I}_c)(\hat{T}_m \otimes \hat{I}_c)^\dagger(\hat{I}_p \otimes \hat{I}_c) = \frac{1}{2^{n+1}}\hat{I}_p \otimes \hat{I}_c. \end{aligned} \tag{2.16}$$

The most that E can learn is the very quantum state $|\psi(m)\rangle$ (although, as proven above, even that is impossible, unless with negligible probability). Nevertheless, without knowing the secret key, this information is not enough for E to infer the message encrypted by B. This is a simple consequence of the fact that for each allowed encryption state, there exists a suitably chosen secret key that can decrypt *any* message m. Indeed, a state $|\psi(m)\rangle$ that for the secret key $SK = (\hat{U}_k, t, l)$ corresponds to the message m, for the secret key $SK' = (\hat{U}_k, t, l - \Delta l)$ corresponds to the message $m + \Delta l$ (below, the subscripts SK and SK' explicitly denote the secret key used to encrypt the corresponding messages m

and $m + \Delta l$, respectively):

$$\begin{aligned} |\psi(m)\rangle_{SK} &= (\hat{T}_m \otimes \hat{I}_c)\,|\psi_{PK}\rangle = (\hat{T}_m \otimes \hat{I}_c)\hat{U}_k^t\,|l\rangle\,|s\rangle \\ &= (\hat{T}_m \otimes \hat{I}_c)\hat{U}_k^t(\hat{T}_{\Delta l} \otimes \hat{I}_c)\,|l - \Delta l\rangle\,|s\rangle \\ &= (\hat{T}_m \otimes \hat{I}_c)(\hat{T}_{\Delta l} \otimes \hat{I}_c)\hat{U}_k^t\,|l - \Delta l\rangle\,|s\rangle \\ &= (\hat{T}_{m+\Delta l} \otimes \hat{I}_c)\hat{U}_k^t\,|l - \Delta l\rangle\,|s\rangle \\ &= |\psi(m + \Delta l)\rangle_{SK'}\,. \end{aligned} \tag{2.17}$$

2.3 Efficiency of the protocol

In this section we show the efficiency of the proposed protocol, i.e. that the overall time τ required for its execution (public-key generation, message encryption and message decryption) scales polynomially with the length n of the message.

The public-key generation, as well as the message decryption are efficient procedures, since performing the respective QWs is efficient. Indeed, denoting by $\Delta\tau_w$ the time required for a single step $\hat{U}$ of the walk, the full walk $\hat{U}^t$ is completed in time $\tau = t \cdot \Delta\tau_w$. In the previous section we took $t \approx poly(n)$ for security purposes, a choice which is also adequate for the efficiency of the QW: the time required to perform the walk is polynomial in n.

In addition to this, for the overall protocol to be efficient, the message encryption, given by the translation operator $\hat{T}_m$, has to be efficient as well. It might seem at first that the encryption of the message is not efficient, as it requires $\boldsymbol{O}(2^n)$ single-position translations, $\hat{T}_m = (\hat{T}_1)^m$. Below, we show that this is not necessarily a non-efficient procedure, i.e., various practical implementations of $\hat{T}_m$ are indeed efficient.

In case the system that performs the QW consists of $n+1$ qubits (n carrying the position of the walker plus the coin one), such that the states of the computational basis encode different positions (see for example [**?**]), the translation operator $\hat{T}_m$ is nothing but the addition by m, which is an efficient operation in a quantum computer. Alternatively, in those cases of physical realisations in which different position states $|i\rangle$ are given by distinct spatial positions (see for example implementations based on integrated photonics[**?**]), B can simply relabel the positions on the device that carries the quantum state of the public key, i.e. $i \to i - m$, which is also efficient, as he can do it in parallel at the same time for all the position states.

2.4 Conclusions

We presented a quantum public-key cryptographic system based on QWs. Unlike a recent similar protocol [**?**], which uses single-qubit rotations to generate the public key, in our scheme the execution of a QW, in general, results in entangled quantum states as public keys, thus increasing the practical security (an eavesdropper has to, in general, perform more complex operations to extract information from entangled rather than from product states). Using Holevo's theorem, we proved the protocol's security. We also analysed the complexity of our public-key generation and message encryption/ decryption procedures and showed their efficiency, i.e., the complexity of our protocol scales polynomially with the size of the message.

In the next chapter, we will use QWs to design QKD protocols. However, we should mention here that the applications of QWs in cryptography are not yet exhausted. A relevant path of future research would be to design other kinds of security protocols based on QWs, such as oblivious transfer (along the lines of the protocol proposed in [**?**]) and commitment schemes, as well as privacy functionalities, like message authentication and quantum digital signatures.

Chapter 3

Quantum key distribution based on quantum walks

In this chapter, we present three new QKD protocols based on QWs. In particular, in Section 3.1, we propose a secure two-way QKD scheme based on QWs, which is a modification of the public-key cryptosystem that was presented in the previous chapter. We equip this protocol with two different verification procedures against full man-in-the-middle attacks. In Section 3.2, we introduce a one-way QKD protocol of the BB84 type, which we prove to be secure against general attacks, by reducing it to an equivalent entanglement-based protocol. We also provide numerical results for the optimal choice of the QW parameters that maximise its noise tolerance. In Section 3.3 we provide a semi-quantum key distribution (SQKD) protocol and show its robustness against eavesdropping. We comment on the efficiency and the quantum memory requirements for all these protocols and in Section 3.4, we discuss some possible practical attacks. In the last section, we summarise our results and suggest relevant directions of future work.

*The work presented in this chapter corresponds to the work published in [**?**].

3.1 Two-way quantum key distribution protocol

In this section, we revisit the QW public-key cryptosystem presented in Chapter 2, in order to construct a secure two-way QKD protocol. We suitably modify it, so that the quantum state generated by means of a QW encodes a key instead of a message; such a key could be used later as input to a one-time-pad encryption system. However, this modification is non-trivial and requires care, since we can no longer rely on the existence of a trusted mechanism for public-key delivery (a public-key infrastructure, for instance), as it is typically assumed in quantum public-key cryptography [**? ?**]. Our motivation for modifying the original public-key protocol is the fact that QKD schemes are quite flexible, as the key can be used by both A and B to send or authenticate messages. Also, more post-processing techniques (e. g. privacy amplification) can be applied, since we have as input a random string and not a plaintext message. In the latter case, we should be careful during the post-processing not to degrade the message (we are left with less techniques). Furthermore, in the case of information leakage, we can safely abort the protocol, while during message transmission it would be late for that. Our two-way protocol is depicted in Figure 3.1 and presented below. We assume that the key can be chosen among P possible keys. We also assume that the QW can be chosen from a prefixed discrete set known by both parties.

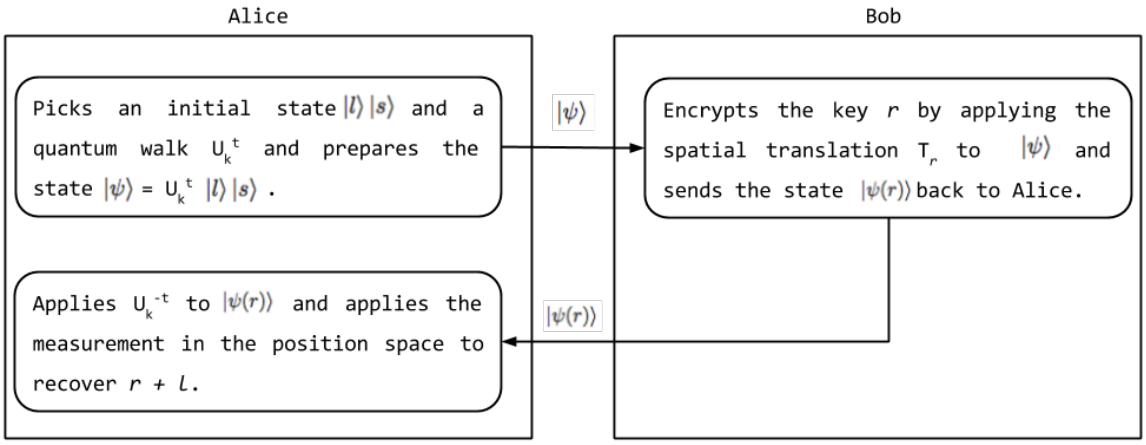

Figure 3.1: Description of the basic steps of Protocol 2.

Protocol 2. *Quantum key-distribution scheme*

Inputs for the protocol

- *Key:*

  $r \in \{0, \ldots, P-1\}$, *i.e., a key of at most* $\log P$ *bits, chosen by* B *uniformly at random;*

- *Quantum state generation:*

  The QW operator U_k *with* $k \in \mathcal{K} = \{1, 2, \ldots, K\}$, *the number of steps* $t \in \mathcal{T} = \{T_0, \ldots, T_{max}\} \subset \mathbb{N}$, *and the initial state* $|l\rangle \otimes |s\rangle$, *where* $l \in \{0, \ldots, P-1\}$, $s \in \{R, L\}$.

In the above, U_k, *the QW operator is defined as* $U_k = S \cdot (I_p \otimes R_c(\theta_k))$, *where* S *is the shift operator and* $R_c(\theta_k)$ *is a rotation of* $\theta_k = k \cdot 2\pi/K$ *in the coin space.*

Quantum state generation

- A *chooses uniformly at random* $l \in \{0, \ldots, P-1\}$ *and* $s \in \{R, L\}$, *and generates the initial state* $|l\rangle\,|s\rangle$.
- *Then she chooses, also at random, the QW* $U_k = S \cdot \big(I_p \otimes R_c(\theta_k)\big)$ *and the number of steps* $t \in \mathcal{T}$.
- *Finally, she generates the quantum state:*

$$|\psi\rangle = U_k^t\,|l\rangle\,|s\rangle = \left[S \cdot \big(I_p \otimes R_c(\theta_k)\big)\right]^t |l\rangle\,|s\rangle\,,$$

  and sends it to B.

Key encryption

- *Upon obtaining the quantum state* $|\psi\rangle$ *from* A, B *encrypts the key* r *by applying spatial translation* $T_r = \sum_{i=0}^{P-1} |i + r \pmod P\rangle\langle i|$ *to obtain:*

$$|\psi(r)\rangle = (T_r \otimes I_c)\,|\psi\rangle\,,$$

  where I_c *is the identity operator in the coin space.*

- B *sends* $|\psi(r)\rangle$ *to* A.

Key decryption

- *A applies* U_k^{-t} *to the state* $|\psi(r)\rangle$.
- *She performs the position measurement*

$$M = \sum_{i=0}^{P-1} |i\rangle \langle i| \otimes I_c$$

and obtains the result i_0.
The key sent by B *is* $r = i_0 - l \pmod P$.

It is clear, from the design of the protocol and the proof of correctness of the QW public-key encryption scheme from Chapter 2 that, if no one interferes with the quantum states, then the protocol is correct and at the end, A and B will share a common string of length $\log P$, that they can use as a key. In the next section we prove the security of the protocol.

3.1.1 Security of the protocol

Following the same steps as in Section 2.2 of Chapter 2, we can use the Holevo theorem to show that E can extract information about the key, by means of the quantum states $|\psi\rangle$ and $|\psi(r)\rangle$ that A and B exchange, only with negligible probability. However, this is not enough for the case of this QKD protocol. In the previous public-key cryptosystem, we have silently assumed the existence of a public-key infrastructure, that operates like a trusted third party, as it is usually assumed in public-key cryptography. In QKD though, such an assumption can not be used, therefore we should complete the security analysis, by taking into account full man-in-the-middle attacks. During such an attack, E impersonates A to B and vice versa, while they think that they are communicating directly. This attack gives E the chance to intercept and alter the communication between them. In what follows, we propose two different verification procedures, that allow A and B to verify that what they receive is actually coming from each other and not from an eavesdropper pretending to be either of them. We should note that for both verification methods, A and B need to share a classical public authenticated channel (a common requirement in QKD protocols, such as the well-known BB84 scheme [**?**]).

Standard verification

The first technique we propose is a standard cut-and-choose verification, which is achieved by adding redundancy to our scheme. Clearly, the verification is needed twice in our protocol: once when A sends the QW state to B and once when B sends the encoded key to A.

Verification 1: *B verifies that it was A who sent him the quantum state.*
It is needed to prevent E from sending her choice of quantum states to B, which would allow her to read the encrypted key while he is sending it back to A.

- A sends to B $\bigotimes_{i=1}^{m} |\psi_i\rangle$, that is, several quantum states $|\psi_i\rangle$, generated by a QW as described in the previous section. Each $|\psi_i\rangle$ is generated using independently chosen walk parameters and initial states (k_i, t_i, l_i, s_i).

- After B receiving $\bigotimes_{i=1}^{m} |\psi_i\rangle$, A, through a classical authenticated channel, sends him a string $v = v_1 v_2 \dots v_m$ of m bits, such that $v_i = 1$ if the corresponding $|\psi_i\rangle$ is going to be used for verification and $v_i = 0$ otherwise, that is, if the corresponding $|\psi_i\rangle$ will be used by B to encode part of the key. Through the classical channel, she also sends (j, k_j, t_j, l_j, s_j), for some uniformly at random chosen j's that belong in the set $\{1, \dots, m\}$. Let the number of these j's be $m/3$.

- B verifies that for all these j's, the received states $\rho_j = |\psi_j\rangle \langle\psi_j|$ are indeed equal to the pure states

$$|\psi_j\rangle = U_{k_j}^{t_j} |l_j\rangle |s_j\rangle .$$

  In order to verify that, he applies $U_{k_j}^{-t_j}$ to the states $|\psi_j\rangle$, for all j and then performs a measurement for each j in the positions space as well as in the spin space. This measurement (for each j) is described by the operator:

$$\begin{aligned} M_{l_j,s_j} &= \sum_{l_j,s_j} \alpha_{l_j,s_j} |l_j, s_j\rangle \langle l_j, s_j| \\ &= \sum_{l_j} l_j |l_j\rangle \langle l_j| \otimes \sum_{s_j} s_j |s_j\rangle \langle s_j| . \end{aligned}$$

  This way, he traces out all these $|\psi_j\rangle$'s and he is left with $2m/3$ quantum states. We call the reader's attention to the fact that if the verification fails for any j, the protocol is stopped.

Verification 2: *A verifies that it was B who sent her the encrypted key.*
This procedure is needed to prevent E from sending to A a message that would decrypt a key different from the one sent by B. In this case, A and B would not be able to communicate, while E would be able to decrypt messages sent by A. To prevent this from happening, A and B repeat the verification procedure 1, with the roles switched. In particular, the two are performing the following steps:

- B encrypts $r_i \in \{0, \dots, P-1\}$ in each of the states of the remaining product state

$\bigotimes_{i=1}^{2m/3} |\psi_i\rangle$ as follows:

$$|\psi(r_i)\rangle = (T_{r_i} \otimes I_c) |\psi_i\rangle \, , \forall i \in \{1, \ldots, 2m/3\}$$

that is, translating each state $|\psi_i\rangle$ by r_i in the positions space, leaving the spin part of the state unaltered.

- He sends the product state $\bigotimes_{i=1}^{2m/3} |\psi(r_i)\rangle$ to A.

- Then he chooses $m/3$ uniformly at random j''s out of the $2m/3$ unused indices from the previous verification procedure. Through the classical public authenticated channel he sends a classical string $v' = v'_1 v'_2 \ldots v'_{2m/3}$ of $2m/3$ bits, such that $v'_i = 1$ if the corresponding $|\psi(r_i)\rangle$ is going to be used for verification and $v'_i = 0$ otherwise, that is, if the corresponding $|\psi(r_i)\rangle$ contains part of the key. For each j' chosen (for which $v'_i = 1$), he also sends through the classical public authenticated channel the index and the respective $r_{j'}$'s used to generate the state $|\psi(r_i)\rangle$.

- In the last step, A applies $U_{k_i}^{-t_i}$ on the $2m/3$ states $|\psi(r_i)\rangle$ and then, for each i, she performs a measurement on the positions space. Let the outcomes be denoted by $\alpha_i, i \in \{1, \ldots, 2m/3\}$. For all the indices she computes $r_i = \alpha_i - l_i$, where l_i are the initial positions on the circle that she used for the generation of the quantum states $|\psi_i\rangle$. Finally, for each $j', r_{j'}$ sent by B, A verifies the consistency of their results.

- The key is given by the concatenation of the bits r_i that were not used during the two verification procedures and it has $m \cdot (\log P)/3$ bits. Usually, the choice of m is dependent on the desired length, $\log P$, of the key, and in order to make the success probability of a man-in-the-middle attack negligible on $\log P$, it is common to use $m = (\log P)/3$.

Verification using maximally entangled states

In this section, we present an alternative verification procedure, which prevents E from trying to infer the key by first entangling her ancillas with the systems sent by A, and then performing an additional operation (say, a measurement) on the joint system of her ancillas and those carrying the encrypted key sent back to A by B; a method which in general would give her access to some non-negligible amount of information, so that A and B are not able to securely communicate. Note that this verification procedure could also be used against the previous attack in which E simply impersonates A to B, and vice versa.

During the first step of the protocol ("Quantum state generation"), in addition to generating QW states

$$|\psi\rangle_{qw} = U_k^t |l\rangle |s\rangle \tag{3.1}$$

used to encode the key, for the verification purposes A also creates a number of Bell-like maximally entangled states

$$|\psi\rangle_{qw} = \frac{1}{\sqrt{(\log 2P)!}} \sum_{i=0}^{2P-1} |i\rangle_a |i\rangle_{qw} . \tag{3.2}$$

between the ancilla systems (denoted by a) and the QW systems (denoted by qw), each of dimension $2P$ (the dimension of the actual QW). At the end of the first step, A sends to B a random sequence of QW states, each either in the form $|\psi\rangle_{qw}$, or $\rho_{qw} = \mathrm{tr}_a |\psi\rangle \langle\psi|_{qw}$, while keeping the ancillas with her. A also sends through a classical public authenticated channel a classical string $v = v_1 \dots v_n$, where $v_i = 0$ if the i-th system is going to be used for the encoding of the key, while $v_i = 1$ if the i-th system is going to be used for verification.

The proportion of states used to obtain the key and used for the verification can be chosen in a similar way as in the previous case. Usually, the dimension of the total Hilbert space $2P$ is of the form 2^n which, in turn, is isomorphic to the Hilbert space resulting from the tensor product of n 2-dimensional Hilbert spaces, and thus this state can be written as the tensor product of n standard two-qubit $|\phi^+\rangle$ Bell states.

After B receives the systems, he and A perform Bell-like measurements on the states meant for the verification and they observe a maximal violation of the Bell's inequalities, since those states are maximally entangled. This way, these states are traced out and B is left with the states (3.1) in which he will encode the key (as previously).

The same procedure is repeated again, when B sends the encoded key to A. He will send a sequence of states, some of the form $(\hat{T}_r \otimes \hat{I}_c) U_k^t |l\rangle |s\rangle$, in which part of the key is encoded and some of the form (4) (with his ancillary system $|i\rangle_B$ maximally entangled to the system sent to A), which are going to be used for the verification, as explained above. In the end of the key decryption phase and if all the verifications were okay, A will concatenate the parts of the key to obtain the full key.

3.1.2 Efficiency and quantum memory requirements

In Section 2.3 of Chapter 2 we showed that the QW public-key protocol is efficient, i.e., it requires only polynomial time (on the length of the message, say n) to transfer n bits of information encoded in $n+1$ qubits. By introducing the verification steps in this QKD scheme we increase the complexity of the system to n^2, in order to make the probability

of eavesdropping negligible. However, we should notice that, out of this scheme, the size of the key that A and B share at the end is also increased to $n^2/3$, considering $m = n$. Therefore, the number of bits in the key is linear in the number of qubits sent to B. As a conclusion, our QKD scheme is efficient, since the complexity increased, but only polynomially.

As already mentioned in Chapter 1, the lack of stable quantum memories is a major issue in quantum cryptography, since it is a practical constraint that is not likely to be solved, at least in the near future. Short-term quantum memories already exist, however it is not always straightforward to argue about the security of a protocol, relying on their existence. In our case, though, things are quite clear. If E does not interfere, A and B do not need quantum memories to execute the protocol, thus the key distribution is independent of such practical constraints. However, the presence of E and the need of verification for A and B introduce memory requirements for *all* the parties.

Below, we present the memory requirements for the case of Section 3.1.1, noting that the case of Section 3.1.1 is analogous. To conduct her attack, E needs a stable quantum memory, in order to keep the states she intercepted by A, while waiting for B to encrypt and send the key. Subsequently, she will encode it in A's states and send it to her. Also, in this scenario, A and B need a quantum memory, in order to perform the verification. They need to save the quantum states for some time, while waiting for the other party to send the classical information. Observe that E's memory should be more stable than A's and B's, as the time E needs to save the quantum states for, is clearly longer than the time that A and B need for the same purpose.

Hence, we conclude that our QKD scheme is secure, as long as A and B have at least as powerful equipment as the adversary E. Obviously, if the adversary is technologically more advanced, then virtually any real-life implementation of a security protocol becomes potentially vulnerable.

3.2 One-way quantum key distribution protocol

In this section, we propose a one-way QKD protocol, where again the key is encoded in a QW state. As opposite to the previous two-way protocol, where both A and B perform QW operations, in this case it is only A that chooses randomly the precise QW to encode the key, while B is randomly choosing in which basis (computational or QW) to measure. After disclosing their choices by means of classical communication, they are able to establish a shared key. We will first present the protocol in its PM form and then we will prove its security against general attacks by considering an equivalent EB protocol. The PM form of the protocol is depicted in Figure 3.2.

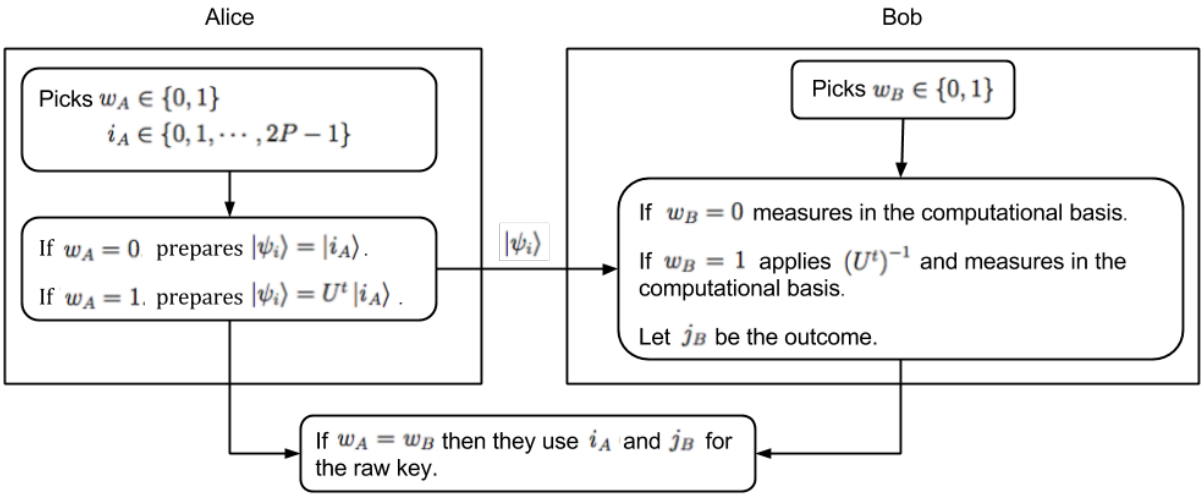

Figure 3.2: Description of the basic steps of Protocol 3.

Protocol 3. *Let θ_k, t, and P be publicly known where P is the dimension of the position space of the QW, t is the number of steps to perform the QW, and θ_k the coin parameter (see Section 2.2 for the exact form of θ_k). Let U_k be the QW operator $U_k = S \cdot (I_p \otimes R_c(\theta_k))$ that is also known by the parties (i.e., it is also publicly known) and let F be an operator acting only on $\mathcal{H}_c$. F's action is to "flip" the coin to some initial state before evolving the walk and is optional (in which case $F = I_c$). Finally, let $|\psi_i\rangle = U_k^t (I_p \otimes F) |i\rangle$ for $|i\rangle \in \mathcal{H}_p \otimes \mathcal{H}_c$. We call the orthonormal basis $\{|\psi_i\rangle\}$ the QW basis and denote the computational basis by Z.*

The protocol consists of N iterations of the following steps:

1. *A picks a random bit $w_A \in \{0,1\}$ and a value $i_A \in \{0,1,\cdots,2P-1\}$.*
   - *If $w_A = 0$: A will prepare and send to B the $2P$-dimensional state $|\psi_i\rangle = |i_A\rangle$.*
   - *If $w_A = 1$: A will prepare and send to B the $2P$-dimensional state $|\psi_i\rangle = U_k^t (I_p \otimes F) |i_A\rangle$.*
2. *B picks a random bit $w_B \in \{0,1\}$.*
   - *If $w_B = 0$: B measures the received $2P$ dimensional state in the computational Z basis resulting in outcome j_B.*
   - *If $w_B = 1$: B measures in the QW basis (alternatively, he inverts the QW by applying $(U_k^t)^{-1}$ and measures the resulting state in the Z basis). The result is translated, in the obvious way, into an integer j_B.*

Note that he measures both the position and coin, as opposite to the previous protocol, where the measurement for the key was only on the positions space.

3. *A and B reveal, via the authenticated classical channel, their choice of w_A and w_B. If $w_A = w_B$, they will use their values i_A and j_B to contribute towards their raw key. Otherwise, if $w_A \neq w_B$, they will discard this iteration.*

*After the above process, A and B will use a cut-and-choose technique similar to Yao's [**?**], to check eavesdropping by choosing a suitable subset of non-discarded iterations for parameter estimation in the usual manner (discarding those chosen iterations from the raw key). This allows them to estimate the disturbance Q_Z and Q_W in the Z and QW bases respectively (i.e., in the absence of noise $Q_Z = Q_W = 0$). If this disturbance is "sufficiently low" (to be discussed below) the users proceed with error correction and privacy amplification in the usual manner.*

3.2.1 Security of the protocol

In order to prove the security of Protocol 3, we will construct, in the usual way, an equivalent EB protocol [**?** **?**]. Proving security of this EB protocol will show the security of the PM version. For this EB version, for each one of the N iterations, we make changes to steps (1) and (2), replacing them as follows:

New Step (1): A prepares the entangled state:

$$|\phi_0\rangle = \frac{1}{\sqrt{2P}} \sum_{i=0}^{2P-1} |i,i\rangle_{AB}$$

which lives in the $4P^2$ dimensional Hilbert space: $(\mathcal{H}_p \otimes \mathcal{H}_c)^{\otimes 2}$. She sends the second half (the B portion of $|\phi_0\rangle$) to B while keeping the first half (the A portion) in her private lab.

New Step (2): A and B choose independently two random bits w_A and w_B. If $w_A = 0$, A will measure her half of the entangled state in the computational Z basis; otherwise she will measure her half in the QW basis. Similarly for B and w_B. Let their measurement results in values be i_A on A's side and j_B on B's side.

We now show the security of this entanglement-based version of the protocol. In the following proof, we will initially make three assumptions:

A1: A and B only use those iterations where $w_A = w_B = 0$ for their raw key.

A2: E is restricted to collective attacks (those whereby she attacks each iteration of the protocol independently and identically, but is free to perform a joint measurement of her ancilla at any future time of her choosing).

A3: E is the party that actually prepares the states which A and B hold.

Assumption A1 is made only to simplify the computation and may be discarded later (alternatively, one may bias the basis choice so that w_A and w_B are chosen to be 0 with high probability, thus increasing the efficiency of the protocol as is done for instance for BB84 in [**?**]). Assumption A2 may be removed later using a de Finetti-type argument [**? ? ?**] (in this paper, we are only concerned with the asymptotic scenario, so the key-rate expression we derive will not be degraded). Note that removing A2 gives us the security. Assumption A3 gives greater advantage to the adversary; if we prove security using A3, then the "real-world" case, where assumption A3 is not used, will certainly be just as secure, if not even more.

In light of A2 and A3, A, B, and E, after N iterations of the protocol, hold a quantum state $\rho_{ABE}^{\otimes N}$, where $\rho_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ with $\mathcal{H}_A \equiv \mathcal{H}_B \equiv \mathcal{H}_p \otimes \mathcal{H}_c$. Following error correction and privacy amplification, A and B will hold a secret key of size $\ell(N)$. Under the assumption of collective attacks (A2), we may use the Devetak-Winter key-rate expression [**?**] to compute:

$$r = \lim_{N\to\infty} \frac{\ell(N)}{N} = S(A|E) - H(A|B).$$

Let A_Z and A_W be the random variables describing A's system, when she measures in the Z or QW basis, respectively. Similarly, define B_Z and B_W. Under assumption A1, we are actually interested in the value:

$$r = S(A_Z|E) - H(A_Z|B_Z).$$

Computing $H(A_Z|B_Z)$ is trivial, given the observable probabilities:

$$p_{i,j}^Z = Pr(i_A = i \text{ and } j_B = j \mid w_A = w_B = 0). \tag{3.3}$$

The challenge is to determine a bound on the von Neumann entropy $S(A_Z|E)$.

To do so, we will use an uncertainty relation, proven in [**?**], which states that for any density operator σ_{ABE} acting on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$, if A and B make measurements using POVMs $\mathcal{M}_0 = \left\{M_x^{(0)}\right\}_x$ or $\mathcal{M}_1 = \left\{M_x^{(1)}\right\}_x$, then

$$S(A_0|E) + H(A_1|B) \geq \log \frac{1}{c}, \tag{3.4}$$

where

$$c = \max_{x,y} \left|\left| M_x^{(0)} M_y^{(1)} \right|\right|_\infty^2 \tag{3.5}$$

where we take $||\cdot||_\infty$ to be the operator norm and A_i to be the random variable describing A's system after measuring $\mathcal{M}_i$ (we will later, similarly, define B_i). Assuming measurements $\mathcal{M}_0$ are used for key distillation, simple algebra, as discussed in [**?**], yields the Devetak-Winter key-rate:

$$\begin{aligned} r = S(A_0|E) - H(A_0|B_0) &\geq \log \frac{1}{c} - H(A_0|B_0) - H(A_1|B) \\ &\geq \log \frac{1}{c} - H(A_0|B_0) - H(A_1|B_1). \end{aligned}$$

The last inequality follows from the basic fact that measurements can only increase entropy.

In our case, we have $M_x^{(0)} = |x\rangle\langle x|$ and $M_x^{(1)} = |\psi_x\rangle\langle\psi_x|$ for $x \in \{0, 1, \cdots, 2P-1\}$. Let $|\psi_x\rangle = \sum_{i=0}^{2P-1} \alpha_{x,i} |i\rangle$; then it is easy to see that for all x, y

$$\left|\left| M_x^{(0)} M_y^{(1)} \right|\right|_\infty^2 = |\alpha_{y,x}|^2,$$

and therefore

$$c = \max_{x,y} |\alpha_{x,y}|^2, \tag{3.6}$$

a quantity which depends exclusively on the choice of the QW parameters and not on the noise in the channel. Therefore, A and B should choose optimal t, θ_k and P in order to minimise c (thereby maximising the key-rate equation). As we will show in the next section, this analysis is sufficient to derive good key-rate bounds.

3.2.2 Evaluation

As mentioned above, the value of c depends solely on the QW parameters which are under A and B's control; therefore it is to their advantage to choose a QW which minimises this value (i.e., such that, after evolving for t steps, the probability of finding the walker at any particular position is small).

It is easy to see that, as $t \to \infty$, the values $|\alpha_{x,y}|$ do not converge to a steady state which is why, usually, one considers the time-averaged distribution when analysing QWs on the cycle [**?** **?**].

However, in our QKD protocol, we do not care what happens at large t; instead, we wish to find an optimal t and one that is preferably not "too large" (the larger it is, the longer, in general, it might take A to prepare the state and B to reverse it).

We begin by looking at various walk parameters and finding the minimal value of c when $F = I_c$, the identity operator. Note that, on the circle, it makes sense only to consider odd P as even P would force the support of the probability amplitudes onto even or odd numbered nodes only thereby increasing the overall value of $|\alpha_{x,y}|$. We wrote a computer program to simulate the walk for time steps $t = 1, 2, \cdots, T_{\max}$ (for user-specified value $T_{\max}$) searching for the optimal value of t (i.e., a value for t whereby c is minimum). For the evaluation we used a more general form of the coin rotation operator:

$$R_c(\theta, \phi) = \begin{pmatrix} e^{i\phi}\cos(\theta) & e^{i\phi}\sin(\theta) \\ -e^{-i\phi}\sin(\theta) & e^{-i\phi}\cos(\theta) \end{pmatrix},$$

The results for $\theta = \pi/4, \phi = 0$, and for various P are shown in Figure 3.3.

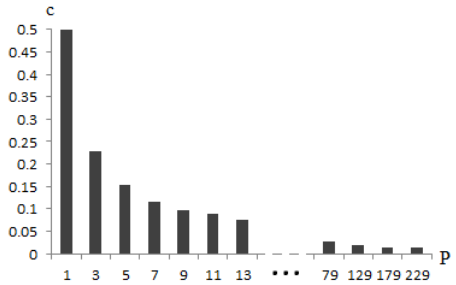

Figure 3.3: Showing minimal value of c found by our program for given position space dimension P when $\theta = \pi/4, \phi = 0$ and $F = I_c$. When $P \leq 13$ we set $T_{\max} = 5000$; when $P \geq 79$ we set $T_{\max} = 50000$. Note that, the smaller c is, the better for A and B. Note also that P is the dimension of the position space, *not* the number of qubits sent which would actually be $\lceil \log P \rceil + 1$ (where the extra "+1" is due to the coin).

Now that we can find the optimal choice of QW parameters for particular values of P and, more importantly for our work here, the resulting value of c. To this end, we have to compute our bound r and determine for what noise levels we can have $r > 0$. In practice, one would observe values $p^Z_{i,j}$ and $p^W_{i,j}$ (see Equation (3.3) and define $p^W_{i,j}$ analogously) and use these to directly compute $H(A_Z|B_Z)$ and $H(A_W|B_W)$ as required by the key-rate equation. For the purpose of illustration in this paper, however, we will evaluate our key-rate bound assuming a generalised Pauli channel as discussed in [**?**] (see, in particular, Section 7 of that source). This channel maps an input state ρ to an output state $\mathcal{E}(\rho)$ defined as:

$$\mathcal{E}(\rho) = \sum_{m=0}^{2P-1} \sum_{n=0}^{2P-1} p_{m,n}\, \mathcal{U}_{m,n}\, \rho\, \mathcal{U}^*_{m,n}, \tag{3.7}$$

where:

$$\mathcal{U}_{m,n} = \sum_{k=0}^{2P-1} e^{\pi \cdot i \cdot k \cdot n/P}\, |k+m\rangle \langle k|\,, \tag{3.8}$$

That is, this channel $\mathcal{E}(\cdot)$ models an adversary's attack which induces phase and flip errors with probabilities denoted by $p_{m,n}$. In our numerical computations to follow, we will use:

$$p_{i,j} = \begin{cases} 1 - E_r & \text{if } i = j = 0 \\ \\ \dfrac{E_r}{(2P)^2 - 1} & \text{otherwise} \end{cases} . \tag{3.9}$$

It is clear that $\sum_{i,j} p_{i,j} = 1$. Furthermore, when $E_r = 0$, we have $\sum_i p^Z_{i,i} = \sum_i p^W_{i,i} = 1$ (i.e., there is no disturbance in the channel) while as E_r increases, the disturbance also increases.

Finally, we define the total noise in the channel to be:

$$Q = \sum_{a \neq b} p^Z_{a,b} = \sum_{a \neq b} Pr\big(A_Z = a \text{ and } B_Z = b \mid w_A = w_B = 0\big).$$

That is to say, Q represents the quantum error rate (QER) of the channel.

The maximally tolerated QER, for those QWs analysed in Figure 3.3, and using the above described noise model, is shown in Figure 3.4. Note that, when $P = 1$ and $t = 1$, we recover the BB84 limit of 11% which is to be expected since, with these choice of parameters, we are essentially running the BB84 protocol. Observe in Figure 3.4 that

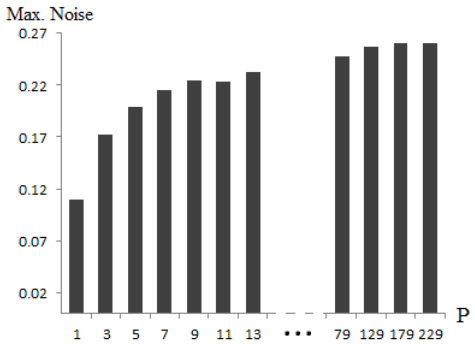

Figure 3.4: Showing the maximally tolerated noise level for our protocol using parameters found in Figure 3.3 and using the quantum channel described by Equations (3.7) and (3.9). The lack of increase in noise tolerance from $P = 9$ to $P = 11$ (while other choices caused an increase) indicates that $T_{\max}$ was too low. Note that, when $P = 1$, we recover the BB84 tolerance of $Q = 0.11$ as expected. Also note that, when $P = 229$, the maximal tolerated noise is $Q = 0.261$.

there is a lack of increase when $P = 9$ and $P = 11$; this indicates that our choice of $T_{\max} = 5000$ was too low. Running our simulator again with $T_{\max} = 50000$ for these small P values yields a maximally tolerated noise level shown in Figure 3.5.

Finally, we re-run the simulator, using $T_{\max} = 5000$ and $T_{\max} = 50000$ for a different

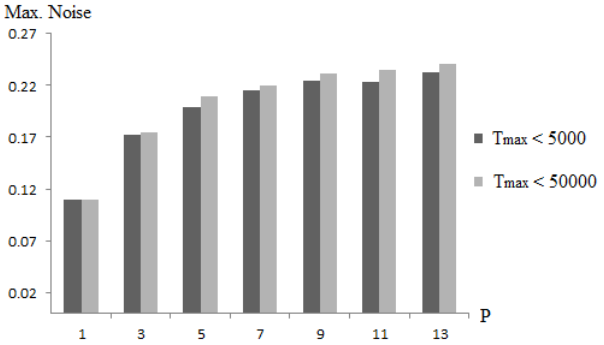

Figure 3.5: Comparing the maximally tolerated noise when t is allowed to be as large as 50000 (light gray) or only 5000 (dark grey); again when $F = I$ and $\phi = 0$. In this case, when $P = 13$ and $T_{\max} = 50000$, the maximal tolerated noise Q is $Q = 0.241$.

QW parameter of $\theta = \sqrt{2}\pi/4$ which, for these particular upper-bounds on t yield a higher tolerated noise as shown in Figures 3.6 and3.7. We comment that, if $T_{\max}$ were larger, the two QWs may produce a QKD protocol with the same tolerated noise; however for these "smaller" bounds on t the QW with parameter $\theta = \sqrt{2}\pi/4$ produces a more secure protocol than when $\theta = \pi/4$. Since smaller t implies a more efficient protocol, this is an advantage. This opens two very interesting questions: first, do these QWs produce equivalent noise tolerances as $T_{\max} \to \infty$? Second, what other values of θ produce even more secure QKD protocols for small $T_{\max}$? We comment that we also ran this numerical experiment for $\theta = \pi/5$ and $\theta = \pi/3$ but got worse noise tolerances.

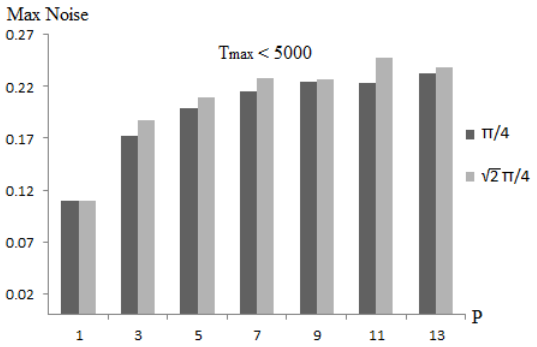

Figure 3.6: Comparing the maximal tolerated noise levels of the QKD protocol when $\theta = \pi/4$ (dark gray) and $\theta = \sqrt{2}\pi/4$ (light grey). In this chart, $T_{\max} = 5000$ which, observing the "drop" in tolerated noise when P goes from 11 to 13, is too small. See also Figure 3.7 for the same chart when $T_{\max} = 50000$.

From the above it is clear that careful choice of the QW parameters is vital for producing a QKD protocol tolerant of high noise channels. To investigate this further, we simulate the QW for all $\theta, \phi \in \{k\pi/10 \mid k = 0, 1, \cdots, 10\}$. Furthermore, for each setting,

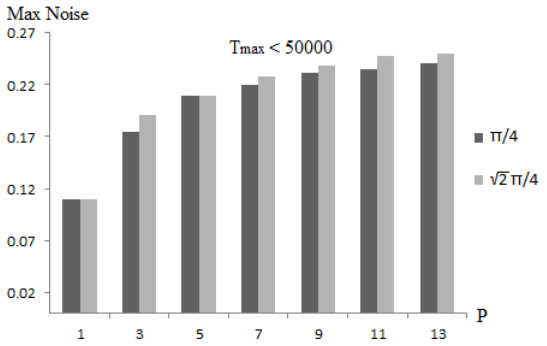

Figure 3.7: Comparing the maximal tolerated noise levels of the QKD protocol when $\theta = \pi/4$ (dark gray) and $\theta = \sqrt{2}\pi/4$ (light grey). In this chart, $T_{\max} = 50000$. In all cases, the QW parameter $\theta = \sqrt{2}\pi/4$ produces a more secure QKD protocol for this upper-bound on t. Note that, as $T_{\max} \to \infty$, they may produce equally secure protocols; this, as discussed in the text, is an open question. In this case, when $P = 13$ and $\theta = \sqrt{2}\pi/4$, the maximally tolerated noise is 0.25 (compared to 0.241 when $\theta = \pi/4$).

we also consider the use of $F = I, F = X$, and $F = Y$, where:

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad Y = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}.$$

For each setting, we find the optimal choice of time $t \leq 5000$ which produces a minimal c. We then take this value and determine the highest disturbance the resulting protocol can withstand. The respective data is summarised in Table 3.1.

	$F = I$					$F = X$					$F = Y$				
P	θ	ϕ	t	c	$Q_{\max}$	θ	ϕ	t	c	$Q_{\max}$	θ	ϕ	t	c	$Q_{\max}$
3	0.4π	0.2π	4584	0.171	0.220	0.8π	0.8π	3994	0.181	0.211	0.7π	0	1502	0.167	0.225
5	0.7π	π	4340	0.147	0.205	0.9π	0.5π	3870	0.132	0.22	0.3π	0	3748	0.106	0.253
7	0.6π	0.9π	3946	0.088	0.252	0.7π	0.8π	3391	0.099	0.236	0.3π	0.5π	1275	0.083	0.261
9	0.6π	0.6π	1269	0.077	0.252	0.9π	0.7π	3041	0.079	0.250	0.3π	0.5π	965	0.069	0.267
11	0.6π	0.4π	1221	0.069	0.252	0.8π	0.4π	481	0.0724	0.245	0.7π	0.5π	277	0.054	0.284

Table 3.1: Showing the optimal choice of QW parameters to maximise the noise tolerance ($Q_{\max}$) of the resulting protocol. For this data, we searched for QWs with at most $T_{\max} = 5000$ steps and with parameters $\theta, \phi \in \{k\pi/10 \mid k = 0, 1, \cdots, 10\}$.

Note that, for some data points (e.g., when $P = 5$ and $F = I$) there is a drop in the maximum tolerated noise. This is a consequence either of setting $T_{\max}$ too small, or we need to simulate more QW parameters. For example, when we set $T_{\max} = 50000$, for $P = 5$ and $F = I$, we get a maximum noise tolerance of 0.236 when $t = 40847$. Note also,

that setting $F = Y$ achieves the best result for this test, $Q_{\max} = 0.284$.

In Table 3.2, we carried out the same experiment, however this time searching over QW parameters in the set $\theta, \phi \in \{k\pi/20 \mid k = 0, 1, \cdots, 20\}$. Again, the best result for this case is $Q_{\max} = 0.284$ and is achieved when considering $F = Y$.

	$F = I$					$F = X$					$F = Y$				
P	θ	ϕ	t	c	$Q_{\max}$	θ	ϕ	t	c	$Q_{\max}$	θ	ϕ	t	c	$Q_{\max}$
3	0.4π	0.2π	4584	0.171	0.220	0.25π	0.15π	2402	0.173	0.218	0.7π	0	1502	0.167	0.225
5	0.6π	0.85π	3258	0.116	0.239	0.8π	0.25π	4659	0.124	0.229	0.3π	0	3748	0.106	0.253
7	0.6π	0.9π	3946	0.088	0.252	0.05π	0.95π	3739	0.091	0.248	0.35π	0.5π	517	0.081	0.265
9	0.45π	0.95π	2531	0.075	0.257	0.85π	0.05π	1669	0.078	0.251	0.45π	0.5π	1240	0.064	0.276
11	0.55π	0.75π	1826	0.059	0.272	0.25π	0.25π	2223	0.069	0.252	0.7π	0.5π	277	0.054	0.284

Table 3.2: Showing the optimal choice of QW parameters to maximise the noise tolerance ($Q_{\max}$) of the resulting protocol. For this data, we searched for QWs with at most $T_{\max} = 5000$ steps and with parameters $\theta, \phi \in \{k\pi/20 \mid k = 0, 1, \cdots, 20\}$.

As mentioned at the beginning of this section, all the numerical results were obtained by simulating the evolution of the QW on a custom QW simulator that we wrote. However, we also verified the results through an alternative technique, namely by computing the probability amplitudes of the QW using the standard Fourier method (see, e.g. [**?** **?**]) of analysing QWs. The results obtained by both methods agree with each other.

Finally, we note that the protocol's security is not compromised by considering the existence or not of quantum memories. It is sufficient to consider the PM form of the protocol. E needs a quantum memory to perform her attack, as she needs to save her ancillary system throughout the execution of the protocol. In the contrary, the secure key distribution between A and B does not require any quantum memory. Therefore, if E does not have a quantum memory she cannot attack, while if even she has one and attacks, A and B can defend against it and securely share a key at the end. Notice, that even if we consider the EB version of the protocol, again the security is independent of any quantum memory requirements, as E for her attack needs a more stable quantum memory than A and B need to defend against it and securely distil the key.

3.3 Semi-quantum key distribution protocol

As a third contribution, in this section, we propose a new *semi-quantum* key-distribution (SQKD) protocol based on QWs. The concept of semi-quantum cryptography was introduced by Boyer *et al.* [**?** **?**], as a way to study "how quantum" does a protocol need to be in order to surpass the security of its classical counterparts – namely, how "quantum" do the parties need to be in order to establish a secret key secure against an all-powerful adversary. A semi-quantum protocol places restrictions on one of the participating users (typically B) in that he may only operate in a "classical" or "semi-quantum" manner. In particular, this limited user – usually called the *classical party* – can only directly work with the computational basis. No restrictions are placed on A, who is fully quantum, i.e., she possesses quantum equipment and can perform quantum operations and of course, no restrictions are placed on E. Implementation-wise, such protocols can be seen as practical instances of QKD, since they involve less quantum hardware. Semi-quantum protocols rely on a two-way quantum channel allowing a quantum state to travel from A to B, and then back to A. When first introduced by Boyer *et al.* in [**?**], these classical operations involved B either measuring the incoming qubit in the $Z = \{|0\rangle, |1\rangle\}$ basis, or reflecting the incoming qubit, bouncing it back to A undisturbed. For our purposes, we extend this definition of "classical" operations to operate with higher dimensional systems. As we do not want to restrict ourselves necessarily to qubit encodings (and thus, dimensions that are powers of two), we will say that B, on receipt of an D dimensional quantum state $|\psi\rangle$, may choose to do one of two operations:

1. Measure and Resend: B may subject the D-dimensional quantum state to a measurement in the computational basis spanned by states: $\{|0\rangle, |1\rangle, \cdots, |D-1\rangle\}$. He will then prepare a new D-dimensional quantum state in this same computational basis based on the result of his measurement. Namely, if he observes $|r\rangle$ for $r \in \{0, 1, \cdots, D-1\}$, he will send to A the quantum state $|r\rangle$.

2. Reflect: B may ignore the incoming D-dimensional quantum state and reflect it back to A. In this case he learns nothing about its state.

With these restrictions on the part of the classical user defined, we now depict our protocol in Figure 3.8 and describe it immediately below.

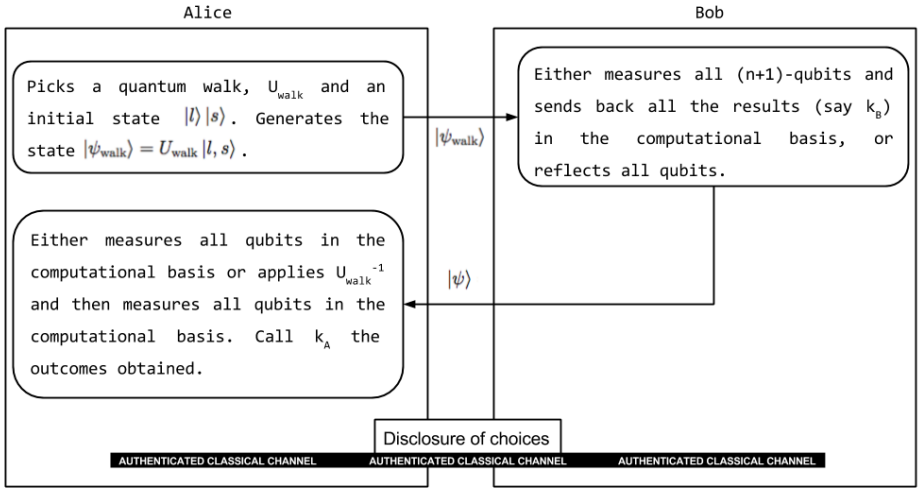

Figure 3.8: Description of the basic steps of Protocol 4.

Protocol 4. *Semi-quantum key-distribution scheme*

Inputs for the protocol

- $|l,s\rangle$, *the initial state of the QW, where* $l \in \mathcal{L} = \{0,\ldots,P-1\}$ *is the initial position of the walker, and* $s \in \mathcal{S} = \{R,L\}$ *gives the initial coin state.*
- $U_{\text{walk}} = (U_k)^t \in \mathcal{Q}$, *the evolution of the QW, where* $k \in \mathcal{K} = \{1,2,\ldots,K\}$ *is the choice of a single step unitary* U_k, *and* $t \in \mathcal{T} = \{T_0,\ldots,T_{max}\}$ *is the number of steps of the QW. Thus,* $\mathcal{Q}$ *is the set of all possible QWs. Note that* $\mathcal{Q}$ *is publicly known.*

Quantum state Generation

- *A chooses uniformly at random* $l \in \mathcal{L} = \{0,1,\cdots,P-1\}$ *and* $s \in \mathcal{S} = \{R,L\}$. *She also chooses a random QW operator* $U_{\text{walk}} \in \mathcal{Q}$ *according to a publicly known distribution (e.g., uniform). She then prepares the following state:*

$$|\psi_{\text{walk}}\rangle = U_{\text{walk}}|l,s\rangle.$$

- *A sends this state to B.*

Classical operations by B

B chooses either to measure-and-resend the quantum state in the computational basis $\{|0\rangle,|1\rangle,\cdots,|2P-1\rangle\}$ *(note that, in this protocol as well, he measures both the position and coin in order to obtain the key, thus his measurement, and subsequent preparation, is of dimension* $2P$*); or he will reflect the quantum state back to A.*

A's final step

A chooses one of the following two options:

- *She measures the returning quantum state in the computational basis and saves the result as κ_A.*
- *She first applies the inverse QW, U_{walk}^{-1}, and then measures in the computational basis. Note that, in the absence of noise, if B reflects, her measurement outcome should be $|l, s\rangle$.*

Disclosure

A discloses her choice of operation and B discloses his choice either to measure and resend or reflect.

Iterations

The above process is repeated N times.

Results

- *Every time B measures and resends and A measures in the computational basis, the parties add $1 + \log P$ bits to their final raw key.*
- *Every time B reflects and A measures after applying the inverse QW, the outcome of her measurement (l_m, s_m) should be what she initially used to generate the QW state (i.e., it should be that $l = l_m$ and $s = s_m$). These iterations, together with some randomly chosen iterations of the first type (where B measures and resends), are used for error detection.*
- *The other iterations are discarded.*

3.3.1 Proof of robustness

As with the first protocol we proposed in this section, the reliance on a two-way quantum channel greatly complicates the security analysis. It was only recently that several SQKD protocols were proven secure [**?** **?** **?** **?**]. However, the proof techniques developed in those works assumed qubit-level systems. In our case, not only must we contend with the two-way channel, but also with the fact that the quantum states traveling between A and B are of dimensions higher than 2. This leads to significant challenges in the security analysis. Therefore, as a first step, we will prove that the protocol is *robust*, as defined in [**?** **?**]. That is, for any attack which E may perform which causes her to

gain information on the raw key, this attack must necessarily lead to a disturbance in the channel which can be detected with non-zero probability by A and B.

Theorem 1. *If $I \in \mathcal{Q}$ (where I is the identity operator on the joint $2P$ dimensional system) and if, for every $(l,s),(l',s') \in \{0,1,\cdots,P-1\}\times\{R,L\}$ there exists a $U_{\text{walk}} \in \mathcal{Q}$ and initial state $|l_0,s_0\rangle$ (all possibly depending on the choice of (l,s) and (l',s')) such that $\langle l,s|U_{\text{walk}}|l_0,s_0|l,s|U_{\text{walk}}|l_0,s_0\rangle \neq 0$ and $\langle l',s'|U_{\text{walk}}|l_0,s_0|l',s'|U_{\text{walk}}|l_0,s_0\rangle \neq 0$, then the SQKD protocol based on QWs is robust.*

Proof. We will assume, similarly to [**?** **?**], that A sends each (in our case $2P$-dimensional) quantum state, only after she receives one from B (excepting, of course, the first iteration). In this case, E's most general attack consists of a collection of unitary operators $\left\{(U_F^{(i)},U_R^{(i)})\right\}_{i=1}^{N}$ where, on iteration i of the protocol, she applies $U_F^{(i)}$ in the forward channel (as the quantum state travels from A to B) and $U_R^{(i)}$ in the reverse channel. These operators act on the $2P$-dimensional quantum state and E's private quantum memory. We make no assumptions about how these operators are chosen – for instance, E may choose them "on the fly"; that is, she may choose operator $U_F^{(2)}$ after attacking with $U_F^{(1)}$.

Consider the first iteration $i=1$. We assume, without loss of generality, that E's quantum memory is cleared to some pure "zero" state, denoted by $|\chi\rangle$, known to her.

In the remainder of this proof, we will treat the position space and the coin space as a single space Σ of dimension $2P$.

We may describe the action of $U_F^{(1)}$ on basis states as follows

$$U_F^{(1)}|i,\chi\rangle = \sum_{j=0}^{2P-1} \left|j,e_i^j\right\rangle,$$

where $\left|e_i^j\right\rangle$ are arbitrary states in E's ancillary system. These states are not necessarily normalised nor orthogonal; the unitarity of $U_F^{(1)}$ imposes some restrictions on them which we will use later.

With non-zero probability, this iteration may be used for error detection. It is also possible that A chose to use $I \in \mathcal{Q}$ in this iteration and, thus, she sends the quantum state $|\sigma\rangle$ to B, for $\sigma \in \Sigma$. Furthermore, B chooses to measure and resend with non-zero probability. Therefore, to avoid detection, it must be that $\left|e_i^j\right\rangle \equiv 0$ for all $i \neq j$, and the unitarity of $U_F^{(1)}$ yields $\langle e_i^i|e_i^i|e_i^i|e_i^i\rangle = 1$ for all i. Thus:

$$U_F^{(1)}|i,\chi\rangle = \left|i,e_i^i\right\rangle, \forall i = 0,1,\cdots,2P-1.$$

Now, consider $U_R^{(1)}$, the attack applied in the reverse channel. We may write its action as

follows:

$$U_R^{(1)} \left| i, e_i^i \right\rangle = \sum_{w=0}^{2P-1} \left| w, e_{i,i}^w \right\rangle .$$

The same argument as before applies: in particular, with non-zero probability A and B will use this iteration to check for errors, and so it must be that $\left| e_{i,i}^w \right\rangle \equiv 0$ for $i \neq w$. Thus

$$U_R^{(1)} \left| i, e_i^i \right\rangle = \left| i, e_{i,i}^i \right\rangle = \left| i, f_i \right\rangle , \forall i = 0, 1, \cdots , 2P-1,$$

where we defined $\left| f_i \right\rangle \equiv \left| e_{i,i}^i \right\rangle$ for ease of notation.

Now, assume that A chooses a QW operator $U_{\text{walk}} \in \mathcal{Q}$, with $U_{\text{walk}} \neq I$. Let $\left| \sigma \right\rangle$ be the initial state she prepares (σ chosen at random from Σ). In this case, the quantum state she sends to B may be written as:

$$U_{\text{walk}} \left| \sigma \right\rangle = \left| \psi_\sigma \right\rangle = \sum_{i=0}^{2P-1} \alpha_i \left| i \right\rangle .$$

Assume that U_{walk} is chosen so that at least two of the α_i's are non-zero (such QWs exist by hypothesis). If B reflects, the qubit state arriving at A's lab, after E's attack on both channels, is

$$U_R^{(1)} U_F^{(1)} (U_{\text{walk}} \otimes I_E) \left| \sigma, \chi \right\rangle = \sum_i \alpha_i \left| i, f_i \right\rangle , \tag{3.10}$$

where I_E is the identity operator on E's ancilla.

A will subsequently apply the inverse QW operator and measure the resulting state, expecting to find $\left| \sigma \right\rangle$. This is equivalent to her measuring in the QW basis $\{ \left| \psi_0 \right\rangle , \left| \psi_1 \right\rangle , \cdots , \left| \psi_{2P-1} \right\rangle \}$, where $\left| \psi_i \right\rangle = U_{\text{walk}} \left| i \right\rangle$, and expecting to observe $\left| \psi_\sigma \right\rangle$. In this QW basis, we clearly have

$$\left| i \right\rangle = \sum_{j=0}^{2P-1} \langle \psi_j | i | \psi_j | i \rangle \left| \psi_j \right\rangle ,$$

from which, we may write Equation (3.10) as:

$$\sum_{i=0}^{2P-1} \alpha_i \left(\sum_{j=0}^{2P-1} \langle \psi_j | i | \psi_j | i \rangle \left| \psi_j \right\rangle \right) \otimes \left| f_i \right\rangle \tag{3.11}$$

$$\tag{3.12}$$

$$= \sum_{j=0}^{2P-1} \left| \psi_j \right\rangle \otimes \left(\sum_{i=0}^{2P-1} \alpha_i \langle \psi_j | i | \psi_j | i \rangle \left| f_i \right\rangle \right) . \tag{3.13}$$

Let p be the probability that this iteration does not result in an error – i.e., the probability

that A measures $|\psi_\sigma\rangle$. From the above equation:

$$p = \left| \sum_{i=0}^{2P-1} \alpha_i \langle \psi_\sigma | i | \psi_\sigma | i \rangle \, | f_i \rangle \right|^2 .$$

Noticing that $\langle \psi_\sigma | i | \psi_\sigma | i \rangle = \alpha_i^*$ (since $|\psi_\sigma\rangle = \sum_i \alpha_i \, |i\rangle$), and also $\langle f_i | f_i | f_i | f_i \rangle = 1$ (due to the unitarity of $U_R^{(1)}$), we find:

$$p = \left| \sum_i |\alpha_i|^2 \, |f_i\rangle \right|^2 = \sum_i |\alpha_i|^4 + 2 \sum_{i>j\geq 0} |\alpha_i|^2 |\alpha_j|^2 \mathrm{Re}(\langle f_i | f_j | f_i | f_j \rangle).$$

When $|f_i\rangle \equiv |f_j\rangle = |F\rangle$, for all i, j, the above quantity attains its maximum of $p = 1$. In this case, after E's attack, the system described by Equation (3.10) is $\sum_i \alpha_i \, |i\rangle \otimes |F\rangle = |\psi_\sigma\rangle \otimes |F\rangle$. Due to the Cauchy-Schwarz inequality $\mathrm{Re}(\langle f_i | f_j | f_i | f_j \rangle) \leq 1$. If, however, one or more of the $\mathrm{Re}(\langle f_i | f_j | f_i | f_j \rangle) < 1$ for any of the $(|f_i\rangle, |f_j\rangle)$ pairs which appear in the expression above (i.e., for those where α_i and α_j are non-zero), it is obvious that $p < 1$ and so E would be detected.

Therefore, to avoid detection, it must be that $\mathrm{Re}(\langle f_i | f_j | f_i | f_j \rangle) = 1$ for all i, j where α_i and α_j are non-zero, implying $|f_i\rangle \equiv |f_j\rangle$. Indeed, if we write $|f_j\rangle = x \, |f_i\rangle + y \, |\zeta\rangle$, where $\langle f_i | \zeta | f_i | \zeta \rangle = 0$, then $\mathrm{Re}(\langle f_i | f_j | f_i | f_j \rangle) = 1 = \mathrm{Re}(x)$. Of course $|x|^2 + |y|^2 = 1$ (since $\langle f_j | f_j | f_j | f_j \rangle = 1$) and so:

$$|x|^2 + |y|^2 = 1 \Rightarrow \mathrm{Re}^2 x + \mathrm{Im}^2 x + |y|^2 = 1 \Rightarrow \mathrm{Im}^2 x + |y|^2 = 0.$$

This implies both $\mathrm{Im}(x) = 0$ and $y = 0$. Since $\mathrm{Re}(x) = 1$, we conclude $x = 1$ and so $|f_i\rangle = |f_j\rangle$.

Since A could have chosen any QW in $\mathcal{Q}$, all possible (i, j) pairs are covered (i.e., at least one QW in $\mathcal{Q}$ is guaranteed to produce a state where α_i and α_j are non-zero) and since E does not know which QW was chosen, it must be that $|f_i\rangle \equiv |f_j\rangle \equiv |F\rangle$ for all i, j.

Thus, after the first iteration, to avoid detection, it must be that the state of E's quantum memory is in the state $|F\rangle$, independently of A's and B's raw key and operations. Thus, E is not able to extract any information during the first iteration. Furthermore, since she is fully aware of the state of her quantum memory in this case (i.e., she knows the state $|F\rangle$), the above arguments may be repeated inductively for the remaining iterations of the protocol, leading to the conclusion that the protocol is robust. □

The above proof of robustness placed certain requirements on the set of QW $\mathcal{Q}$, but can such a set even exist? We show that, at least for all odd P, such a set may be easily

constructed.

Lemma 2. *If P is odd, then there exists a set of QWs $\mathcal{Q}$ which satisfy the requirements of Theorem 1.*

Proof. Let $(l,s),(l',s') \in \{0,1,\cdots,P-1\}\times\{R,L\}$. We construct a QW $U_{l,s,l',s'}$ and an initial state $|l_0,s_0\rangle$ such that $\langle l,s|U_{l,s,l',s'}|l_0,s_0|l,s|U_{l,s,l',s'}|l_0,s_0\rangle \neq 0$ and $\langle l',s'|U_{l,s,l',s'}|l_0,s_0|l',s'|U_{l,s,l',s'}|l_0,s_0\rangle$ 0.

Since P is odd, there exits a position index $q \in \{0,1,\cdots,P-1\}$ and a value $q_0 \in \mathbb{Z}$ such that $|q_0| < P$, $q - q_0 \equiv l \pmod{P}$, and $q + q_0 \equiv l' \pmod{P}$. We assume that $q_0 \geq 0$; if $q_0 < 0$ the result is symmetric by simply "flipping" l with l' (in which case q_0 becomes non-negative).

The shift operator S for our QW is simply the usual

$$S = \sum_{i=0}^{P-1} |i-1\rangle\langle i| \otimes |R\rangle\langle R| + \sum_{i=0}^{P-1} |i+1\rangle\langle i| \otimes |L\rangle\langle L|,$$

where all arithmetic, of course, is done modulo P. Our coin operator will simply be the Hadamard coin:

$$R_c = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

We claim the desired operator is $U_{l,s,l',s'} = [(I_p \otimes R_c)\cdot S]^{t+1}$. (Note that the shift operator is applied before the coin in this case to simplify the construction) Now, consider the initial state $|q+1,R\rangle$. After the first step of the QW (i.e., after applying $(I_p \otimes R_c)\cdot S$), the QW evolves to the state $\frac{1}{\sqrt{2}}|q\rangle(|R\rangle + |L\rangle)$. It is not difficult to see that, after t additional steps with this QW, *but before the final application of $I_p \otimes R_c$ on the $(t+1)$-th step*, the quantum state evolves to:

$$\alpha|l,R\rangle + \beta|l',L\rangle + |\phi\rangle,$$

where $|\alpha| \neq 0, |\beta| \neq 0$, and $|\phi\rangle$ is a non-normalised state orthogonal to both $|l,R\rangle$ and $|l',L\rangle$. Finally, after the last $I_p \otimes R_c$, the state becomes

$$\begin{aligned} U_{l,s,l',s'}|q+1,R\rangle = \frac{1}{\sqrt{2}}(&\alpha|l,R\rangle + \alpha|l,L\rangle \\ &+\beta|l',R\rangle - \beta|l',L\rangle) + |\phi'\rangle, \end{aligned}$$

with $|\phi'\rangle$ being a state orthogonal to $|l,R\rangle, |l,L\rangle, |l',R\rangle$, and $|l',L\rangle$, thus yielding the desired state. Taking $\mathcal{Q} = \bigcup_{l,s,l',s'} \{U_{l,s,l',s'}\} \cup \{I\}$ proves the result. □

Finally, we should notice that the robustness of this SQKD protocol is independent

of the existence or absence of quantum memories. In fact, E's attack requires a stable quantum memory, in which she keeps her ancillary system during the execution of the protocol. On the other hand, A does not need any quantum memory in order to share the key with B at the end, and B is, of course, restricted to classical operations. Therefore, without a quantum memory E cannot even conduct the attack, whereas even if she has access to a quantum memory, she is not able to extract any useful information about the key without being detected by A and B.

3.4 Practical attacks

While our work includes theoretical cryptographic proposals, and a detailed analysis of practical attacks is out of its scope, it is worthy presenting a short discussion of possible attacks and countermeasures for the case of optical implementations. The term practical attacks refers to attacks during which E is taking advantage of possible loopholes in the implementation of the protocols, i.e., the fact that the setups used for the implementation of the protocols are not perfect, can seriously compromise the security of the key. Such attacks have been thoroughly investigated in the literature and several countermeasures have been proposed in different setups and scenarios. For an overview of the recent progress and current status of this area of QKD, see the following detailed reviews [**?** **?** **?** **?** **?**].

One of the most studied of such attacks is the photon number splitting attack (PNS), which is based on the fact that there are no perfect single-photon sources [**?** **?** **?**]. Instead, the current sources emit in general multi-photon pulses, whose photon number statistics are described by a Poisson distribution. E, who is considered all-powerful and bounded only by the laws of physics, can thus, by placing herself in front of A, detect genuine multi-photon pulses, extract one photon from each, and send the rest to B through a lossless channel, while blocking single-photon pulses. Due to the fact that the quantum channel connecting A and B has losses exponential in the channel length, there exists a maximal distance, known to E, below which E is not able to spot E's interference. By storing the extracted photons in her quantum memory, E can measure them in the correct basis upon the classical communication between A and B, during which they publicly reveal their choices of preparation/measurement bases. Since all the photons of the same pulse are in the same state, E thus has the key shared by A and B.

The standard technique used to defend against a PNS attack is by introducing the so-called decoy states [**?**]. In addition to the signal states, from which the key is obtained, A sends coherent states $\left|e^{i\theta}|\alpha|\right\rangle$, with phase θ chosen uniformly at random, and the variable intensity $I \propto |\alpha|$. Note that such decoy pulses are to E indistinguishable from the signal

ones. Thus, A and B can subsequently detect E's interference (extracting single photons from multi-photon pulses) by comparing the yields of signal and decoy states (given the channel loss ℓ, the yield y is defined as $y = 1 - \ell$ [**?**]). For more details, see [**?**], as well as subsequent improvements and modifications [**? ? ? ? ? ? ?**]. This method, developed for standard one-way QKD schemes, can be straightforwardly applied to our second proposal, which is a one-way protocol as well. It can also be applied to our first and third two-way proposals. Indeed, in our first proposal, as B does not perform any measurement, it is A who performs the yield estimation upon receiving back the pulses. The same can be done by A alone for the photons reflected by B in our third proposal, in which in addition the yield check could be done for the pulses measured by B. As mentioned above, the details of the techniques depend on particular implementations and are beyond the scope of our theoretical study.

While the PNS attack is applicable to most of the protocols that use imperfect photon sources, the above description of its particular implementation is given on the example of a standard QKD *one-way* scheme. Thus, it has to be re-examined when applied to different protocols. The crucial feature of the standard QKD protocol is the exchange of classical information between A and B, which allows E to extract the key exchanged. Therefore, since such exchange is present in our second and third protocol, the above described PNS attack is applicable to those protocols as well. Note though that in the case of the third, *two-way* protocol, E can possibly extract information only upon intercepting the pulses re-sent from B to A. Indeed, in the third protocol the key is obtained from the cases in which B and, upon receiving them back, A too, perform measurements in the computational basis, thus sharing the same set of bits. Extracting photons from the pulse before it came to B, and consequently before his measurement, gives E no information about the key.

Nevertheless, our first, *two-way* QKD protocol, is considerably different from the standard QKD ones, as A and B reveal *no classical information* regarding their quantum operations (they only exchange information regarding the cases used for verification procedure, which do not contribute to the key generation). Thus, E's task is more difficult than in the case of standard QKD protocols. What E can do is to extract *two* photons from each pulse, one on the way from A to B, and another on the way back to A, and compare their states, $|\psi\rangle$ and $|\psi(r)\rangle$, in the attempt to learn the key r. Note that, even in the noiseless scenario, the described comparison does not have perfect efficiency, unlike the standard application of the PNS attack in which E learns the key with certainty. Moreover, in the case of our protocol, E can attack only three or more photon pulses, thus decreasing the efficiency of her attack with respect to the standard one, which makes use of more probable two-photon pulses as well. For example, for the commonly used

order of the mean photons per pulse, $\mu = 0.2$, the probability for emitting three or more photons is $p(n \geq 3) \approx 0.001$, while the probability to emit exactly two photons (the "deficit" with respect to the standard PNS attack) is of the order of magnitude higher, $p(n = 2) \approx 0.016$, where n is the number of photons per pulse emitted.

Finally, we would like to note that, although in practical attacks E is assumed to be all powerful, exceeding the current technological equipment used by everyday users, not all practical attacks are based on the same level of subtle equipment. In the case of the PNS attack, E should be able to perform photon non-demolition number measurements, a task beyond any current and (at least mid-term) foreseeable technology.

Nevertheless, there exist other practical protocols that do not requite such sophisticated technology. Below, we briefly analyse three such kinds of attacks, extensively studied in the literature: the Trojan horse, the detector blinding and the time-shift attacks.

The Trojan horse attack is one of the first attacks ever considered and since then it has been thoroughly investigated and continuously developed in different contexts. In a nutshell, Trojan horse attacks benefits from the imperfections in the quantum channel between A and B that allows for E's interference by modulating A's pulses, sending them to B and analysing the reflected/backscattered signal [**?** **?** **?**]. The first such attack benefitted from the detector imperfections, by collecting the light emitted upon the detection of the photons [**?**]. To counter such attacks, introducing simple optical isolators suffice in one-way protocols, while for two-way protocols one needs to introduce additional monitoring detectors [**?**].

Furthermore, we would like to briefly discuss two more attacks, namely the detector blinding and the time-shift attacks, which are both considered in the broader context of intercept and resend with faked states attacks [**?**]. In general, during an intercept and resend with faked states attack, E is not trying to extract information about the key from the original states that the legitimate parties exchange. Instead, she generates and sends to them classical or quantum light pulses, which are tailored in a way that she can control their measurement outcomes, while she is blocking the original states. At the end of such an attack, E and the legitimate parties share the same key, without A and B being able to detect her interference. In both the aforementioned attacks, E is taking advantage of loopholes in the performance and efficiency of the detectors of the legitimate parties.

First, we consider the detector blinding attacks to standard one-way QKD protocols [**?** **?**]. E first intercepts the state that A sends to B and measures it in one of the two possible bases, that she randomly chooses. Then, she sends to one of B's detectors a bright light pulse according to her measurement outcome. Note that the intensity of the bright light pulse is just a bit above the detector's threshold. If B chooses to measure in the same basis as E, all the light will be directed to one of his detectors, due to the

interference. The detector, which is now operating in the linear instead of the Geiger mode (avalanche photon diode), will click and E will now share the same key bit with B. If B chooses to measure in the complementary basis, the light will be divided in two components and its intensity will not be enough to trigger neither of the the detectors, therefore B will not get a click and this iteration will be discarded. Subsequently, A and B will keep for the key the bits for which A's preparation basis and B's measuring basis agree. During their classical communication, E will learn exactly which are these bits, therefore she will share the same key, while her interference remains unnoticed.

This attack is ineffective for the case of our first, two-way, protocol, in which only A is performing the measurement on the pulses received back from B. Note that her performing the inverse QW, followed by the measurement in the computational basis, is equivalent to measuring in an *unknown* to E (ensured by our Holevo argument mentioned in Section 3.1.1, and presented with details in Chapter 2), "rotated" basis, with respect to the computational one. Therefore, virtually all E's attempts to perform the detector blinding attack would result in no detection events for A. Moreover, even the (rare) detections, being uncorrelated with the initial state sent by A, would not pass the verification procedure described in Section 3.1.1, as well as the analogous checking rounds of the third, two-way semi-quantum protocol (when B reflects the pulses back to A and she performs the inverse walk and measures in the computational basis).

Regarding our second, one-way key distribution protocol, B's action is similar to the one in the standard protocols: he measures in one of the two publicly known bases. To counter such an attack, B can apply one of the known counter-measures proposed and analysed in [**?** **?** **?** **?** **?**]. Nevertheless, we would like to note again that our QW protocol is more complex than the standard ones based on few (typically four) quantum states, and thus its implementations might possibly invoke new challenges, a topic worth a separate study.

Time-shift attacks take advantage of the different timing responses of the detectors. Assuming E knows the timings of during which each detector is (in)sensitive, allows her to, similarly as in the previous case of the detector blinding, enforce the particular outcomes of B's/A's measurements. Analogously as in the case of detector blinding attacks, such strategy cannot pass the two-way verification procedures and checking rounds of our first and third protocols. In the case of our one-way protocol, one could employ similar methods to the ones proposed in [**?** **?** **?** **?**], in order to defend against a time-shift attack.

3.5 Conclusions

In the work presented in this chapter, we employed, for the first time to the best of our knowledge, QWs in order to design and analyze new secure QKD protocols. Besides the theoretically interesting intersection of two unique and fascinating fields of quantum information science, there are also potential practical benefits in pursuing this investigation. Some high-dimensional QKD protocols have the ability to withstand a high noise tolerance, as recently shown in several studies [**?** **?** **?** **?** **?** **?**]. Here we proposed QKD protocols based on high-dimensional states generated by means of QWs, and we showed that they are more tolerant to noise compared to protocols based on two-dimensional states. Apart from their interesting theoretical properties, it could be that, in a future quantum infrastructure, the generation of these QW states would be easier compared to other higher-dimensional systems. Indeed, producing such states may not need the high entanglement of many qubits – instead they could be generated through the evolution of a single-qubit walker on, for instance, a multi-node quantum network.

In what follows, we point out some directions of future work. First, it would be interesting to perform a more detailed study on the two verification procedures presented in Section 3.1.1 and compare them with respect to various attack strategies. Moreover, one could analyse the relation between the two for concrete cases of E's cheating strategies in the presence of noise.
In Section 3.2, we proved the security of the one-way protocol, but still some improvements could be done. In particular, one could find an analytical solution for the optimal choice of QW parameters or, alternatively, given particular QW parameters, to find an analytical solution for the value of c from Equation (3.6). Another interesting question would be to understand the maximally tolerated noise as the dimension of the position space and the number of steps of the QW go to infinity. For instance, in [**?**] a high-dimensional QKD protocol was introduced (not using QWs, but simpler states), which could suffer a bit error rate of up to 50% as the dimension of the state sent by A approached infinity. Can we construct a QW-QKD protocol with similar features? Does our protocol approach this disturbance level for high P?

Moreover, studying and employing other QW models (perhaps the memory-based QWs described and analysed in, e.g., [**?** **?** **?** **?** **?** **?**]) or QWs on different graphs, would be interesting – our key-rate equation would generalize to these cases; the only change would be the value of c. Perhaps different QW models, or different graphs, would produce more optimal values, thus increasing the key rate.

Finally, the SQKD protocol we proposed lacks of a proof of security beyond robustness. As we already mentioned in Section 3.3, this proof is technically very challenging due to the high-dimensional QW states and the use of a two-way channel. Hence, computing

analytically the key rate is extremely hard. Moreover, the numerical simulation is equally challenging, even for low-dimensional walks. Nevertheless, we believe that obtaining the key rate is not impossible, and we expect that this analysis will yield quite high error-tolerance. A first step towards this direction would be to try to reduce this protocol to a simpler one (for instance, the one in [**?**], for which there is a security proof [**?**]) and prove that it is at least as secure. This reduction does not seem to be a straightforward task and requires a thorough analysis.

Part II

Phase Transitions of Topological Systems at Finite Temperature

Chapter 4

Fidelity and Uhlmann connection analysis of fermionic systems undergoing phase transitions

In this chapter, we analyse the behaviour of the fidelity and the Uhlmann connection with respect to thermal states in fermionic systems undergoing PTs. To this end, we will consider the space consisting of the parameters of the Hamiltonian and the temperature, as it provides a physically sensible base space for the principal bundle, describing the amplitudes of the density operator.

The chapter is organised as follows: in Section 4.1, we perform the fidelity and Uhlmann connection analysis of PTs for paradigmatic models of 1D topologically non-trivial insulators (TIs) and superconductors (TSCs). We further confirm these results in Section 4.2, by studying the behaviour of the edge states in these systems. In Section 4.3 we investigate the behaviour of the fidelity and the Uhlmann connection in the case of a topologically trivial superconductor in 3D, as described by the BCS theory. We compare these results to the respective ones obtained in Section 4.1 and explain the reasons behind the different behaviours. In Section 4.4, we comment on the relevance of the choice of the base space in the study of PTs for topological systems. In the last section, we summarise our results, present our conclusions and point out some possible directions of future work.

*The work presented in this chapter corresponds to the work published in [**?**].

4.1 Fidelity and Δ analysis of topological insulators and superconductors

In our analysis we probe the fidelity and the quantity Δ associated to the Uhlamnn factor, as presented in Section 1.6 of the introductory Chapter 1, with respect to the parameters of the Hamiltonian describing the system and the temperature, independently. In this section, we will perform this study for paradigmatic models of TIs, namely the Su-Schrieffer-Heeger (SSH) [**?**] and the Creutz ladder [**? ?**] models, and TSCs, namely the Kitaev Chain [**?**] model in 1D.

These are free-fermion models, which can be described by quadratic Hamiltonians of the form

$$\mathcal{H} = \sum_{k\in\mathcal{B}} \Psi_k^\dagger H_k \Psi_k, \tag{4.1}$$

where $\Psi_k^\dagger, \Psi_k$ are the Nambu spinors, constructed by the corresponding fermion creation and annihilation operators, depending on the specific model (insulator or superconductor) and H_k is the single-particle Hamiltonian in momentum space. Notice that the sum is over all momenta in the first Brillouin zone $\mathcal{B}$. The single-particle Hamiltonians H_k are of the form

$$H_k = E_k\ \vec{n}_k \cdot \vec{\sigma}, \tag{4.2}$$

where E_k is the spectrum of H_k that gives the band gap, $\vec{n}_k$ is the so-called winding vector pointing along the quantisation axis and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the Pauli vector. Note that the symmetries that the Hamiltonians of topological systems possess, which we mentioned in the Introduction (TRS, PHS and CS), are imposed on the level of the single-particle H_k.

For our study, we analytically calculated the closed expressions for the fidelity and Δ, with respect to thermal states $\rho = e^{-\beta\mathcal{H}}/Z$, where β is the inverse temperature. We used natural units $\hbar = k_{\mathrm{B}} = 1$, and we obtained

$$F(\rho,\rho') = \prod_{k\in\mathcal{B}} \frac{2+\sqrt{2\left(1+\cosh(E_k/2T)\cosh(E_k'/2T')+\sinh(E_k/2T)\sinh(E_k'/2T')\vec{n}_k\cdot\vec{n}_k'\right)}}{\sqrt{(2+2\cosh(E_k/2T))(2+2\cosh(E_k'/2T'))}}, \tag{4.3}$$

and

$$\Delta(\rho,\rho') = F(\rho,\rho') - \prod_{k\in\mathcal{B}} \frac{2+2\left(\cosh(E_k/4T)\cosh(E_k'/4T')+\sinh(E_k/4T)\sinh(E_k'/4T')\vec{n}_k\cdot\vec{n}_k'\right)}{\sqrt{(2+2\cosh(E_k/2T))(2+2\cosh(E_k'/2T'))}}. \tag{4.4}$$

For the details of the derivation, see Appendix A.

The Hamiltonian for the TI SSH model [**?**] is given by

$$\mathcal{H} = \sum_{i\in\mathbb{Z}} v c^\dagger_{i,A} c_{i,B} + w c^\dagger_{i,B} c_{i+1,A} + \text{H.c.}, \tag{4.5}$$

where c_i are fermionic annihilation operators, A, B correspond to the two parts of the dimerised chain and v, w are coupling constants. The change of the difference $|v-w|$ between the two parameters of the Hamiltonian drives the topological PT. In particular, the PT occurs for $|v-w|=0$. Given two close points $(|v-w|, T)$ and $(|v-w|', T') = (|v-w| + \delta|v-w|, T+\delta T)$, we compute $F(\rho,\rho')$ and $\Delta(\rho,\rho')$ between the states $\rho = \rho(|v-w|, T)$ and $\rho' = \rho(|v-w|', T')$. To distinguish the contributions due to the change of Hamiltonian's parameter and the temperature, we consider the cases $\delta T = 0$ and $\delta|v-w| = 0$, respectively, see Figure 4.1.

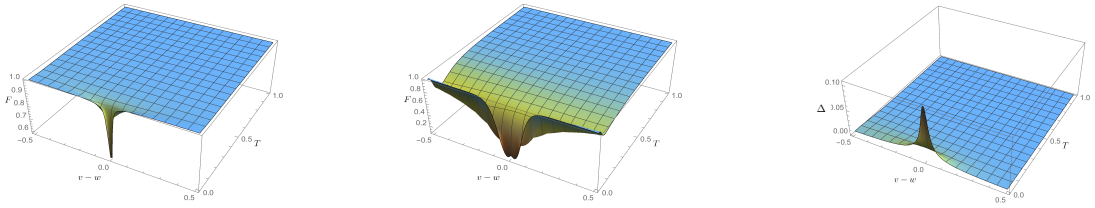

Figure 4.1: The fidelity for thermal states ρ, when probing the parameter of the Hamiltonian that drives the topological PT $\delta|v-w| = |v-w|' - |v-w| = 0.01$ (left), and the temperature $\delta T = T' - T = 0.01$ (centre), and the Uhlmann connection, when probing the parameter of the Hamiltonian $|v-w|$ (right), for the TI SSH model (representative of the symmetry class BDI). The plot for Δ when $\delta|v-w| = 0$ is omitted, since it is equal to zero everywhere.

The Hamiltonian for the TI Creutz Ladder model [**?** **?**] is given by

$$\begin{aligned}\mathcal{H} = \quad & -\textstyle\sum_{i\in\mathbb{Z}} K\left(e^{-i\phi} a^\dagger_{i+1} a_i + e^{i\phi} b^\dagger_{i+1} b_i\right) \\ & + K(b^\dagger_{i+1} a_i + a^\dagger_{i+1} b_i) + M a^\dagger_i b_i + \text{H.c.},\end{aligned} \tag{4.6}$$

where a_i, b_i, with $i \in \mathbb{Z}$, are fermion annihilation operators, K and M are hopping amplitudes (horizontal/diagonal and vertical, respectively) and $e^{i\phi}$ is a phase factor associated to a discrete gauge field. We take $2K = 1$, $\phi = \pi/2$. Under these conditions, the system is topologically nontrivial when $M < 1$ and trivial when $M > 1$. Similarly to the case of the SSH model, for two close points (M, T) and $(M', T') = (M + \delta M, T + \delta T)$, we compute $F(\rho,\rho')$ and $\Delta(\rho,\rho')$ between $\rho = \rho(M, T)$ and $\rho' = \rho(M', T')$ and we consider the cases $\delta T = 0$ and $\delta M = 0$, respectively, see Figure 4.2.

Finally, we present our quantitative results for the TSC model. The Hamiltonian for

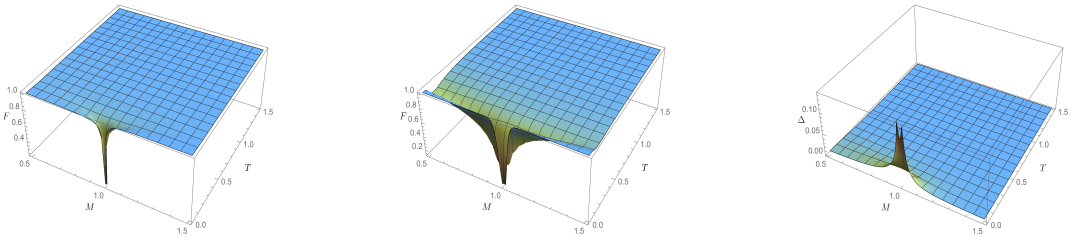

Figure 4.2: The fidelity for thermal states ρ, when probing the parameter of the Hamiltonian that drives the topological PT $\delta M = M' - M = 0.01$ (left), and the temperature $\delta T = T' - T = 0.01$ (centre), and the Uhlmann connection, when probing the parameter of the Hamiltonian M (right), for the TI Creutz ladder model (representative of the symmetry class AIII). The plot for Δ when deforming the thermal state along T is omitted since it is equal to zero everywhere.

the Kitaev Chain model [**?**] is given by

$$\mathcal{H} = -\mu \sum_{i=1}^{N} c_i^\dagger c_i + \sum_{i=1}^{N-1} \left[-t(c_{i+1}^\dagger c_i + c_i^\dagger c_{i+1}) - |\Delta|(c_i c_{i+1} + c_{i+1}^\dagger c_i^\dagger) \right], \tag{4.7}$$

where μ is the chemical potential, t is the hopping amplitude and Δ is the superconducting gap. We fix $t = 0.5, \Delta = 1$, while the change of μ along the sites of the line drives the topological PT. In particular, the PT occurs at $\mu = 1$ (gap closing point). Again, we calculate $F(\rho, \rho')$ and $\Delta(\rho, \rho')$ for $\rho = \rho(\mu, T)$ and $\rho' = \rho(\mu', T')$ for two close points (μ, T) and $(\mu', T') = (\mu + \delta\mu, T + \delta T)$ of the parameter space. In Figure 4.3, we show our results when probing the parameter of the Hamiltonian ($\delta T = 0$) and the temperature ($\delta\mu = 0$), separately.

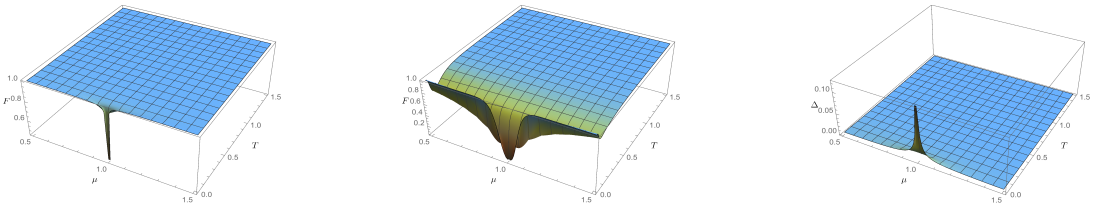

Figure 4.3: The fidelity for thermal states ρ, when probing the parameter of the Hamiltonian that drives the topological PT $\delta\mu = \mu' - \mu = 0.01$ (left), and the temperature $\delta T = T' - T = 0.01$ (centre), and the Uhlmann connection, when probing the parameter of the Hamiltonian μ (right), for the TSC Kitaev chain model. The plot for Δ when $\delta\mu = 0$, is trivial (equal to zero everywhere), thus we omit it.

For all the three cases that we presented the behaviour of the fidelity and the quantity Δ is qualitatively the same. We see that for $T = 0$ the fidelity exhibits a sudden drop in the neighbourhood of the gap-closing points, signalling the topological quantum PTs. As temperature increases, the drop of fidelity at the quantum critical points is rapidly smoothened towards the $F = 1$ value. This shows the absence of both finite-temperature

parameter-driven, as well as temperature-driven (i.e., thermal) PTs. The plots of Δ for $\delta T = 0$, show a behaviour similar to that of the fidelity, while if we only change the temperature and not the parameter of the Hamiltonian, we obtain no information, as Δ is identically equal to zero, due to the triviality of the Uhlmann connection associated to the mutually commuting states (a consequence of the Hamiltonian's independence on the temperature). Δ is sensitive to PTs for which the state change is accompanied by a change of the eigenbasis (in contrast to fidelity, which is sensitive to both changes of eigenvalues and eigenvectors). For TIs and TSCs, this corresponds to parameter-driven transitions only.

4.2 Edge states of topological insulators and superconductors

When one considers topological systems on a finite-size chain with open boundary conditions, the bulk-to-boundary correspondence principle [**?** **?**] predicts the existence of zero modes localised at the ends of the chain, whenever the bulk is in a topologically non-trivial phase. It is then possible to consider the associated thermal states, $\rho = \exp(-\beta\mathcal{H})/Z$, and probe the effects of temperature. The study of the Uhlmann connection and the fidelity conducted in the previous section suggests that at zero temperature the edge states should exhibit an abrupt change as the system passes the point of quantum phase transition, while at finite temperatures they should smoothly change, slowly being washed away with the temperature increase, as a consequence of the absence of finite-temperature transitions. Below, we first study TIs in Section 4.2.1, while in Section 4.2.2 we analyse a TSC given by the Kitaev model, showing the agreement with the above inferred behaviour.

4.2.1 Topological insulators

Let us consider the Creutz ladder model as a representative of TIs. Similar results are obtained when considering the SSH model and we omit them for the sake of briefness. In the trivial phase, the spectrum decomposes into two bands of states separated by a gap. At zero chemical potential, the zero-temperature limit of ρ is the projector onto the Fermi sea state $|\mathrm{FS}\rangle$, obtained by occupying the lower band. On a topologically non-trivial phase, however, the spectrum is composed of the two bands *and* the zero modes. At zero chemical potential, the zero temperature limit of ρ is now the projector onto the ground state manifold of $\mathcal{H}$, which is spanned by $|\mathrm{FS}\rangle$ and additional linearly independent states by creating excitations associated to the zero modes. Since the Fermi sea does not have these edge state excitations (exponentially localised at the boundary) included, the

occupation number as a function of position, $n_i = a_i^\dagger a_i + b_i^\dagger b_i$, will see this effect at the boundary of the chain. Indeed, this is what we see in Figure 4.4: the occupation number, as a function of position, drops significantly at the edges in the topologically non-trivial phase. On the other hand, on the topologically trivial side the occupation number stays constant throughout the whole chain (both bulk and the edges).

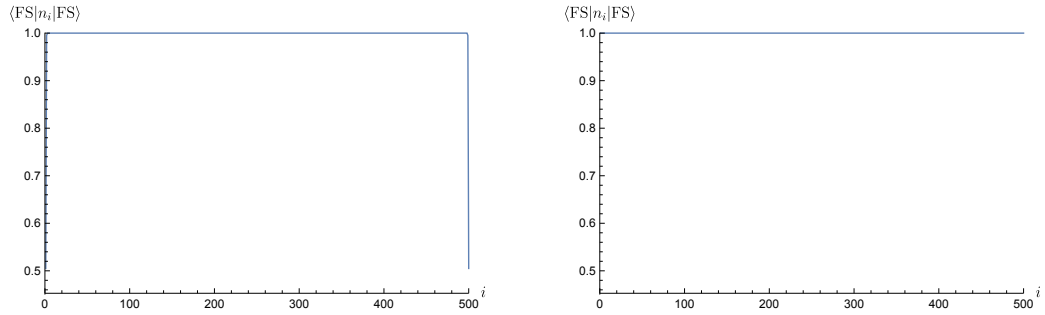

Figure 4.4: Fermi sea expectation value of the occupation number $n_i = a_i^\dagger a_i + b_i^\dagger b_i$ as a function of position i on a chain of 500 sites with open boundary conditions for a TI (Creutz ladder model). On the left panel the system is in a topologically non-trivial phase with $2K = 1, M = 0.1, \phi = \pi/2$. On the right panel the system is in a topologically trivial phase with $2K = 1, M = 1.0001, \phi = \pi/2$.

If we want the thermal state's $T = 0$ limit to be the Fermi sea, we have to add a very small (negative) chemical potential. It has to be small enough so that the lower band gets completely filled. In the following Figure 4.5, we see that the expectation value $\mathrm{tr}(\rho n_i)$ coincides with $\langle \mathrm{FS}| \, n_i \, |\mathrm{FS}\rangle$ in the $T = 0$ limit and the deviation of the occupation number at the edge from that in the bulk gets washed out smoothly as the temperature increases. In fact, in the large temperature limit, the state is totally mixed, implying that the expected value of the occupation number will be constant and equal to 1, as a function of position.

We see that the results presented in Figures 4.4 and 4.5 confirm the results obtained by the fidelity analysis and the study of the Uhlmann connection in terms of the quantity Δ. Indeed, the fact that the edge states localised at the boundary between two distinct topological phases, that manifest the topological order at zero temperature, are gradually smeared out as we increase the temperature, confirm the absence of finite-temperature PTs. Furthermore, our results on the edge states, obtained for systems in thermal equilibrium, agree with those concerning open systems treated within the Lindbladian approach [**?**] (and consequently, due to considerable computational hardness, obtained for an open chain of only 8 sites).

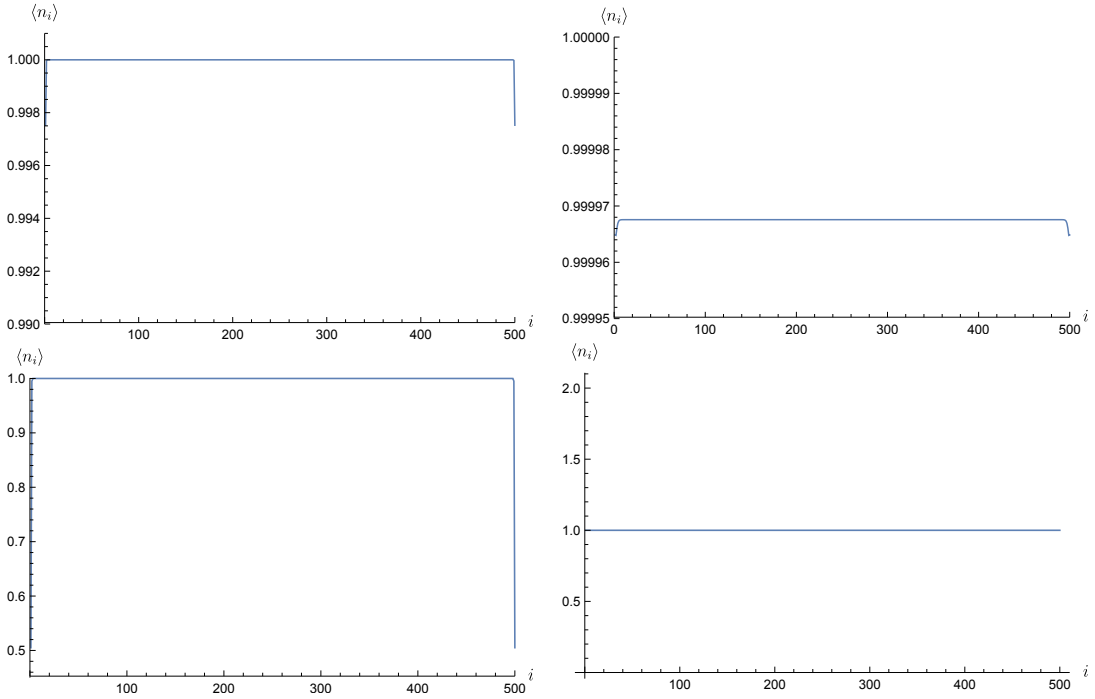

Figure 4.5: Expectation value of the occupation number $n_i = a_i^\dagger a_i + b_i^\dagger b_i$ as a function of position i on a chain of 500 sites with open boundary conditions for a TI (Creutz ladder model). In the left panel, we show the topologically non-trivial phase with $2K = 1, M = 0.1, \phi = \pi/2$, for temperatures $T = 10^{-5}$ (down) and $T = 0.2$ (up). On the right panel we have a topologically trivial phase near the critical value of the parameter $2K = 1, M = 1.0001, \phi = \pi/2$, for temperatures $T = 10^{-5}$ (down) and $T = 0.2$ (up). Increasing M, the edge behaviour is washed out smoothly, for finite T, and it becomes trivial as for the $T = 0$ case.

4.2.2 Topological superconductors

As far as the TSC Kitaev model is concerned, the chemical potential is a parameter of the Hamiltonian and we cannot lift the zero modes from the zero-temperature limit of ρ with the above method. Moreover, the Kitaev Hamiltonian does not conserve the particle number, and adding chemical potential associated to the total particle number would not lift the zero modes even if μ were not a parameter of the Hamiltonian. Note though, that the total number of Bogoliubov *quasi-particles* which diagonalise the Hamiltonian is conserved. Hence, we add a very small (negative) chemical potential associated with the total quasi-particle number, thereby lifting the Majorana zero modes energy. We found that the good quantity to be studied is not the occupation number as a function of the position in the chain, but the ratio between the average particle occupation number at the edge and the average particle occupation number at the bulk $f(\mu; T) = \langle n_{\text{edge}} \rangle / \langle n_{\text{bulk}} \rangle$ (without loss of generality, we have chosen for n_{bulk} the site in the middle of the chain, since it is approximately constant throughout the bulk). In Figure 4.6, we present the results obtained for a chain with open boundary conditions, consisting of 300 sites.

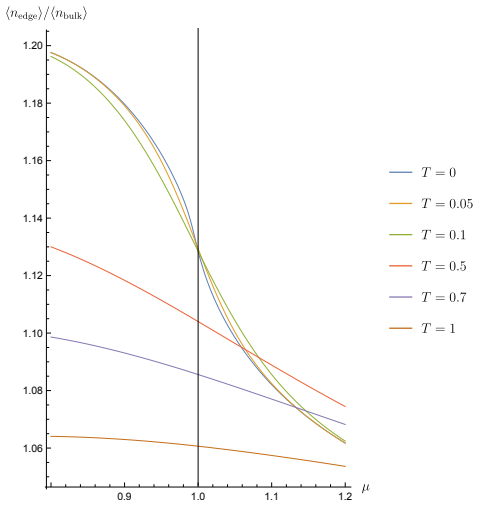

Figure 4.6: $\langle n_{\text{edge}} \rangle / \langle n_{\text{bulk}} \rangle$ as a function of the chemical potential μ for a chain of 300 sites with open boundary conditions, for several values of the temperature T.

The results are consistent with the behaviour inferred by the Uhlmann connection and the fidelity: Majorana modes exhibit an abrupt change at zero temperature (a signature of the quantum PT), while for fixed finite temperatures they smoothly change with the parameter change, and are slowly washed away with the temperature increase. Indeed, the behaviour of the finite-temperature curves is smooth, while the zero-temperature quench-like curve is expected to develop a discontinuity at $\mu = 1$ in the thermodynamic limit (see for example Fig.4(b) and the respective discussion in [**?**]). To show this more accurately, one needs considerably higher computational power to probe chain lengths of much higher orders of magnitude, a relevant future direction of work.

The behaviour of the edge states and the associated Majorana modes reveals an interesting property of these systems which, at finite temperatures, despite the absence of phase transitions, they keep exhibiting their topological features even on the "trivial side" of the phase diagram (for parameter values for which on zero temperature the system is topologically trivial). At zero temperature, the Majorana modes are known to be good candidates for qubit encoding, see [**?** **?** **?** **?**] and references therein. Therefore, the aforementioned property of Majorana modes at the low but finite-temperature regime, is potentially significant in constructing realistic quantum memories. Furthermore, the existence of stable quantum memories has considerable impact in cryptography [**?** **?** **?** **?** **?** **?** **?** **?** **?** **?**], as explained in Chapter 1.

Finally, we should stress that this new method to study Majorana modes is more general and also applicable to TIs: since the Hamiltonian conserves the total particle number, and the quasi-particle creation operators are linear combinations of *just* the particle creation operators (and not of the holes as well), the total quasi-particle and particle numbers coincide in this case. The results obtained for TIs using this new method lead

to the same qualitative conclusion regarding the behaviour of the edge states (consistent with our previous results) and we omit them in order to avoid repetition.

4.3 Fidelity and Δ analysis of BCS superconductors

In this section we study a topologically trivial superconducting system, as described by the BCS theory [**?**], with the effective Hamiltonian

$$\mathcal{H} = \sum_k (\varepsilon_k - \mu) c_k^\dagger c_k - \Delta_k c_k^\dagger c_{-k}^\dagger + \text{H.c.}, \tag{4.8}$$

where ε_k is the energy spectrum, μ is the chemical potential, Δ_k is the superconducting gap, $c_k \equiv c_{k\uparrow}$ and $c_{-k} \equiv c_{-k\downarrow}$ are operators annihilating an electron with momentum k and spin up and an electron with momentum $-k$ and spin down, respectively. The gap parameter is determined in the above mean-field Hamiltonian through a self-consistent mass gap equation and it depends on the original Hamiltonian's coupling associated to the lattice-mediated pairing interaction V, absorbed in Δ_k (for more details, see [**?**]). The solution of the equation renders the gap temperature-dependent. In Figure 4.7, we show the quantitative results for the fidelity and Δ. We observe that both quantities show

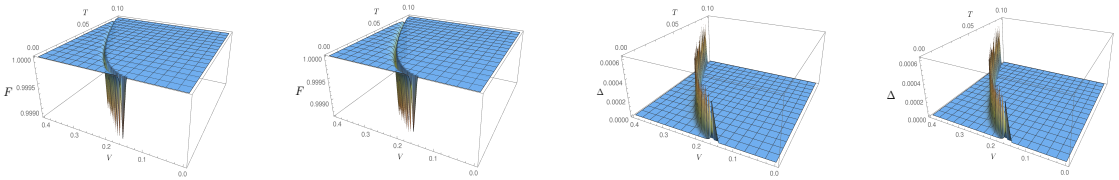

Figure 4.7: The fidelity for thermal states ρ when probing the parameter of the Hamiltonian $\delta V = V' - V = 10^{-3}$ (left) and the temperature $\delta T = T' - T = 10^{-3}$ (centre left), and the Uhlmann connection (centre right and right, respectively), for BCS superconductivity.

the existence of thermally driven PTs, as their abrupt change in the point of criticality at $T = 0$, survive and drift, as temperature increases. This behaviour is in sharp contrast to the respective behaviour of the topologically non-trivial systems, for which there exist no finite-temperature PTs.

It is interesting to compare the two cases of superconductors studied, and try to isolate the reasons for such difference. Unlike TSCs, in the BCS model the temperature does not only appear in the thermal state, but it is also a parameter of the effective Hamiltonian (recall that the superconducting gap depends on temperature), resulting in the change of the system's eigenbasis and consequently a non-trivial Uhlmann connection. In particular, the quantity Δ, which quantifies the rate of change of the system's eigenbasis, reflects the quantum contribution to the state distinguishability (see also [**?**], equation (3), in

which the Bures metric is split into classical and non-classical terms, the first quantifying the change of system's eigenvalues and the second the change of the corresponding eigenvectors). Thus, the Uhlmann connection is trivial in the cases of the topological systems considered, as their Hamiltonians do not explicitly depend on temperature and thus commute with each other at finite temperatures. On the other hand, the mean-field BCS Hamiltonian considered does explicitly depend on the temperature, and as the results presented above clearly show, the change of the eigenbasis of the BCS thermal states carries the signature of a thermally driven PT. Note that, having a purely non-classical contribution, such a temperature-driven PT has quantum features as well, which is on its own an interesting consequence of the study of the Uhlmann connection.

To illustrate this difference between TSCs and BCS better, let us explain the above with a few more details. In the case of the BCS superconductivity we considered the effective mean-field Hamiltonian given by Equation (4.8), in which the gap $\Delta(V,T)$ is a function of temperature. Had we considered a more fundamental "pairing Hamiltonian", which takes into account the quartic electron interaction mediated by the phonons of the lattice,

$$\mathcal{H}^P = \sum_k (\varepsilon_k - \mu) c_k^\dagger c_k - \sum_{k,k'} V_{k,k'} c_{k'}^\dagger c_{-k'}^\dagger c_{-k} c_k + \text{H.c.}, \tag{4.9}$$

the Uhlmann connection would be trivial. The mean-field Hamiltonian of Equation (4.8) is obtained from Equation (4.9) by means of the BCS decoupling scheme with an averaging procedure, setting the effective gap for the mean-field state $\rho = e^{-\beta\mathcal{H}}/Z$ (for simplicity, we assume $V_{kk'} = -V$ for k, k' close to the Fermi momentum k_F, and zero otherwise) to be

$$\Delta(V,T) = -\sum_{k'} V_{kk'} \langle c_{-k} c_k \rangle = V \sum_k \text{Tr}(c_{-k} c_k \rho). \tag{4.10}$$

In other words, the effective mean-field Hamiltonian of Equation (4.8) is obtained from Equation (4.9) by expanding $c_{-k}c_k = \langle c_{-k}c_k \rangle + \delta(c_{-k}c_k)$ around the suitably chosen superconducting ground state. Thus, $\mathcal{H}$ breaks the U(1)− particle-number conservation symmetry of $\mathcal{H}^P$ to a residual $\mathbb{Z}_2$ symmetry, in order to accommodate the superconducting properties of the system. As a result, the Uhlmann connection becomes sensitive to temperature-driven PTs, due to the enhanced state distinguishability in terms of the system's eigenbasis. On the other hand, the Hamiltonian of the Kitaev model is phenomenological, modelled upon the success of the related BCS mean-field Hamiltonian. In this model, the gap is, for simplicity, considered to be temperature-independent. One might thus question whether the gap of a general superconducting material should also a priori depend on the temperature. It would be interesting to probe this in experiments with realistic topological superconducting materials. Our method based on the Uhlmann

connection could then be particularly useful in the analysis of such experiments.

4.4 The choice of the parameter space in the study of topological phase transitions

We will conclude this chapter, by commenting on the relevance of the choice of the parameter space in the study of PTs in topologically ordered systems. In order for the Uhlmann connection and the fidelity to be in tune, they must be taken over the same base space, which in our study consists of the parameters of the Hamiltonian and the temperature. In a previous study [**?**], the Uhlmann connection for 1D topologically ordered systems was considered in the momentum space and with respect to single-particle density matrices of the form $\{\rho_k := e^{-\beta H_k}/Z : k \in \mathcal{B}\}$. In order to infer the possibility of finite-temperature PTs, the authors used the Uhlmann geometric phase $\Phi_U(\gamma_c)$ along the closed curve $\gamma_c(k) = \rho_k$, given as

$$\Phi_U(\gamma_c) = \arg \mathrm{tr}\{w(-\pi)^\dagger w(\pi)\} = \arg \mathrm{tr}\{\rho_\pi U(\gamma_c)\},$$

where $w(k)$ is the horizontal lift of the loop of density matrices ρ_k, and $U(\gamma_c)$ is the so-called Uhlmann holonomy obtained by imposing the Uhlmann parallel transport condition along the first Brillouin zone $\mathcal{B}$. It was found that $\Phi_U(\gamma_c)$ changes abruptly from π to 0 after some "critical" temperature T_U. The authors identified this abrupt change of $\Phi_U(\gamma_c)$, as a finite-temperature topological PT "in the Uhlmann sense", in analogy to the pure-state case, where the abrupt change of the Berry phase signals a topological PT [**?**]. Note, also, that the zero-temperature limit of the Uhlmann geometric phase is the Berry phase. However, for the topological systems studied in [**?**], the Uhlmann holonomy is a smooth function of the temperature and is given, in the basis in which the CS operator is diagonal, by:

$$U(\gamma_c) = \exp\Big\{ -\frac{i}{2}\int_{-\pi}^{\pi} \Big[1 - \mathrm{sech}\left(\frac{E_k}{2T}\right)\Big] \frac{\partial \varphi_k}{\partial k} dk\ \sigma_z \Big\},$$

where φ_k is the polar angle coordinate of the vector $\vec{n}_k$ lying on the equator of the Bloch sphere. So, while the Uhlmann phase suffers from an abrupt change, the Uhlmann holonomy is smooth, hence there is no PT-like behaviour. Conversely, there might be cases, where the Uhlmann phase is trivial, $\Phi_U(\gamma_c) = 0$, while the corresponding holonomy is not, $U(\gamma_c) \neq I$. Moreover, the associated critical temperature is not necessarily related to a physical quantity that characterises a system's phase.

In the paradigmatic case of the quantum Hall effect [**?**], at $T = 0$, the Hall conductivity is quantised in multiples of the first Chern number of a vector bundle in momentum space through several methods. For example, one can use linear response theory or integrate the fermions to obtain the effective action of an external U(1)− gauge field. The band topology appears, thus, in the response of the system to an external field. In this context, it is unclear how the Uhlmann geometric phase along the cycle of the 1D momentum space, can have an interpretation in terms of the physical response of the system. In order to measure it, one would have to be able to change the quasi-momentum of a state in an adiabatic way. In realistic setups, the states at finite temperatures are statistical mixtures over all momenta, such as the thermal states considered, and realising closed curves of states ρ_k with precise momenta changing in an adiabatic way seems to be a tricky task. The fidelity computed in our work though, refers to the change of the system's *overall* state, with respect to its parameters (controlled in the laboratory much like an external gauge field), and is related to an, *a priori*, physically relevant geometric quantity, the Uhlmann factor V. The quantity Δ, which can be written as $\Delta = \mathrm{tr}\left[|\sqrt{\rho(t+\delta t)}\sqrt{\rho(t)}|(I - V)\right]$ also contains information about the Uhlmann factor, therefore it seems that both of these quantities, computed over the base space consisting of the parameters of the Hamiltonian and the temperature, are physically more sensible to be considered in order to infer the possibility of PTs.

Conclusions and future work

By means of the fidelity and the Uhlmann connection analysis, we showed the absence of finite-temperature PTs in 1D TIs and TSCs. We further confirmed this result through the study of the edge states that appear on the boundary between two distinct topological phases. We also performed the same analysis for a topologically trivial BCS superconductor, where, in contrast to the former systems, temperature-driven PTs occur and are captured by both the fidelity and the Uhlmann connection. This shows that, when changing the temperature, the density operator is changing both at the level of its spectrum and its eigenvectors. We analysed in detail the origin of the differences between topologically trivial and non-trivial superconductors and suggested that, in realistic scenarios, the gap of TSCs could also, generically, be temperature-dependent. We also discussed the relevance of the choice of the base space. We clarified that the Uhlmann geometric phase considered in *momentum space* is not adequate to infer such PTs, since it is only a part of the information contained in the Uhlmann holonomy. Indeed, this holonomy, as a function of temperature, is smooth (Equation (4.4)), hence no PT-like phenomenon is expected.

Finally, we would like to point out possible future lines of research. The study of Majorana modes at finite temperature suggested that they can be used in achieving realistic quantum memories. The detailed quantitative analysis of their robustness, in concrete practical implementations, is a relevant direction for future work. Another related subject is to perform the same fidelity and Uhlmann connection analysis in the context of open systems, where the system interacts with a bath and eventually thermalises. There, the parameter space would also include the parameters associated to the system-bath interaction.

Chapter 5

Simulation of topological systems with quantum walks

Recently, Kitagawa *et al.* [**?**] showed that DTQWs can realise topological phases in 1D and 2D for all the symmetry classes [**?** **?**] of free-fermion systems. In particular, the authors engineered specific QW protocols that simulate representatives of all topological phases, featured by the presence of robust symmetry-protected edge states (see also [**?**]). In general, QW realisations are particularly useful, because, in addition to the simplicity of their mathematical description, the parameters that define them can be easily controlled in the lab. Therefore they provide a powerful simulating platform. The aforementioned topological QWs have been experimentally realised as periodically driven systems [**?**] and there are several experimental proposals for measuring topological invariants employing this approach [**?** **?** **?**]. In this chapter, we apply the previously introduced fidelity and Δ analysis of PTs, to the case of the effective Hamiltonians obtained from 1D topological DTQWs, realising representatives of two chiral symmetric classes of TIs. In particular, we study their topological features at finite temperatures with respect to both single-particle and many-body Boltzmann-Gibbs (BG) thermal-like states.

The chapter is organised as follows: in Section 5.1, we describe the main topological features of QWs and their origin, and present the respective protocols that we use. For a detailed and complete analysis of the topological QW protocols, see [**?** **?**]. In Section 5.2 we present the BG states considered: the single-particle QW states and their many-body counterparts. Furthermore, we clarify the relationship between them and explain the motivation for their use in different physical scenarios. In Section 5.3, we present our results on the fidelity and the quantity Δ at finite temperatures, and discuss the possibility of temperature-driven PTs. We further confirm these results in Section 5.4, where we study the behaviour of the edge states. Finally, we summarise and discuss our results and point out possible directions of future work.

*The work presented in this chapter corresponds to the work published in [**?**].

5.1 Topological quantum walks

In this section, we briefly present the QW protocols that we will use for the simulation of the two chiral symmetric classes BDI and AIII [**?** **?**] and describe the origin of their topological features. In [**?**], the authors show that the standard DTQW on the line that we presented in Section 1.4 of Chapter 1, can simulate the non-trivial topological phase of the SSH model for TIs (representative of the BDI symmetry class). In order to be able to study also the trivial topological phase and the edge states, that appear on the boundary between the two, the authors in [**?**] introduce the so-called *split-step* QW. As the name suggests, each step of the walk is split in two parts, each having a structure analogous to that of a standard DTQW

$$U_{ss} = T_1 R_y(\theta_2) T_0 R_y(\theta_1). \tag{5.1}$$

The coin operators are $R_y(\theta_i) = e^{i\frac{\theta_i}{2}\vec{y}\cdot\vec{\sigma}}$, with $\vec{y} = (0,1,0)$ and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ the Pauli vector. They represent rotations in the coin space by an angle θ_i along the y-axis, and the shift operators are given as

$$T_c = \sum_x |x + (-1)^c\rangle \langle x| \otimes |c\rangle \langle c| + |x\rangle \langle x| \otimes |1 \oplus c\rangle \langle 1 \oplus c|\,, \tag{5.2}$$

where $c \in \{0,1\}$ denotes the two possible coin states and $\oplus$ is addition modulo 2. For different values of the parameters θ_1 and θ_2 this protocol is shown to realise both the trivial and non-trivial topological phases for the SSH model.

As already mentioned, topological QWs can be realised by means of periodically driven systems given by periodic time-dependent Hamiltonians $H(t + \delta t) = H(t)$, where δt represents the time of a single step. The evolution operator for one period of the driving, $[0, \delta t]$, called the Floquet operator, is given by

$$U(\delta t) = \mathcal{T} e^{-i\int_0^{\delta t} H(t)dt}, \tag{5.3}$$

where $\mathcal{T}$ is the time ordering operator. Using homotopy theory, in [**?**] the authors propose a classification of periodically driven systems, according to the topological properties of their Floquet operators. They consider the Floquet operator in terms of a local effective Hamiltonian, given by $U(\delta t) = e^{-iH_{\text{eff}}(\delta t)}$. They show that if $U(\delta t)$ is trivial under all homotopy groups, then the associated H_{eff} can exhibit non-trivial topological behaviour. The triviality of $U(\delta t)$ under the homotopy groups implies the existence of a gap in the spectrum of H_{eff} and if moreover H_{eff} has some of the following symmetries, namely TRS, PHS and CS, the system supports the topological phases present in static TIs and TSCs, classified according to the system's dimension and the presence of these symmetries [**?** **?**

].

The unitary operator that describes one step of the evolution of the split-step QW, as given in Equation (5.1), is trivial under all homotopy groups, therefore we can define a local effective Hamiltonian

$$H_{\text{eff}}(\theta_1, \theta_2) \equiv -i\delta t^{-1} \log U(\theta_1, \theta_2), \tag{5.4}$$

whose quasienergy spectrum has a gap [**?**]. To fix the branch of the logarithm, we choose the first Brillouin zone for the energy spectrum, as in [**?** **?**], obtaining the single-particle H_{eff} consistent with realistic many-body counterparts discussed in the next section. This way, the QW "provides a stroboscopic simulation of the evolution generated by H_{eff} at discrete times $N\delta t$" [**?**]. In other words, the evolution of the QW is performed in discrete time steps which last δt units of time each. For simplicity, we take $\delta t = 1$.

Writing the effective Hamiltonian as

$$H_{\text{eff}}(\theta_1, \theta_2) = \sum_{k \in \mathcal{B}} [E_k(\theta_1, \theta_2) \vec{n}_k(\theta_1, \theta_2) \cdot \vec{\sigma}] \otimes |k\rangle \langle k| \,, \tag{5.5}$$

where $\mathcal{B}$ is the first Brillouin zone, $E_k(\theta_1, \theta_2) \geq 0$ are the eigenvalues and $\vec{n}_k(\theta_1, \theta_2)$ the eigenstates of $H_{\text{eff},k}$:

$$H_{\text{eff},k}(\theta_1, \theta_2) \, |\pm \vec{n}_k(\theta_1, \theta_2)\rangle = \pm E_k(\theta_1, \theta_2) \, |\pm \vec{n}_k(\theta_1, \theta_2)\rangle \,, \tag{5.6}$$

forming the two energy bands $\{\pm E_k(\theta_1, \theta_2),\ k \in \mathcal{B}\}$, we can obtain the specific form of the spectrum $E_k(\theta_1, \theta_2)$ and the vectors $\vec{n}_k(\theta_1, \theta_2)$. The BDI symmetry class has CS, given by the operator [**?** **?**]

$$\Gamma^y_{\theta_1} = \exp\Big(-i\pi \vec{A}^y_{\theta_1} \cdot \vec{\sigma}/2\Big), \tag{5.7}$$

where $\vec{A}^y_{\theta_1} = (\cos(\theta_1/2), 0, \sin(\theta_1/2))$. The CS restricts $\vec{n}_k(\theta_1, \theta_2)$, which defines the quantisation axis for each quasimomentum k, to lie on a great circle of the Bloch sphere. The number of times that $\vec{n}_k(\theta_1, \theta_2)$ winds around the origin, as k ranges within the first Brillouin zone $\mathcal{B}$, is the *winding number* ν of the map between the two circles. This is exactly what manifests the topological features of the QW: the winding number is the topological invariant, whose value characterises each distinct topological phase. Moreover, the BDI class has PHS given by

$$\mathcal{P} = \mathcal{K}, \tag{5.8}$$

where $\mathcal{K}$ denotes the complex conjugation operator, and TRS given by the operator:

$$\mathcal{T} = \Gamma^{y}_{\theta_1}\mathcal{P}. \tag{5.9}$$

We can fix $\theta_1 = -\pi/2$ for both topological phases, trivial ($\nu = 0$) and non-trivial ($\nu = 1$). The closure of the gap implies a change of phase, so by varying the value of θ_2 we change the energy spectrum and we are able to close the gap, thus having a PT.

In order to simulate different symmetry classes, we can further modify this basic split-step protocol. By changing the rotation axis from $\vec{y} = (0, 1, 0)$ to $\vec{\alpha} = \frac{1}{\sqrt{2}}(0, 1, 1)$, we manage to break TRS and PHS, while maintaining CS. That leads us to the split-step protocol that simulates the symmetry class AIII. The CS of the AIII class is given by the operator [**?** **?**]

$$\Gamma^{\alpha}_{\theta_1} = \exp\Big(-i\pi\vec{A}^{\alpha}_{\theta_1}\cdot\vec{\sigma}/2\Big), \tag{5.10}$$

where $\vec{A}^{\alpha}_{\theta_1} = (\cos(\theta_1/2), -\frac{1}{\sqrt{2}}\sin(\theta_1/2), \frac{1}{\sqrt{2}}\sin(\theta_1/2))$. Similarly to the case of the BDI class, the existence of CS implies that the vector $\vec{n}_k(\theta_1, \theta_2)$ is restricted to lie on a great circle of the Bloch sphere. The winding number ν of the map from the first Brillouin zone to this circle is the topological invariant that characterises the two distinct topological phases (the trivial one with $\nu = 0$ and the non-trivial with $\nu = 1$). For the AIII class, we fix $\theta_1 = \pi/2$ and by varying θ_2 along the line of the walk, it is possible to create a domain wall that separates the two different phases.

In Table 5.1 we summarise the above, by presenting the aforementioned 1D chiral classes, their symmetries, the QW protocols that simulate them and the values of the parameters for each distinct topological phase, characterised by the winding number ν.

Class	TRS	PHS	CS	Protocol	Parameters	ν
BDI	$\mathcal{T}^2 = 1$	$\mathcal{P}^2 = 1$	$(\Gamma^{y}_{\theta_1})^2 = 1$	$T_1R_y(\theta_2)T_0R_y(\theta_1)$	$\theta_1 = -\pi/2, \theta_2 = 3\pi/4$	$\nu = 0$
					$\theta_1 = -\pi/2, \theta_2 = \pi/4$	$\nu = 1$
AIII	Absent	Absent	$(\Gamma^{\alpha}_{\theta_1})^2 = 1$	$T_1R_\alpha(\theta_2)T_0R_\alpha(\theta_1)$	$\theta_1 = \pi/2, \theta_2 = 3\pi/4$	$\nu = 0$
					$\theta_1 = \pi/2, \theta_2 = \pi/4$	$\nu = 1$

Table 5.1: Classes with CS in 1D and the respective QW protocols. The values of the parameters θ_1 and θ_2 that correspond to distinct topological phases are shown, as well as the respective winding numbers ν of each phase.

5.2 Boltzmann-Gibbs density operators

In the previous section, we described how QWs simulate topological phases of free-fermion systems at zero temperature. What we wish to investigate is wether they can also be used to infer the topological behaviour of such systems at finite temperatures. To do that, we study two types of BG-like states for many-body systems, as well as their single-particle counterparts, with respect to the effective Hamiltonian of the topological QW. Since topological QWs can be realised as periodically driven systems, it is natural to ask if such states can be considered in this context, since the energy is not conserved and the quasienergies (defined modulo 2π) which are conserved, have no natural ordering. It has been shown that these states, called Floquet-Gibbs states, can emerge under certain conditions [**?** **?**] (see also the justification for the existence of a "quasienergy Brillouin zone" in the previous section). Moreover, regardless of the realisations using periodically driven systems, the QWs that we consider can also be achieved by means of time-independent effective Hamiltonians (which were subject of a number of theoretical studies [**?** **?** **?**], and also experimentally realised [**?** **?**]), for which the BG states are well defined.

Let us consider a collection of fermion creation and annihilation operators $\{\psi_{k\sigma}, \psi^\dagger_{k\sigma} : k \in \mathcal{B},\ \sigma \in \{\uparrow, \downarrow\}\}$ and form the spinors $\Psi_k = (\psi_{k\uparrow}, \psi_{k\downarrow})^T$. The first state that we consider is the canonical ensemble given by,

$$\varrho^{(0)} = \frac{e^{-\beta\mathcal{H}}}{\mathcal{Z}^{(0)}} = \frac{1}{\mathcal{Z}^{(0)}} \prod_{k\in\mathcal{B}} \exp\Big(-\beta \Psi^\dagger_k H_k \Psi_k\Big), \tag{5.11}$$

where $\mathcal{H}$ is the sum over the momenta of quadratic Hamiltonians $\mathcal{H} = \sum_k \Psi^\dagger_k H_k \Psi_k$, H_k is given by Equation (5.6), and $\mathcal{Z}^{(0)} = \mathrm{tr}\big(e^{-\beta\mathcal{H}}\big)$ is the corresponding partition function (note that $\mathcal{H}$ conserves the particle number and its action on the whole Hilbert space is determined by the action on the single-particle sector). This state maximises the von Neumann entropy, subject to the constraint $\langle\mathcal{H}\rangle = \text{const}$.

The second state that we consider is obtained when one maximises the von Neumann entropy, subject to two constraints: the above mentioned energy constraint, as well as the constraints on the average number of particles $\langle n_k\rangle = \langle\Psi^\dagger_k\Psi_k\rangle$ which are constant in time, but in general different for each k. This state is of the form:

$$\varrho^{(1)} = \frac{e^{-\beta\mathcal{O}}}{\mathcal{Z}^{(1)}} = \frac{1}{\mathcal{Z}^{(1)}} \prod_{k\in\mathcal{B}} \exp\Big[-\beta(\Psi^\dagger_k H_k \Psi_k - \mu_k \Psi^\dagger_k \Psi_k)\Big], \tag{5.12}$$

where $\mathcal{O} = \sum_k \mathcal{O}_k = \sum_k \mathcal{H}_k - \mu_k n_k$, with $\mu_k = -(1/\beta)\log(Z_k)$ being a momentum dependent chemical potential (which, in this case, coincides with the Helmholtz free energy associated to momentum k), and $\mathcal{Z}^{(1)} = \mathrm{tr}\big(e^{-\beta\mathcal{O}}\big)$ is the corresponding partition func-

tion. For details concerning the derivation of these states or, more generally, of states maximising the von Neumann entropy subject to constraints, cf. the appendix of [**?**]. In the field of quantum integrable systems, the state $\varrho^{(1)}$ is known as the "generalised Gibbs ensemble", which was introduced in [**?** **?**] (for a review, see [**?**]).

Since the previous zero-temperature studies (both theoretical and experimental) of symmetry-protected topological orders were conducted for single-particle QWs, we present the corresponding single-particle counterparts $\rho^{(0)}$ and $\rho^{(1)}$ of the many-body states given by Equations (5.11) and (5.12), respectively.

The first is the standard thermal state, resulting from the effective Hamiltonian of the QW:

$$\rho^{(0)} \quad = \tfrac{e^{-\beta H_{\text{eff}}}}{Z} = \tfrac{1}{Z} \textstyle\sum_{k\in\mathcal{B}} e^{-\beta H_k} \otimes |k\rangle \langle k| \,, \tag{5.13}$$

where $Z = \operatorname{tr} e^{-\beta H_{\text{eff}}}$, while the second is:

$$\rho^{(1)} = \frac{1}{\Omega} \sum_{k\in\mathcal{B}} \frac{e^{-\beta H_k}}{Z_k} \otimes |k\rangle \langle k| = \frac{1}{\Omega} \sum_{k\in\mathcal{B}} \rho_k \otimes |k\rangle \langle k| \,, \tag{5.14}$$

where $Z_k = \operatorname{tr} e^{-\beta H_k}$ and $\Omega = \sum_k 1$ is the k-space volume. Note that by tracing out the momenta, the state $\rho^{(0)}$ remains to be of the BG form (it is "globally", with respect to k, thermal-like), while $\rho^{(1)}$ is not – only by measuring the momenta, the state collapses to a "local" BG form ρ_k. Notice also that $Z = \sum_k Z_k$. The difference between $\rho^{(0)}$ and $\rho^{(1)}$ becomes even more clear by looking at their asymptotic behaviours. Namely, when $\beta \to +\infty$

$$\rho^{(0)} \to \frac{1}{|M|} \sum_{k\in M} |-\vec{n}_k\rangle \langle -\vec{n}_k| \otimes |k\rangle \langle k| \,, \tag{5.15}$$

where $M = \{k_* \in \mathcal{B} : E(k_*) = \max_{k\in\mathcal{B}} E(k)\}$ is the set of momenta minimising the lower band dispersion and $|-\vec{n}_k\rangle$ is defined in Equation (5.6), while

$$\rho^{(1)} \to \frac{1}{\Omega} \sum_{k\in\mathcal{B}} |-\vec{n}_k\rangle \langle -\vec{n}_k| \otimes |k\rangle \langle k| \,, \tag{5.16}$$

is a statistical mixture of the *entire* lower band of the Hamiltonian.

Note that there exists a bijection between single-particle and quadratic many-body Hamiltonians, given by $H_k \leftrightarrow \mathcal{H}_k = \Psi_k^\dagger H_k \Psi_k$, where the left arrow represents the projection onto the single-particle sector, thus inducing the corresponding bijections between the BG states $\rho^{(0)} \leftrightarrow \varrho^{(0)}$ and $\rho^{(1)} \leftrightarrow \varrho^{(1)}$.

5.3 Fidelity and Δ analysis

In our analysis, we study the overall quantum states over the parameter space denoted by $\vec{q} = (\beta^{-1}, \theta)$, including the temperature and the parameter of the Hamiltonian that drives the topological PT. Recall that we have fixed the value of θ_1 for both classes BDI and AIII, so in what follows θ stands for θ_2, which is the angle that we vary in order to drive the topological PT. We consider the fidelity F and the quantity Δ between two states ρ and ρ' separated in the parameters' space by an "infinitesimal" displacement: namely $F(\rho, \rho')$ and $\Delta(\rho, \rho')$, where prime denotes the "infinitesimally" close parameters. We can consider three different cases. In the first case, which is the most general, we probe the system with respect to both the parameter θ and the temperature T on the same time, that is

$$\rho' = \rho(\vec{q}\prime) = \rho(\vec{q} + \delta\vec{q}),$$

with $\delta\vec{q} = (\delta\theta, \delta T)$ and $||\delta\vec{q}|| << ||\vec{q}||$, since $|\delta\theta| << |\theta|$ and $|\delta T| << |T|$. The other two cases occur when we wish to probe the system with respect to the parameter of the Hamiltonian and the temperature separately, these are for $\delta\vec{q} = (\delta\theta, 0)$ and $\delta\vec{q} = (0, \delta T)$, respectively. The analytic derivation of the expressions for F and Δ in the first general case, where we simultaneously probe the parameter θ and the temperature, was performed according to the method presented in Appendix A. For the specific many-body and single-particle BG states, considered in this chapter, this analysis yielded the following closed expressions for the fidelity:

$$F(\varrho^{(0)}, \varrho'^{(0)}) = \prod_{k\in\mathcal{B}} \frac{2 + \sqrt{2\left(1 + \cosh(E_k/2T)\cosh(E'_k/2T') + \sinh(E_k/2T)\sinh(E'_k/2T')\vec{n}_k \cdot \vec{n}'_k\right)}}{\sqrt{[2 + 2\cosh(E_k/2T)][2 + 2\cosh(E'_k/2T')]}}, \tag{5.17}$$

$$\begin{aligned} F(\varrho^{(1)}, \varrho'^{(1)}) = \prod_{k\in\mathcal{B}} \Bigg(1 + \frac{2(1+\cosh(E_k/2T)\cosh\left(E'_k/2T'\right)+\sinh(E_k/2T)\sinh\left(E'_k/2T'\right)\vec{n}_k\cdot\vec{n}'_k)}{\sqrt{(2\cosh(E_k/2T))(2\cosh\left(E'_k/2T'\right))}} \\ + \frac{1}{(2\cosh(E_k/2T))(2\cosh\left(E'_k/2T'\right))}\Bigg) \\ \times \left(\sqrt{[2 + (2\cosh(E_k/2T))^{-2}][2 + (2\cosh(E'_k/2T'))^{-2}]}\right)^{-1}, \end{aligned} \tag{5.18}$$

$$F(\rho^{(0)}, \rho'^{(0)}) = \frac{\sum_{k\in\mathcal{B}} \sqrt{2\left(1 + \cosh(E_k/2T)\cosh(E'_k/2T') + \sinh(E_k/2T)\sinh(E'_k/2T')\vec{n}_k \cdot \vec{n}'_k\right)}}{\sqrt{\sum_{k\in\mathcal{B}} 2\cosh(E_k/2T)\sum_{k\in\mathcal{B}} 2\cosh(E'_k/2T')}}, \tag{5.19}$$

$$F(\rho^{(1)},\rho'^{(1)})=\sum_{k\in\mathcal{B}}\frac{\sqrt{2\left(1+\cosh(E_k/2T)\cosh(E'_k/2T')+\sinh(E_k/2T)\sinh(E'_k/2T')\vec{n}_k\cdot\vec{n}'_k\right)}}{\sqrt{2\cosh(E_k/2T)2\cosh(E'_k/2T')}}. \tag{5.20}$$

To compute the quantity $\Delta(\rho,\rho')$ we need, in addition, $\mathrm{tr}\,\sqrt{\rho}\sqrt{\rho'}$, which we calculated along the same lines to be:

$$\mathrm{tr}\,\sqrt{\varrho^{(0)}}\sqrt{\varrho'^{(0)}}=\prod_{k\in\mathcal{B}}\frac{2+2\left(\cosh(E_k/4T)\cosh(E'_k/4T')+\sinh(E_k/4T)\sinh(E'_k/4T')\vec{n}_k\cdot\vec{n}'_k\right)}{\sqrt{(2+2\cosh(E_k/2T))(2+2\cosh(E'_k/2T'))}}, \tag{5.21}$$

$$\begin{aligned}\mathrm{tr}\,\sqrt{\varrho^{(1)}}\sqrt{\varrho'^{(1)}} &= \prod_{k\in\mathcal{B}}\left(1+\frac{2\left(\cosh(E_k/4T)\cosh\left(E'_k/4T'\right)+\sinh(E_k/4T)\sinh\left(E'_k/4T'\right)\vec{n}_k\cdot\vec{n}'_k\right)}{\sqrt{(2\cosh(E_k/2T))(2\cosh\left(E'_k/2T'\right))}}\right.\\ &\qquad\left.+\frac{1}{(2\cosh(E_k/2T))(2\cosh\left(E'_k/2T'\right))}\right)\\ &\quad\times\left(\sqrt{[2+(2\cosh(E_k/2T))^{-2}][2+(2\cosh(E'_k/2T'))^{-2}]}\right)^{-1},\end{aligned} \tag{5.22}$$

$$\mathrm{tr}\,\sqrt{\rho^{(0)}}\sqrt{\rho'^{(0)}}=\frac{\sum_{k\in\mathcal{B}}2\left(\cosh(E_k/4T)\cosh(E'_k/4T')+\sinh(E_k/4T)\sinh(E'_k/4T')\vec{n}_k\cdot\vec{n}'_k\right)}{\sqrt{\sum_{k\in\mathcal{B}}2\cosh(E_k/2T)}\sqrt{\sum_{k\in\mathcal{B}}2\cosh(E'_k/2T')}}, \tag{5.23}$$

$$\mathrm{tr}\,\sqrt{\rho^{(1)}}\sqrt{\rho'^{(1)}}=\sum_{k\in\mathcal{B}}\frac{2\left(\cosh(E_k/4T)\cosh(E'_k/4T')+\sinh(E_k/4T)\sinh(E'_k/4T')\vec{n}_k\cdot\vec{n}'_k\right)}{\sqrt{2\cosh(E_k/2T)}\sqrt{2\cosh(E'_k/2T')}}. \tag{5.24}$$

The quantitative results for the representative of the class BDI are given in Figure 5.1 and the results for the representative of the AIII class are shown in Figure 5.2. For both classes, the quantitative results are obtained in the most general case, for which $\delta\vec{q}=(\delta\theta,\delta T)=(0.01,0.01)$. In what follows we also comment on the results obtained for the other two cases $\delta\vec{q}=(\delta\theta,0)=(0.01,0)$ and $\delta\vec{q}=(0,\delta T)=(0,0.01)$, however we do not present them, as they are qualitatively similar.

A unique feature of periodically driven systems and their corresponding effective Hamiltonians is that both energies $E_k=0$ and $E_k=\pi$ correspond to a closed gap (the difference between the two energy levels $\pm E_k$ becomes zero modulo 2π). This special feature of QWs yields a surprising result in our analysis. In our study, we observe a different behaviour of

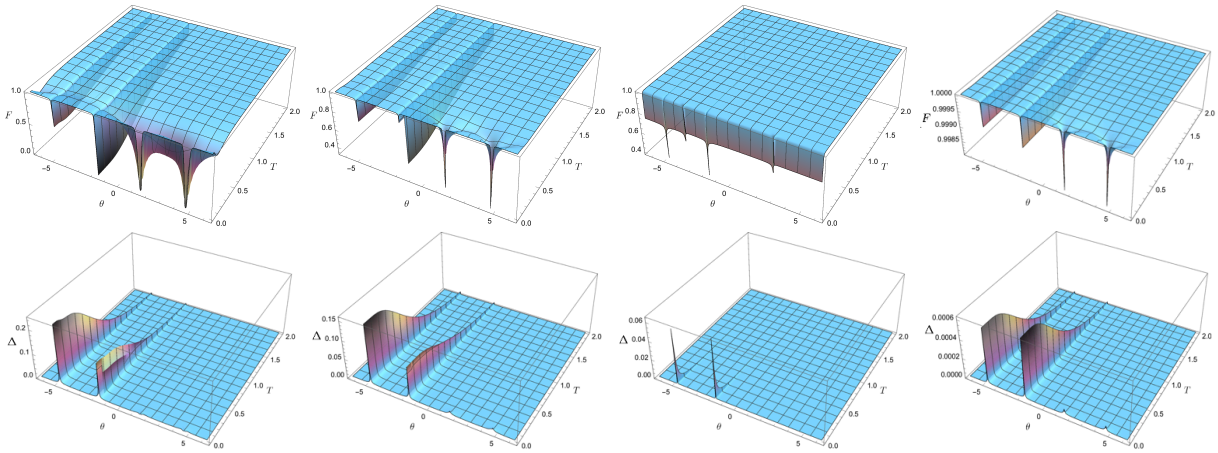

Figure 5.1: Fidelity (top) and Δ (bottom) for the many-body states $\varrho^{(0)}$ (left) and $\varrho^{(1)}$ (middle-left) and the single-particle states $\rho^{(0)}$ (middle-right) and $\rho^{(1)}$ (right), for the BDI symmetry class. $\delta\theta = \theta' - \theta = 0.01$ and $\delta T = T' - T = 0.01$. The small step in the top middle-left plot is due to numerical instability.

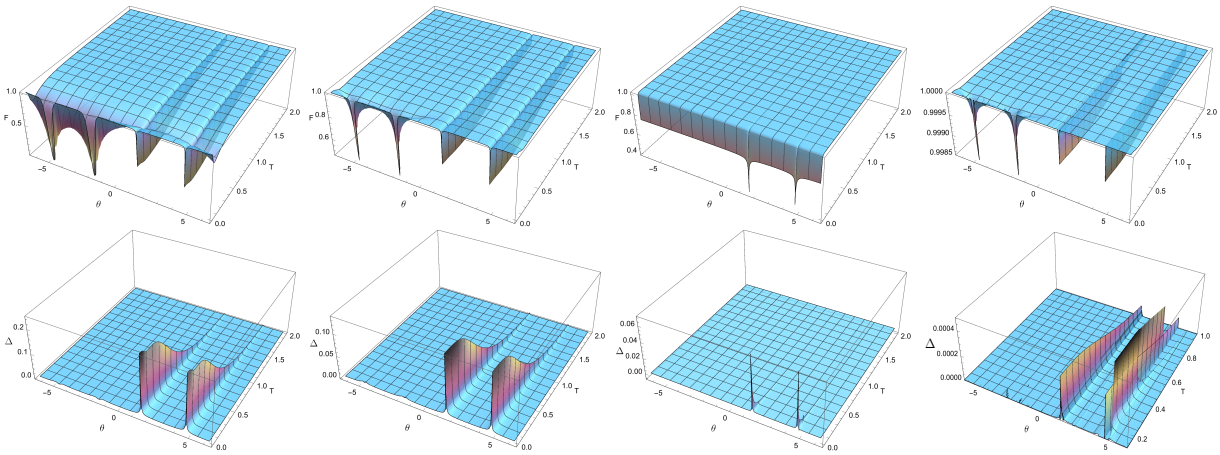

Figure 5.2: Fidelity (top) and Δ (bottom) for the many-body states $\varrho^{(0)}$ (left) and $\varrho^{(1)}$ (middle-left), and the single-particle states $\rho^{(0)}$ (middle-right) and $\rho^{(1)}$ (right), for the AIII symmetry class. $\delta\theta = \theta' - \theta = 0.01$ and $\delta T = T' - T = 0.01$. In the case of the state $\rho^{(1)}$, the quantity Δ is highly oscillating for temperatures close to 0 in the neighbourhood of the critical points, therefore we show the results for a range of temperatures where these numerical instabilities are less prominent.

the gap closing points with temperature, depending on whether they correspond to $E_k = 0$ (the two points with $\theta > 0$) or $E_k = \pi$ energy (the two points with $\theta < 0$). Whenever the gap closes, the vector $\vec{n}_k(\theta)$ is ill-defined, but the behaviour of F and Δ will be different due to their dependence on the entire energy spectrum. For the case of $E_k = 0$, they signal two isolated zero-temperature points of quantum PTs, corresponding to $\theta = \pi/2,\ 3\pi/2$ (in the case of Δ we notice small, but still present, peaks at these points). As the temperature increases, they are no longer signalling a PT and this is due to the dependence on the hyperbolic sine of E_k, which vanishes for $E_k = 0$ (see the respective formulae), thus

eliminating the $\vec{n}_k \cdot \vec{n}'_k$ term carrying the relevant topological features. The significance of these points of the zero-temperature quantum PTs on the system in the low-temperature regime, and the existence of possible crossovers, remain as open questions and require further investigation. In contrast to that, for the $E_k = \pi$ gap closing points, the PT lines survive with temperature, hence revealing a "finite-temperature quantum PT" (a PT occurring at finite temperature, driven solely by the Hamiltonian's parameter(s), and not the temperature). Again, this can be understood through the dependence on E_k via hyperbolic functions which take finite values for $E_k = \pi$, thus maintaining the dependence on $\vec{n}_k \cdot \vec{n}'_k$.

Notice that for $\rho^{(0)}$ the qualitative behaviour is different from the other three types of states: the fidelity does not drop for $T = 0$ and $\theta = \pi/2, 3\pi/2$, while it does for two new $T = 0$ points at $\theta = \pm\pi$. The first difference is due to the fact that the zero temperature limit of $\rho^{(0)}$ projects only onto M given by the points of minimum energy $-E_k = -\pi$, see Equation (5.15). Thus, both quantities do not see the critical momentum at which the gap closes at zero energy, which is above the lowest mode. The abrupt change of the fidelity at the points where $\theta = \pm\pi$ is the consequence of the enhanced zero-temperature ground state distinguishability due to the fact that E_k becomes constant and independent of k, i.e., the zero-temperature state projects onto the whole Brillouin zone ($M(\theta = \pm\pi) = \mathcal{B}$). Notice also that in the respective plot for Δ, the absence of peaks at $\theta = \pm\pi$ is consistent with the fact that the Uhlmann factor quantifies the change of eigenvectors, while the presence of two peaks at the corresponding fidelity plot is due to the flattening of the spectrum, i.e., solely to the change of eigenvalues. Observe that while the results for the representatives of BDI and AIII classes are qualitatively similar, the zero-temperature fidelity corresponding to the $\rho^{(0)}$ states for the AIII representative only exhibits drops in the gap closing points ($-E_k = -\pi$), as the spectrum is always non-trivially k-dependent.

Let us now comment on the results for the fidelity and the quantity Δ, in the case where we probe the system with respect to the parameter of the Hamiltonian and the temperature, separately. In the first case, where $\delta\theta = 0.01$ and $\delta T = 0$ ($\delta\vec{q} = (0.01, 0)$), the results are qualitatively the same as the ones presented in Figures 5.1 and 5.2 for $\delta\vec{q} = (0.01, 0.01)$. In the second case, where we probe the system only with respect to temperature, that is $\delta\theta = 0, \delta T = 0.01$ or more concisely $\delta\vec{q} = (0, 0.01)$, the results for the fidelity are qualitatively the same as the ones for $\delta\vec{q} = (0.01, 0.01)$, while the results for the quantity Δ are different. In particular, we obtain that Δ is equal to zero everywhere. This triviality is due to the fact that Δ quantifies the difference between the eigenbases of ρ and ρ', as mentioned before and in this case that we only change the temperature and not the parameter of the Hamiltonian, the eigenbasis remains the same. On the other hand, the fidelity drops at the points of the PT, since it is also sensitive to changes in the

spectrum. Notice that the results for these two cases are in agreement with the results presented in the previous Chapter 4, which were also obtained by separately probing the system with respect to the temperature and the Hamiltonian parameter.

5.4 The edge states

We proceed to our study of the edge states. The bulk-to-boundary correspondence principle [**?** **?**] predicts their existence on the boundary between distinct topological phases. These states are symmetry protected, i.e., they are robust against perturbations of the Hamiltonian which respect the symmetries of the system. In the case of pure states, QWs realise the aforementioned principle as shown in [**?** **?**]. In particular, the authors made θ change along the line, as $\theta(x) = \theta^{(t)}H(x_0 - x) + \theta^{(n)}H(x - x_0)$, where $H(x - x_0)$ is the Heaviside step function and $\theta^{(t/n)}$ are the values of the angle for the trivial/non-trivial phase, respectively. This way, they were able to create a phase boundary at the site x_0 of the line, where θ changes. The edge states are then observed by evolving the walk *in time* from the initial state localised at the phase boundary: the probability to find the system in the initial position keeps being (considerably) higher than for the rest of the line, due to the overlap between the initial state with the edge state that is localised there.

In our case, we are interested in probing the robustness of the edge states with respect to temperature. Therefore, we study an ensemble of the BG type which corresponds to a stationary state of the split-step QWs realising the BDI and AIII class representatives, with the position-dependent coin operation, parameterised by its temperature β^{-1}. This stationary state appears naturally if one looks at the von Neumann evolution equation for the density matrix and imposes the stationarity condition. By diagonalising H_{eff} we obtain the localised states which can either have quasienergy 0 or π. Here, we choose a different order for the energy spectrum, by promoting the edge states with energies $E = \pi$ and $E = 0$ to be ground states, so that they survive at the zero-temperature limit.

We observe that at $T = 0$, the edge state has the major contribution to the probability distribution. As temperature increases, the edge states are smeared out, see Figure 5.3 for the BDI class representative and Figure 5.4 for the representative of the class AIII. Since the presence of an edge state is a clear manifestation of the topological order at $T = 0$, the fact that it does not disappear for higher temperatures, but it is rather smeared out, suggests that the topological nature of the system is preserved in agreement with the fidelity and Δ analysis for the $E_k = \pi$ gap-closing points.

Our fidelity and Δ analysis revealed that for $T > 0$ there exist no thermal PTs (i.e., no temperature-driven PTs), as also shown in Chapter 4 for paradigmatic models of TIs and TSCs. However, here we observe finite temperature *parameter*-driven PTs. The non-

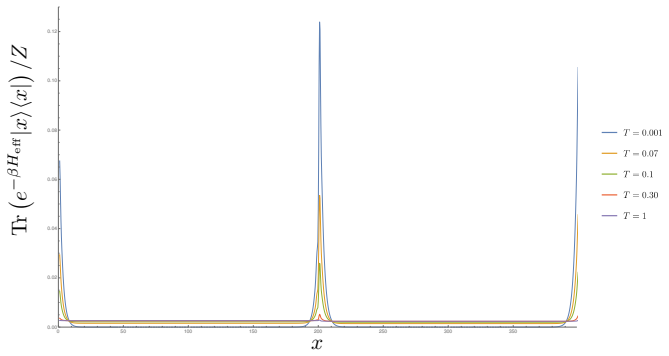

Figure 5.3: Position probability distribution of the QW simulating the representative of the BDI class, as a function of the sites, $\mathrm{tr}\left(e^{-H/T}\,|x\rangle\,\langle x|\right)/Z$. The Hamiltonian H is obtained by varying θ along x through a step-like function [**?**]. The domain wall is centred in the middle of the line. Periodic boundary conditions are taken, hence the edge state at the boundary.

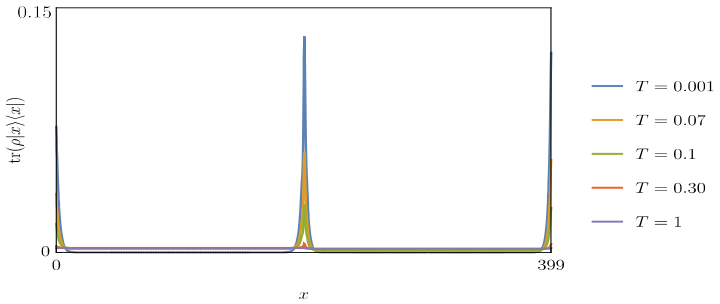

Figure 5.4: Position probability distribution of the QW simulating the representative of the AIII class, as a function of the sites, $\mathrm{tr}\left(e^{-H/T}\,|x\rangle\,\langle x|\right)/Z$. Again, the parameter θ of the Hamiltonian, changes along x according to a step-like function [**?**]. The boundary is centred in the middle of the line and periodic boundary conditions are taken.

existence of thermal PTs is further confirmed by the behaviour of the edge states, which are gradually smeared out as temperature increases, as also pointed out in [**?**]. Note that the edge states studied here are probed through a different method from the one used in Chapter 4. There, a small chemical potential was introduced in such a way that the zero-temperature behaviour of the many-body density operator is the projector onto the Fermi sea. Consequently, the existence of the edge states was signalled by the abrupt change in the number operator on the sites where they appeared.

5.5 Conclusions

We derived analytic expressions for the fidelity and the quantity Δ between two BG states for QW representatives of topological phases for the chiral symmetric classes BDI and AIII and their many-body counterparts. For the systems considered, the fidelity is detecting the points where the Bloch vector is ill-defined, which corresponds to the closure of the

gap. Since in our case the phase diagram is such that the closure of the gap always means the change from a trivial phase to a nontrivial one, and vice versa, the fidelity is capturing the topological PT. Our results show the absence of temperature-driven PTs in two ways: through the fidelity analysis and through the behaviour of the edge states appearing on the phase boundary. In addition, the analysis of the fidelity and, through the quantity Δ, the Uhlmann connection shows the existence of finite-temperature PTs driven solely by the Hamiltonian's parameter θ. We would also like to point out that, providing that one of the goals of this study is to investigate the finite-temperature behaviour of topological order in realistic many-body systems, the fact that the behaviour of the single-particle BG states is consistent with that of their many-body counterparts, shows that the analysis of the former can be a useful mathematical tool in the study of the latter.

Finally, we would like to point out some possible future lines of research. First, the same study could be applied to the rest of the symmetry classes in 1D and 2D using the protocols introduced in [**?**]. Further analysis of realistic noise effects that can give rise to these BG states, in particular the single-particle ones, presents another interesting line of research (for a partial answer to this question, see also a recent study of the effects of thermal noise onto single-particle factor states of a topological insulator [**?**]). The above study could also be conducted for 2D QWs, as well as in the realm of multi-particle QWs.

Chapter 6

Phase transitions at finite temperatures of topological systems out of equilibrium

In this chapter, we investigate the existence of finite-temperature PTs in topological systems out of equilibrium. As mentioned in the Introduction, recently, there have been proposed two different approaches to DPTs, which give opposite predictions. Our goal is to compare and contrast these two approaches and clarify which is the one that better captures the many-body nature of these systems. This chapter is organised as follows: in Section 6.1, after a brief introduction to the study of DQPTs in the case of pure states, we proceed by analytically deriving the two different finite-temperature generalisations of the LE (fidelity LE and interferometric LE) and the associated susceptibilities, which give opposite predictions about the fate of DQPTs in the case of mixed states. Subsequently, we specialise this derivation in the case of two-band Hamiltonians, since the topological systems that we are interested in are described by such Hamiltonians. Based on the analysis of the two different dynamical susceptibilities, we compare the two approaches to DPTs, analyse the reasons for their different predictions and argue that the fidelity LE approach is more suitable in the case of realistic many-body systems. In Section 6.2, we present quantitative results for the fidelity-induced first time derivative of the rate function in the case of the 1D SSH model [**?**] of a TI and the 2D Massive Dirac (MD) model of a Chern insulator [**?**]. Finally, in the last section we summarise our results and present our conclusions.

*The work presented in this chapter corresponds to the work published in [**?**].

6.1 Dynamical (quantum) phase transitions and the associated susceptibilities

The authors in [**?**] introduce the concept of DQPTs and illustrate their properties in the case of the transverse-field Ising model. They observe a similarity between the partition function of a quantum system in equilibrium, $Z(\beta) = \mathrm{tr}\big(e^{-\beta H}\big)$, and the overlap amplitude of some time-evolved initial quantum state $|\psi_i\rangle$ with itself, $G(t) = \langle\psi_i|e^{-iHt}|\psi_i\rangle$. During a temperature-driven PT, the abrupt change of the properties of the system is indicated by the non-analyticity of the free energy density $f(\beta) = -\lim_{N\to\infty}\frac{1}{N}\ln Z(\beta)$ at the critical temperature (N being the number of degrees of freedom). It is then possible to establish an analogy with the case of the real-time evolution of a quantum system out of equilibrium, by considering the rate function

$$g(t) = -\frac{1}{N}\log|G(t)|^2, \tag{6.1}$$

where $|G(t)|^2$ is a mixed-state LE, as we detail below. The rate function $g(t)$ may exhibit non-analyticities at some critical times t_c, after a quantum quench.

6.1.1 DQPTs for pure states

At zero temperature, the LE $G(t)$ from Equation (6.1) between the ground state for $\lambda = \lambda_i \in M$ and the evolved state with respect to the Hamiltonian for $\lambda = \lambda_f \in M$ is given by the fidelity between the two states

$$\mathcal{F}(t;\lambda_f,\lambda_i) \equiv |\,\langle\psi(\lambda_i)|\,e^{-itH(\lambda_f)}\,|\psi(\lambda_i)\rangle\,|. \tag{6.2}$$

For $\lambda_i = \lambda_f$, the fidelity is trivial, since the system remains in the same state. Fixing $\lambda_i \equiv \lambda$ and $\lambda_f = \lambda + \delta\lambda$, with $\delta\lambda << 1$, in the $t\to\infty$ limit Equation (6.2) is nothing but the familiar S-matrix with an unperturbed Hamiltonian $H(\lambda)$ and an interaction Hamiltonian $V(\lambda)$, which is approximated by

$$V(\lambda) \equiv H(\lambda_f) - H(\lambda) \approx \frac{\partial H}{\partial\lambda^a}(\lambda)\delta\lambda^a. \tag{6.3}$$

After applying standard perturbation theory techniques (see Appendix B), we obtain

$$\mathcal{F}(t;\lambda_f,\lambda) \approx 1 - \chi_{ab}(t;\lambda)\delta\lambda^a\delta\lambda^b, \tag{6.4}$$

where the dynamical susceptibility $\chi_{ab}(t;\lambda)$ is given by

$$\chi_{ab}(t;\lambda) = \int_0^t \int_0^t dt_2 dt_1 \left(\tfrac{1}{2}\langle\{V_a(t_2), V_b(t_1)\}\rangle - \langle V_a(t_2)\rangle\langle V_b(t_1)\rangle\right), \tag{6.5}$$

with $V_a(t,\lambda) = e^{itH(\lambda)}\partial H/\partial\lambda^a(\lambda)e^{-itH(\lambda)}$ and $\langle *\rangle = \langle\psi(\lambda)| * |\psi(\lambda)\rangle$. The family of symmetric tensors $\{ds^2(t) = \chi_{ab}(t,\lambda)d\lambda^a d\lambda^b\}_{t\in\mathbb{R}}$ defines a family of metrics in the manifold M, which can be seen as pullback metrics of the Bures metric (Fubini-Study metric) in the manifold of pure states [**?**]. Specifically, at time t, the pullback is given by the map $\Phi_t : \lambda_f \mapsto e^{-itH(\lambda_f)}\,|\psi(\lambda)\rangle\,\langle\psi(\lambda)|\,e^{itH(\lambda_f)}$, evaluated at $\lambda_f = \lambda$.

6.1.2 Generalisations at finite temperatures

The generalisation of DQPTs to mixed states is not unique. There are several ways to construct a LE for a general density matrix. In what follows, we derive two finite-temperature generalisations, such that they have the same zero-temperature limit.

Fidelity Loschmidt Echo at $T > 0$

First, we introduce the *fidelity LE* between the state $\rho(\beta;\lambda_i) = e^{-\beta H(\lambda_i)}/\operatorname{tr}\{e^{-\beta H(\lambda_i)}\}$ and the one evolved by the unitary operator $e^{-itH(\lambda_f)}$ as

$$\mathcal{F}(t,\beta;\lambda_i,\lambda_f) = F(\rho(\beta;\lambda_i), e^{-itH(\lambda_f)}\rho(\beta;\lambda_i)e^{itH(\lambda_f)}), \tag{6.6}$$

where $F(\rho,\sigma) = \operatorname{tr}\{\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\}$ is the quantum fidelity between arbitrary mixed states ρ and σ. For λ_f close to $\lambda_i = \lambda$, we can write

$$\mathcal{F}(t,\beta;\lambda_f,\lambda) \approx 1 - \chi_{ab}(t,\beta;\lambda)\delta\lambda^a\delta\lambda^b, \tag{6.7}$$

with $\chi_{ab}(t,\beta,\lambda)$ being the *Dynamical Fidelity Susceptibility* (DFS). Notice that

$$\lim_{\beta\to\infty}\chi_{ab}(t,\beta;\lambda) = \chi_{ab}(t;\lambda),$$

where $\chi_{ab}(t;\lambda)$ is given by Equation (6.5). At time t and inverse temperature β, we have a map $\Phi_{(t,\beta)} : \lambda_f \mapsto e^{-itH(\lambda_f)}\rho(\beta;\lambda)e^{itH(\lambda_f)}$. The 2-parameter family of metrics defined by $ds^2(\beta,t) = \chi_{ab}(t,\beta;\lambda)d\lambda^a d\lambda^b$ is the pullback by $\Phi_{(t,\beta)}$ of the Bures metric on the manifold of full-rank density operators, evaluated at $\lambda_f = \lambda$ (see Appendix B).

The fidelity LE is closely related to the Uhlmann connection: $F(\rho_1,\rho_2)$ equals the overlap between purifications W_1 and W_2, $\langle W_1, W_2\rangle = \operatorname{tr}\left\{W_1^\dagger W_2\right\}$, satisfying discrete

parallel transport condition (see, for instance, [**?**]).

Interferometric Loschmidt Echo at $T > 0$

Here, we consider an alternative generalisation of the LE for mixed states [$G(t)$ from Equation (6.1)]. In particular, we define the *interferometric LE* as

$$\mathcal{L}(t, \beta; \lambda_f, \lambda_i) = \left| \frac{\mathrm{tr}\left\{ e^{-\beta H(\lambda_i)} e^{itH(\lambda_i)} e^{-itH(\lambda_f)} \right\}}{\mathrm{tr}\left\{ e^{-\beta H(\lambda_i)} \right\}} \right|. \tag{6.8}$$

The $e^{itH(\lambda_i)}$ factor does not appear at zero temperature, since it just gives a phase which is canceled by taking the absolute value. This differs from previous treatments in the literature [**?**] (see Section 5.5.4 of [**?**], where the variation of the interferometric phase, $\mathrm{tr}\{\rho_0 e^{-itH}\}$, exposes this structure). However, it is convenient to introduce it in order to have the usual form of the perturbation expansion, as will become clear later.

For λ_f close to $\lambda_i = \lambda$, we get

$$\mathcal{L}(t, \beta; \lambda_f, \lambda) \approx \left| \frac{\mathrm{tr}\left\{ e^{-\beta H(\lambda)} T e^{-i \int_0^t dt' V_a(t,\lambda) \delta\lambda^a} \right\}}{\mathrm{tr}\left\{ e^{-\beta H(\lambda)} \right\}} \right|, \tag{6.9}$$

so that the perturbation expansion goes as in Equation (6.5), yielding

$$\mathcal{L}(t, \beta; \lambda_f, \lambda) \approx 1 - \tilde{\chi}_{ab}(t, \beta; \lambda) \delta\lambda^a \delta\lambda^b, \tag{6.10}$$

with the dynamical susceptibility given by

$$\tilde{\chi}_{ab}(t, \beta; \lambda) = \int_0^t \int_0^t dt_2 dt_1 \left(\frac{1}{2} \langle \{ V_a(t_2), V_b(t_1) \} \rangle - \langle V_a(t_2) \rangle \langle V_b(t_1) \rangle \right), \tag{6.11}$$

where $\langle * \rangle = \mathrm{tr}\{e^{-\beta H(\lambda)} * \} / \mathrm{tr}\{e^{-\beta H(\lambda)}\}$. Notice that Equations (6.11) and (6.5) are formally the same with the average over the ground state replaced by the thermal average. This justifies the extra $e^{itH(\lambda_i)}$ factor. Since this susceptibility comes from the interferometric LE, we call it *Dynamical Interferometric Susceptibility* (DIS). The quantity $ds^2(\beta, t) = \tilde{\chi}_{ab}(t, \beta; \lambda) d\lambda^a d\lambda^b$ defines a 2-parameter family of metrics over the manifold M, except that they cannot be seen as pullbacks of metrics on the manifold of density operators with full rank. However, it can be interpreted as the pullback by a map from M to the unitary group associated with the Hilbert space of a particular Riemannian metric. For a detailed analysis, see Appendix B. Note that this version of the LE is related to the interferometric geometric phase introduced by Sjöqvist *et. al* [**?** **?**].

6.1.3 Two-band systems

Many representative examples of TIs and TSCs can be described by effective two-band Hamiltonians. Therefore, we derive closed expressions of the previously introduced dynamical susceptibilities for topological systems within this class.

The general form of such Hamiltonians is $\{H(\lambda) = \vec{x}(\lambda) \cdot \vec{\sigma} : \lambda \in M\}$, where $\vec{\sigma}$ is the Pauli vector. The interaction Hamiltonian $V(\lambda)$, introduced in Equation (6.2), casts the form

$$V(\lambda) \approx \left(\frac{\partial \vec{x}}{\partial \lambda^a} \cdot \vec{\sigma} \right) \delta\lambda^a.$$

It is convenient to decompose $\partial\vec{x}/\partial\lambda^a$ into one component perpendicular to $\vec{x}$ and one parallel to it:

$$\frac{\partial \vec{x}}{\partial \lambda^a} = \left(\frac{\partial \vec{x}}{\partial \lambda^a} \right)^{\perp} + \left(\frac{\partial \vec{x}}{\partial \lambda^a} \right)^{\parallel} = \vec{t}_a + \vec{n}_a.$$

The first term is tangent, in $\mathbb{R}^3$, at $\vec{x}(\lambda)$, to a sphere of constant radius $r = |\vec{x}(\lambda)|$. Hence, this kind of perturbations does not change the spectrum of H, only its eigenbasis. The second term is a variation of the length of $\vec{x}$ and hence, it changes the spectrum of H, while keeping the eigenbasis fixed. The DFS and the DIS are given by (for the details of the derivation, see Appendix B)

$$\chi_{ab} = \tanh^2(\beta|\vec{x}(\lambda)|) \frac{\sin^2(|\vec{x}(\lambda)|t)}{|\vec{x}(\lambda)|^2} \vec{t}_a \cdot \vec{t}_b \tag{6.12}$$

$$\tilde{\chi}_{ab} = \frac{\sin^2(|\vec{x}(\lambda)|t)}{|\vec{x}(\lambda)|^2} \vec{t}_a \cdot \vec{t}_b + t^2 (1 - \tanh^2(\beta|\vec{x}(\lambda)|)) \vec{n}_a \vec{n}_b. \tag{6.13}$$

While the DIS from Equation (6.13) depends on the variation of both the spectrum and the eigenbasis of the Hamiltonian, the DFS from Equation (6.12) depends only on the variations which preserve the spectrum, i.e., changes in the eigenbasis. This is quite remarkable, since in general the fidelity between two quantum states, being their distinguishability measure, does depend on both the variations of the spectrum and the eigenbasis. In our particular case of a quenched system, the eigenvalues are preserved (see Equation (6.6)), as the system is subject to a unitary evolution. The tangential components of both susceptibilities are modulated by the function $\sin^2(Et)/E^2$, where E is the gap. This captures the *Fisher zeros*, i.e., the zeros of the (dynamical) partition function which here is given by the fidelity $\mathcal{F}$ from Equation (6.6), see [**? ? ?**]. Observe that whenever $t = (2n+1)\pi/2E$, $n \in \mathbb{Z}$, this factor is maximal and hence, both LEs decrease abruptly. The difference between the two susceptibilities is given by

$$\tilde{\chi}_{ab} - \chi_{ab} = (1 - \tanh^2(\beta|\vec{x}(\lambda)|)) \left(\frac{\sin^2(|\vec{x}(\lambda)|t)}{|\vec{x}(\lambda)|^2} \vec{t}_a \cdot \vec{t}_b + t^2 \vec{n}_a \cdot \vec{n}_b \right).$$

The quantity $(1 - \tanh^2(\beta E))$ is nothing but the static susceptibility, see [**?**]. Therefore, the difference between DIS and DFS is modulated by the static susceptibility at finite temperature.

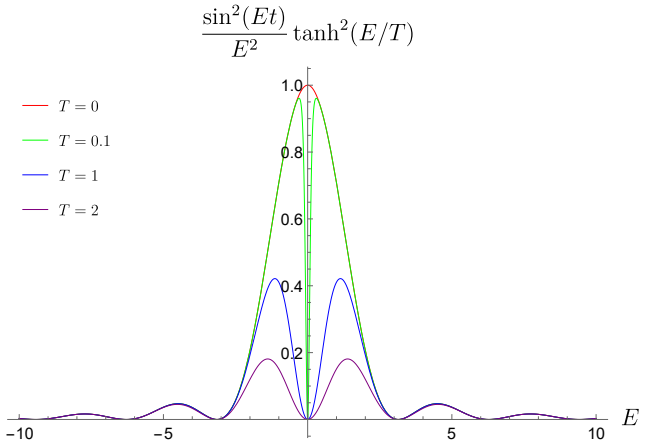

Figure 6.1: The susceptibility modulating function for the tangential components at $t = 1$.

To illustrate the relationship between the two susceptibilities, in Figure 6.1 we plotted the modulating function for the tangential components of both. We observe that at zero temperature they coincide. As the temperature increases, in the case of the fidelity LE, the gap-vanishing points become less important. On the contrary, for the interferometric LE, the associated tangential part of the susceptibility does not depend on temperature, thus the gap-vanishing points remain prominent. The DFS from Equation (6.12) thus predicts gradual smearing of critical behaviour, consistent with our results from the previous two chapters that showed the absence of PTs at finite temperatures in the static case. The DIS from Equation (6.13) has a tangential term that is not coupled to the temperature, persisting at higher temperatures and giving rise to abrupt changes in the finite-temperature system's behaviour. This is also consistent with previous studies in the literature, where DPTs were found even at finite temperatures [**?** **?**]. Additionally, the interferometric LE depends on the normal components of the variation of $\vec{x}$. In other words, the finite-temperature PTs inferred by the behaviour of the interferometric LE occur due to the change of the parameters of the Hamiltonian and not due to temperature.

6.1.4 Comparing the two approaches

The above analysis of the two dynamical susceptibilities (metrics) reflects the essential difference between the two distinguishability measures, one based on the fidelity, the other on interferometric experiments. From the quantum information theoretical point of view,

the two quantities can be interpreted as distances between *states*, or between *processes*, respectively. The Hamiltonian evaluated at a certain point of parameter space M defines the macroscopic phase. Associated to it we have thermal states and unitary processes. The fidelity LE is obtained from the Bures distance between a thermal state ρ_1 in phase 1 and the one obtained by unitarily evolving this state, $\rho_2 = U_2\rho_1 U_2^\dagger$, with U_2 associated to phase 2. Given a thermal state ρ_1 prepared in phase 1, the interferometric LE is obtained from the distance between two unitary processes U_1 and U_2 (defined modulo a phase factor), associated to phases 1 and 2.

The quantum fidelity between two states is in fact the classical fidelity between the probability distributions obtained by performing an optimal measurement on them. Measuring an observable M on the two states ρ_1 and ρ_2, one obtains the probability distributions $\{p_1(i)\}$ and $\{p_2(i)\}$, respectively. The quantum fidelity F_Q between the two states ρ_1 and ρ_2 is bounded by the classical fidelity F_C between the probability distributions $\{p_1(i)\}$ and $\{p_2(i)\}$, $F_Q(\rho_1,\rho_2) = \mathrm{Tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}} \leq \sum_i \sqrt{p_1(i)p_2(i) = F_c(p_1(i),p_2(i))}$, such that the equality is obtained by measuring an *optimal observable*, given by $M_{\mathrm{op}} = \rho_1^{-1/2}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\rho_1^{-1/2}$ (note that optimal observable is not unique). For that reason, one can argue that the fidelity is capturing all order parameters (i.e., measurements) through its optimal observables M_{op}. Fidelity-induced distances, the *Bures distance* $D_B(\rho_1,\rho_2) = \sqrt{2(1-F_Q(\rho_1,\rho_2))}$, the *sine distance* $D_S(\rho_1,\rho_2) = \sqrt{1-F_Q^2(\rho_1,\rho_2)}$ and the *F-distance* $D_F(\rho_1,\rho_2) = 1 - F_Q(\rho_1,\rho_2)$ satisfy the following set of inequalities

$$D_F(\rho_1,\rho_2) \leq D_T(\rho_1,\rho_2) \leq D_S(\rho_1,\rho_2) \leq D_B(\rho_1,\rho_2),$$

where the *trace distance* is given by $D_T(\rho_1,\rho_2) = \frac{1}{2}\mathrm{Tr}|\rho_1 - \rho_2|$. In other words, the fidelity-induced distances and the trace distance establish the same order on the space of quantum states. This is important, as the trace distance is giving the optimal value for the success probability in ambiguously discriminating in a *single shot-measurement* between two *a priori*equally probable states ρ_1 and ρ_2, given by the so-called Helstrom bound $P_H(\rho_1,\rho_2) = (1 + D_T(\rho_1,\rho_2))/2$ [**?**].

On the other hand, the interferometric phase is based on some interferometric experiment to distinguish two states, $\rho_1 = \sum_i r_i |i\rangle\langle i|$ and $\rho_2 = U_2\rho_1 U_2^\dagger$: it measures how the intensities at the outputs of the interferometer are affected by applying U_2 to only one of its arms [**?**]. Therefore, to set up such an experiment, one does not need to know the state ρ_1 that enters the interferometer, as only the knowledge of U_2 is required. Note that this does not mean that the output intensities do not depend on the interferometric LE: indeed, the inner product $\langle U_1, U_2\rangle_{\rho_1}$ is defined with respect to the state ρ_1. This is a different type of experiment, not based on the observation of any physical property of

a system. It is analogous to comparing two masses with weighing scales, which would show the same difference of $\Delta m = m_1 - m_2$, regardless of how large the two masses m_1 and m_2 are. For that reason, interferometric distinguishability is more sensitive than the fidelity (fidelity depends on more information, not only how much the two states are different, but in what aspects this difference is observable). Indeed, the interferometric LE between ρ_1 and ρ_2 can be written as the overlap $L(\rho_1, \rho_2) = |\langle\rho_1|\rho_2\rangle|$ between the purifications $|\rho_1\rangle = \sum_i \sqrt{r_i}|i\rangle|i\rangle$ and $|\rho_2\rangle = (U \otimes I)|\rho_1\rangle$. On the other hand, the fidelity satisfies $F(\rho_1, \rho_2) = \max_{|\psi\rangle,|\varphi\rangle} |\langle\psi|\varphi\rangle|$, where $|\psi\rangle$ and $|\varphi\rangle$ are purifications of ρ_1 and ρ_2, respectively, i.e., $L(\rho_1, \rho_2) \leq F(\rho_1, \rho_2)$. Moreover, what one does observe in interferometric experiments are the mentioned output intensities, i.e., one needs a number of identical systems prepared in the same state to obtain results in interferometric measurements. This additionally explains why interferometric LE is more sensible than the fidelity one, as the latter is based on the observations performed on single systems. The fact that interferometric LE is more sensitive than the fidelity LE is consistent with the result that the former is able to capture the changes of some of the system's features at finite temperatures (thus they predict DPTs), while the latter cannot.

In terms of experimental feasibility, the fidelity is more suitable for the study of many-body macroscopic systems and phenomena, while the interferometric measurements provide a more detailed information on genuinely quantum (microscopic) systems. Finally, interferometric experiments involve coherent superpositions of two states. Therefore, when applied to many-body systems, one would need to create genuine Schrödinger cat-like states, which goes beyond the current, and any foreseeable, technology (and could possibly be forbidden by more fundamental laws of physics; see for example objective collapse theories [**?**]).

6.2 DPTs of topological insulators at finite temperatures

Our general study of two-band Hamiltonians showed that the fidelity-induced LE predicts a gradual smearing of DPTs with temperature. In order to further confirm this result, we study the fidelity LE for two concrete examples of TIs (the analogous study for the interferometric LE on concrete examples has already been performed, and is consistent with our findings [**? ?**]). In particular, we present quantitative results obtained for the first derivative of the rate function, dg/dt, where $g(t) = -\frac{1}{N}\log\mathcal{F}$, and

$$\mathcal{F}(t, \beta; \lambda_i, \lambda_f) = F(\rho(\beta; \lambda_i), e^{-itH(\lambda_f)}\rho(\beta; \lambda_i)e^{itH(\lambda_f)}).$$

The fidelity F is obtained by taking the product of the single-mode fidelities, each of which has the form

$$F(\rho(\beta;\lambda_i), e^{-itH(\lambda_f)}\rho(\beta;\lambda_i)e^{itH(\lambda_f)}) = \sqrt{\frac{1+\cosh^2(\beta E_i)+\sinh^2(\beta E_i)\left[\cos(2E_f t)+(1-\cos(2E_f t))(\vec{n}_i\cdot\vec{n}_f)^2\right]}{2\cosh^2(\beta E_i)}},$$

with $H_a = E_a\vec{n}_a\cdot\vec{\sigma}$ and $a = i, f$. This expression can be obtained by using Equation (22) and the result found in Appendix A. The quantity dg/dt is the figure of merit in the study of the DQPTs, therefore we present the respective results that confirm the previous study: the generalisation of the LE with respect to the fidelity shows the absence of finite-temperature DPTs. The models of TIs that we consider are the SSH [**?**] and the MD [**?**] model.

6.2.1 SSH model (1D)

The SSH model was introduced in [**?**] to describe polyacetilene, and it was later found to describe diatomic polymers [**?**]. In momentum space, the Hamiltonian for this model is of the form $H(k,m) = \vec{x}(k,m)\cdot\vec{\sigma}$, with m being the parameter that drives the static PT. The vector $\vec{x}(k,m)$ is given by:

$$\vec{x}(k,m) = (m+\cos(k), \sin(k), 0).$$

By varying m we find two distinct topological regimes. For $m < m_c = 1$ the system is in a non-trivial phase with winding number 1, while for $m > m_c = 1$ the system is in a topologically trivial phase with winding number 0.

We consider both cases in which we go from a trivial to a topological phase and vice versa (Figures 6.2 and 6.3, respectively). We notice that non-analyticities of the first derivative appear at zero temperature, and they are smeared out for higher temperatures.

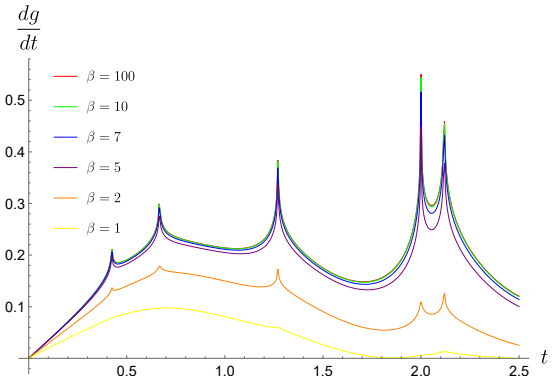

Figure 6.2: We plot the time derivative of the rate function, dg/dt, as a function of time for different values of the inverse temperature $\beta = 1/T$. We consider a quantum quench from a trivial phase ($m = 1.2$) to a topological phase ($m = 0.8$).

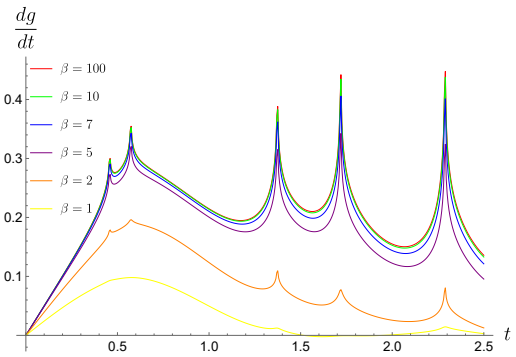

Figure 6.3: The time derivative of the rate function, dg/dt, as a function of time for different values of the inverse temperature. The quench is from a topological ($m = 0.8$) to a trivial phase ($m = 1.2$).

6.2.2 MD model (2D)

The Massive Dirac model (MDM) captures the physics of a 2D Chern insulator [**?**], and features several different topologically distinct phases. In momentum space, the Hamiltonian for the MDM is of the form $H(\vec{k}, m) = \vec{x}(\vec{k}, m)\cdot\vec{\sigma}$, with m being the parameter that drives the static PT. The vector $\vec{x}(\vec{k}, m)$ is given by

$$\vec{x}(\vec{k}, m) = (\sin(k_x), \sin(k_y), m - \cos(k_x) - \cos(k_y)).$$

By varying m we find four different topological regimes:

- For $-\infty < m < m_{c_1} = -2$ it is trivial (the Chern number is zero) – Regime I
- For $-2 = m_{c_1} < m < m_{c_2} = 0$ it is topological (the Chern number is -1) – Regime II
- For $0 = m_{c_2} < m < m_{c_3} = 2$ it is topological (the Chern number is $+1$) – Regime III
- For $2 = m_{c_3} < m < \infty$ it is trivial (the Chern number is zero) – Regime IV

In Figures 6.4, 6.5 and 6.6 we plot the first derivative of the rate function $g(t)$, as a function of time for different temperatures. We only consider quenches that traverse a single PT point.

We observe that at zero temperature there exist non-analyticities at the critical times – the signatures of DQPTs. As we increase the temperature, these non-analyticities are gradually smeared out, resulting in smooth curves for higher finite temperatures. We note

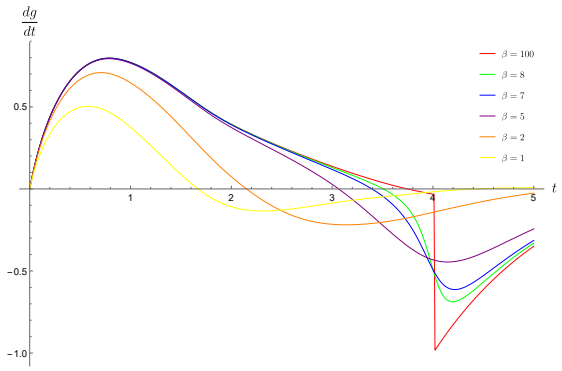

Figure 6.4: The time derivative of the rate function, dg/dt, as a function of time for different values of the inverse temperature. We quench the system from a trivial to a topological regime (Regimes from I to II and from IV to III).

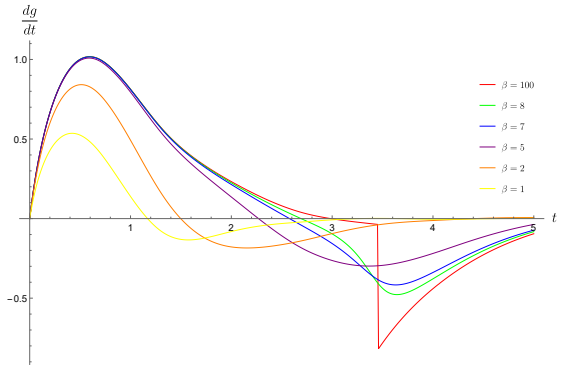

Figure 6.5: The time derivative of the rate function, dg/dt, as a function of time for different values of the inverse temperature. The quench is from a topological to a trivial regime (Regimes from II to I and from III to IV).

that the peak of the derivative $dg(t)/dt$ is drifted when increasing the temperature, in analogy to the usual drift of static quantum PTs at finite temperature [**?**].

Next, we proceed by considering the cases in which we cross two PT points, as shown in Figures 6.7 and 6.8. At zero temperature we obtain a non-analytic behaviour, which gradually disappears for higher temperatures.

Finally, we have also studied the case in which we move inside the same topological regime from left to right and vice versa. We obtained smooth curves without non-analyticities, which we omit for the sake of briefness.

6.3 Conclusions

In this chapter, we analysed the fidelity and the interferometric generalisations of the LE for general mixed states, and applied them to the study of finite temperature DPTs in topological systems. We showed that the dynamical fidelity susceptibility is the pullback

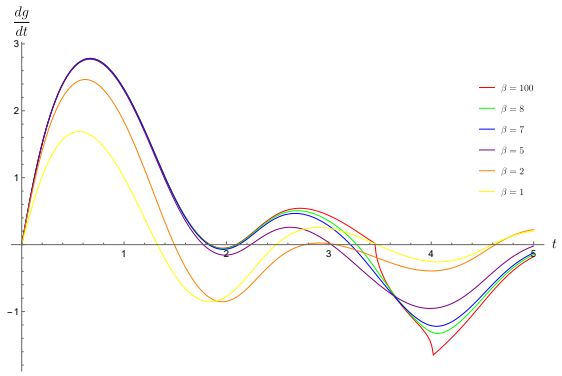

Figure 6.6: The time derivative of the rate function, dg/dt, as a function of time for different inverse temperatures. The quantum quench is from a topological to a topological regime (Regimes from II to III and vice versa).

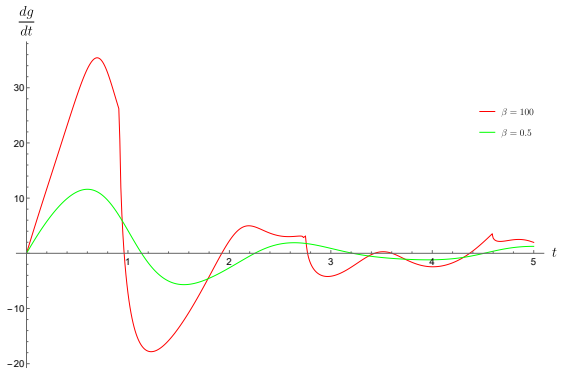

Figure 6.7: The time derivative of the rate function, dg/dt, as a function of time for different values of the inverse temperature, in the case that we quench the system from a trivial to a topological regime (Regimes from I to III and from IV to II).

of the Bures metric in the *space of density matrices* (i.e., in the space of quantum states). On the other hand, the dynamical interferometric susceptibility is the pullback of a metric in the *space of unitaries* (i.e., quantum channels). The difference between the two metrics reflects the fact that the fidelity is a measure of the state distinguishability between two *given* states ρ and σ in terms of observations, while the "interferometric distinguishability" quantifies how a quantum channel (a unitary U) changes an *arbitrary* state ρ to $U\rho U^\dagger$. Therefore, while the "interferometric distinguishability" is in general more sensitive, and thus appropriate for the study of genuine (microscopic) systems, it is the fidelity that is the most suitable for the study of many-body system phases. Moreover, interferometric experiments involve coherent superpositions of two states, which for many-body systems would require creating and manipulating genuine Schrödinger cat-like states. This seems to be experimentally beyond current technology.

We analytically derived and presented closed expressions for the dynamical susceptibilities in the case of two-band Hamiltonians. At finite temperature, the fidelity LE

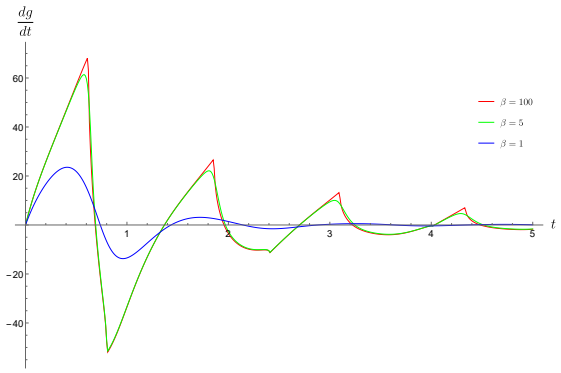

Figure 6.8: The time derivative of the rate function, dg/dt, as a function of time for different values of the inverse temperature. The system is quenched from a topological to a trivial regime (Regimes from III to I and from II to IV).

indicates gradual disappearance of the zero-temperature DQPTs, while the interferometric LE predicts finite-temperature DPTs. We applied this finite-temperature study on two representatives of TIs: the 1D SSH model and the 2D MD model. In perfect agreement with the general result, the fidelity-induced first derivatives are gradually smeared out with temperature, not exhibiting any critical behaviour at finite temperatures. This is also consistent with the study of 1D symmetry protected topological phases at finite temperatures that we presented in the previous two chapters. On the contrary, the interferometric LE exhibits critical behaviour even at finite temperatures (confirming previous studies on DPTs [**?** **?**]).

Chapter 7

Conclusions

In the first part of this thesis, we presented our work on quantum cryptography based on QWs. We proposed a new secure quantum public-key cryptosystem, where the public key used for the encyption of messages is a quantum state generated by a QW. Since the security of some of the currently used classical public-key cryptosystems can be compromised by adversaries with access to quantum computers, we believe that our protocol provides a useful alternative for future quantum communications. Moreover, our proposal is an improvement compared to a previously proposed protocol [**?**], where single-qubit rotations are used for the generation of the public key, which is given by a separable state. The states resulting from a QW are in general entangled states, so an eavesdropper should be able to apply more complex operations in order to infer the secret key and/ or the message. Therefore, the practical security of our protocol is higher.

Furthermore, we employed QWs in order to design and analyse new secure QKD protocols. We proposed two novel secure QKD protocols, where the parties exchange quantum states generated by means of QWs, in order to establish a common key that they can in turn use for message encryption or authentication. We also presented a semi-quantum variation of QKD, where one of the parties is restricted to perform only classical operations. We showed that this protocol, which can be considered more practical, since less quantum hardware is required, is robust against eavesdropping. This means that if E attempts to interfere in the protocol, she will be detected by the legitimate parties, who will in turn abort the protocol. QKD is so far the most secure and practical instance of quantum cryptography, therefore it would be interesting in the future to study concrete practical implementations of our theoretical proposals. In particular, one could perform a detailed analysis of the cheating strategies that an eavesdropper could use in the presence of noise, as well as to adapt the practical attacks and the corresponding countermeasures that we discussed in general, in the case of specific implementations. Moreover, we showed that our one-way QKD protocol withstands a high noise tolerance, due to the high di-

mension of the positions space, in agreement with several recent studies [**? ? ? ? ? ?**]. Thus, the application of QWs for QKD purposes seems to be very promising for practical applications.

To summarise, perhaps the most important contribution of our work on QWs in cryptography, is the fact that we introduced the use of QWs in public-key cryptography and QKD and showed how the properties of QWs can be translated into significant security properties of cryptographic protocols. Besides the theoretically interesting intersection of these two fascinating fields of quantum information science, we argued that there are also potential practical benefits in pursuing this investigation. Along these lines, in the future, it would be very relevant to apply QWs in the design of different cryptographic protocols, such as oblivious transfer and commitment schemes, as well as other privacy functionalities, like message authentication and digital signatures.

As described in the introductory Chapter 1, the existence or absence of long-term stable quantum memories has serious implications on both classical and quantum cryptography. Therefore, in the second part of this thesis, we studied the finite-temperature behaviour of systems exhibiting topological order, which are arguably among the best candidates for the design of quantum memories. We studied the PTs of topological systems at finite temperatures, by means of the well-established fidelity approach, as well as by employing a different quantity associated to the Uhlmann connection and the fidelity through the Bures metric. We applied this analysis to paradigmatic models of TIs and TSCs and showed that the topological features present at zero temperature are gradually smeared out as the temperature increases. We also analysed a topologically trivial superconductor, described by the BCS theory. In contrast to the case of the TSC, both quantities indicated the existence of thermal PTs, as the effective BCS Hamiltonian depends explicitly on temperature. We explained this different behaviour by further identifying the significance of thermal and purely quantum contributions to PTs. We believe that our study, which reveals this difference and clarifies the reasons behind it, could be used to probe several properties of the aforementioned systems in realistic experimental setups. We further confirmed the absence of thermally driven PTs in TIs and TSCs by investigating the behaviour of their edge states. The study of the Majorana modes (edge states of the TSC) at finite temperatures suggested that they can be used in achieving realistic quantum memories. Thus, a relevant path of future research would be to perform a detailed quantitative study on the robustness of these modes against temperature based on the method that we proposed.

We did the same analysis for the effective Hamiltonians resulting from specific single-particle QW protocols that have been shown to simulate all topological phases in 1D and 2D [**? ?**]. In particular, we studied representatives of two chiral symmetric classes of TIs

and we ended up with the same conclusion: the effective temperature only smears out the topological features exhibited at zero temperature, without causing any temperature-driven PTs. However, we observe finite-temperature parameter-driven PTs. We performed our study not only for the single-particle BG states with respect to the effective Hamiltonians of the single-particle QW protocols, but also for their many-body counterparts, and showed that their behaviour is consistent. Thus, the analysis of the single-particle sector could be a very useful mathematical tool in the study of the corresponding many-body systems. Also, the parameters that describe QWs can be easily controlled in experimental implementations, providing a simulating platform for topologically ordered systems. Therefore, it would be interesting to study in a future work the realistic noise effects that can give rise to these QW single-particle BG states and use our analysis to probe the topological features at finite temperatures in realistic setups.

Finally, we studied the behaviour of the topological order with respect to temperature for systems out of equilibrium. The figure of merit in the study of the corresponding PTs for pure states (DQPTs) is the LE, and there have been proposed two generalisations for mixed states: the fidelity LE and the interferometric LE. However, these two quantities give opposite predictions, when studying DPTs in topological systems: the fidelity LE approach does not predict finite-temperature PTs (consistent with our previous results in the case of topological PTs of systems in equilibrium), while the interferometric LE shows the persistence of topological PTs at finite temperatures. In order to clarify the origin of these different predictions, we analytically derived the form of the associated dynamical susceptibilities. The fidelity LE quantifies the state distinguishability in terms of measurements of physical properties, inducing a metric over the space of quantum states, while the interferometric LE quantifies the effects of quantum channels acting upon a state, inducing a pullback metric over the space of unitaries. Thus, we argue that the fidelity LE and its associated dynamical susceptibility are more suitable for the study of many-body systems, while the more sensitive interferometric counterparts are preferable when considering genuine microscopic quantum systems. In addition, interferometric experiments involve coherent superpositions of two states, which is, in the case of many-body macroscopic systems, experimentally infeasible with current technology.

To conclude, we believe that the work presented in this thesis not only complements the literature, but also opens new directions of research in different areas, namely quantum cryptography and communication, the study of topologically ordered quantum matter, as well as the pursue of physical systems that could be used to design realistic quantum memories.

Appendix A
Analytic derivation of the closed expressions for the fidelity and Δ

As already mentioned, the fidelity between two states ρ and ρ' is given by

$$F(\rho, \rho') = \mathrm{Tr}\sqrt{\sqrt{\rho}\rho'\sqrt{\rho}}. \tag{1}$$

We consider unnormalized thermal states $\rho = \exp(-\beta H)$ and $\rho' = \exp(-\beta' H')$. At the end of the calculation one must, of course, normalize the expressions appropriately. We wish to find closed expressions for the fidelity and the quantity Δ with respect to these thermal states. In order to do that we will proceed by finding e^C, such that

$$e^A e^B e^A = e^C, \tag{2}$$

for $A = -\beta H$, $B = -\beta' H'$ and, ultimately, take the square root of the result. The previous equation is equivalent to

$$e^A e^B = e^C e^{-A}. \tag{3}$$

The Hamiltonians H and H' are taken to be of the form $\vec{h} \cdot \vec{\sigma}$, and thus we can write

$$e^A = a_0 + \vec{a} \cdot \vec{\sigma}, e^B = b_0 + \vec{b} \cdot \vec{\sigma}, e^C = c_0 + \vec{c} \cdot \vec{\sigma},$$

where all the coefficients are real, with the following constraints:

$$\begin{cases} 1 = \det e^A = a_0^2 - \vec{a}^2, \\ 1 = \det e^B = b_0^2 - \vec{b}^2, \\ 1 = \det e^C = c_0^2 - \vec{c}^2, \end{cases} \tag{4}$$

which are equivalent to $\mathrm{tr}\, A = \mathrm{tr}\, B = \mathrm{tr}\, C = 0$, since Pauli matrices are traceless. Let us proceed by expanding the LHS and the RHS of Eq.(3),

$$\begin{aligned}
&(a_0 + \vec{a}\cdot\vec{\sigma})(b_0 + \vec{b}\cdot\vec{\sigma}) = (c_0 + \vec{c}\cdot\vec{\sigma})(a_0 - \vec{a}\cdot\vec{\sigma}) \\
\Leftrightarrow\ & a_0 b_0 + a_0\vec{b}\cdot\vec{\sigma} + \vec{a}\cdot\vec{\sigma} b_0 + (\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = c_0 a_0 - c_0\vec{a}\cdot\vec{\sigma} + \vec{c}\cdot\vec{\sigma} a_0 - (\vec{c}\cdot\vec{\sigma})(\vec{a}\cdot\vec{\sigma}) \\
\Leftrightarrow\ & a_0 b_0 + a_0\vec{b}\cdot\vec{\sigma} + \vec{a}\cdot\vec{\sigma} b_0 + \vec{a}\cdot\vec{b} + i(\vec{a}\times\vec{b})\cdot\vec{\sigma} = c_0 a_0 - c_0\vec{a}\cdot\vec{\sigma} + \vec{c}\cdot\vec{\sigma} a_0 - \vec{c}\cdot\vec{a} - i(\vec{c}\times\vec{a})\cdot\vec{\sigma} \quad (5)
\end{aligned}$$

Now, collecting terms in 1, $\vec{\sigma}$ and $i\vec{\sigma}$, we get a system of linear equations on c_0 and $\vec{c}$,

$$\begin{cases}
a_0 b_0 + \vec{a}\cdot\vec{b} - a_0 c_0 + \vec{a}\cdot\vec{c} = 0, \\
a_0\vec{b} + b_0\vec{a} + \vec{a} c_0 - a_0\vec{c} = 0, \\
\vec{a}\times\vec{b} - \vec{a}\times\vec{c} = 0.
\end{cases} \quad (6)$$

The third equation from (6) can be written as $\vec{a}\times(\vec{b}-\vec{c}) = 0$, whose solution is given by $\vec{c} = \vec{b} + \lambda\vec{a}$, where λ is a real number. This means that the solution depends only on two real parameters: c_0 and λ. Hence, we are left with a simpler system given by,

$$\begin{cases}
a_0 b_0 + \vec{a}\cdot\vec{b} - a_0 c_0 + \vec{a}\cdot(\vec{b} + \lambda\vec{a}) = 0 \\
a_0\vec{b} + b_0\vec{a} + \vec{a} c_0 - a_0(\vec{b} + \lambda\vec{a}) = 0
\end{cases}. \quad (7)$$

Or,

$$\begin{cases}
a_0 c_0 - \lambda\vec{a}^2 = a_0 b_0 + 2\vec{a}\cdot\vec{b} \\
(a_0\lambda - c_0)\vec{a} = b_0\vec{a}
\end{cases}. \quad (8)$$

In matrix form, the above system of equations can be written as

$$\begin{bmatrix} a_0 & -\vec{a}^2 \\ -1 & a_0 \end{bmatrix} \begin{bmatrix} c_0 \\ \lambda \end{bmatrix} = \begin{bmatrix} a_0 b_0 + 2\vec{a}\cdot\vec{b} \\ b_0 \end{bmatrix}. \quad (9)$$

Inverting the matrix, we get

$$\begin{aligned}
\begin{bmatrix} c_0 \\ \lambda \end{bmatrix} &= \tfrac{1}{a_0^2 - \vec{a}^2} \begin{bmatrix} a_0 & \vec{a}^2 \\ 1 & a_0 \end{bmatrix} \begin{bmatrix} a_0 b_0 + 2\vec{a}\cdot\vec{b} \\ b_0 \end{bmatrix} \\
&= \begin{bmatrix} (2a_0^2 - 1)b_0 + 2a_0\vec{a}\cdot\vec{b} \\ 2(a_0 b_0 + \vec{a}\cdot\vec{b}) \end{bmatrix}, \quad (10)
\end{aligned}$$

where we used the constraints (4). Because of the constraints, c_0 and λ are not independent, namely, $e^C = c_0 + (\vec{b} + \lambda\vec{a}) \cdot \vec{\sigma}$, and we get

$$c_0^2 - (\vec{b} + \lambda\vec{a})^2 = c_0^2 - \vec{b}^2 - 2\lambda\vec{a} \cdot \vec{b} - \vec{a}^2 = 1. \tag{11}$$

Now we want to make $A = -\beta H/2 \equiv -\xi\vec{x} \cdot \vec{\sigma}/2$ and $B = -\beta' H' \equiv -\zeta\vec{y} \cdot \vec{\sigma}$, with $\vec{x}^2 = \vec{y}^2 = 1$ and ξ and ζ real parameters, meaning,

$$a_0 = \cosh(\xi/2) \text{ and } \vec{a} = -\sinh(\xi/2)\vec{x}, b_0 = \cosh(\zeta) \text{ and } \vec{b} = -\sinh(\zeta)\vec{y}. \tag{12}$$

If we write $C = \rho\vec{z} \cdot \vec{\sigma}$ (because the product of matrices with determinant 1 has to have determinant 1, it has to be of this form),

$$\begin{aligned} c_0 = \cosh(\rho) \qquad & = (2a_0^2 - 1)b_0 + 2a_0\vec{a} \cdot \vec{b} = \\ & (2\cosh^2(\xi/2) - 1)\cosh(\zeta) + 2\cosh(\xi/2)\sinh(\xi/2)\sinh(\zeta)\vec{x} \cdot \vec{y} = \\ & \cosh(\xi)\cosh(\zeta) + \sinh(\xi)\sinh(\zeta)\vec{x} \cdot \vec{y}. \end{aligned} \tag{13}$$

For all the expressions concerning fidelity, we wish to compute $\mathrm{Tr}(e^{C/2}) = 2\cosh(\rho/2)$. If we use the formula $\cosh(\rho/2) = \sqrt{(1 + \cosh(\rho))/2}$, we obtain,

$$\mathrm{tr}\big(e^{C/2}\big) = 2\sqrt{\frac{(1 + \cosh(\xi)\cosh(\zeta) + \sinh(\xi)\sinh(\zeta)\vec{x} \cdot \vec{y})}{2}}. \tag{14}$$

Hence, if we let $\xi = \beta E/2$, $\vec{x} = \vec{n}$, $\zeta = \beta' E'/2$ and $\vec{y} = \vec{n}'$, then

$$\mathrm{tr}\Big(\sqrt{e^{-\beta H/2} e^{-\beta' H'} e^{-\beta H/2}}\Big) = 2\sqrt{\frac{(1 + \cosh(\beta E/2)\cosh(\beta' E'/2) + \sinh(\beta E/2)\sinh(\beta' E'/2)\vec{n} \cdot \vec{n}')}{2}}. \tag{15}$$

To be able to compute the fidelities, we will just need the following expression relating the traces of quadratic many-body fermion Hamiltonians (preserving the number operator) and the single-particle sector Hamiltonian obtained by projection:

$$\mathrm{tr}\big(e^{-\beta\mathcal{H}}\big) = \mathrm{tr}\Big(e^{-\beta\Psi^\dagger H\Psi}\Big) = \det\big(I + e^{-\beta H}\big). \tag{16}$$

From the previous results, it is straightforward to derive the following formulae for the fidelities concerning the thermal states considered:

$$
\begin{aligned}
F(\rho,\rho') &= \prod_{k\in\mathcal{B}} \frac{\mathrm{tr}\left(e^{-\mathcal{C}_k/2}\right)}{\mathrm{tr}\left(e^{-\beta\mathcal{H}_k}\right)\mathrm{tr}\left(e^{-\beta'\mathcal{H}'_k}\right)} \\
&= \prod_{k\in\mathcal{B}} \frac{\det\left(I+e^{-C_k/2}\right)}{\det^{1/2}(I+e^{-\beta H_k})\det^{1/2}(I+e^{-\beta' H'_k})} \\
&= \prod_{k\in\mathcal{B}} \frac{2+\sqrt{2\left(1+\cosh(E_k/2T)\cosh\left(E'_k/2T'\right)+\sinh(E_k/2T)\sinh\left(E'_k/2T'\right)\vec{n}_k\cdot\vec{n}'_k\right)}}{\sqrt{(2+2\cosh(E_k/2T))(2+2\cosh\left(E'_k/2T'\right))}},
\end{aligned}
\tag{17}
$$

where the matrix C_k is such that $e^{-C_k} = e^{-\beta H_k/2}e^{-\beta' H'_k}e^{-\beta H_k/2}$ and $\mathcal{C}_k = \Psi_k^\dagger C_k \Psi_k$ is the corresponding many-body quadratic operator.

To compute $\Delta(\rho,\rho')$ one needs, in addition, $\mathrm{tr}\,\sqrt{\rho}\sqrt{\rho'}$. This can be done along the lines of what was presented above, hence we shall omit the proof for the sake of briefness and directly provide the result:

$$
\mathrm{tr}\,\sqrt{\rho}\sqrt{\rho'} = \prod_{k\in\mathcal{B}} \frac{2+2\left(\cosh(E_k/4T)\cosh(E'_k/4T')+\sinh(E_k/4T)\sinh(E'_k/4T')\vec{n}_k\cdot\vec{n}'_k\right)}{\sqrt{(2+2\cosh(E_k/2T))(2+2\cosh(E'_k/2T'))}}
\tag{18}
$$

Appendix B
Analytic derivation of the dynamical susceptibilities

Zero-temperature case

Let $\mathscr{H}$ be a Hilbert space. Suppose we have a family of Hamiltonians $\{H(\lambda) : \lambda \in M\}$ where M is a smooth compact manifold of the Hamiltonian's parameters. We assume that aside from a closed finite subset of M, $C = \{\lambda_i\}_{i=1}^n \subset M$, the Hamiltonian is gapped and the ground state subspace is one-dimensional. Locally, on $M - C$, we can find a ground state (with unit norm) described by $|\psi(\lambda)\rangle$. Take $\lambda_i \in C$, and let U be an open neighbourhood containing λ_i. Of course, for sufficiently small U, on the open set $U - \{\lambda_i\}$ one can find a smooth assignment $\lambda \mapsto |\psi(\lambda)\rangle$. Consider a curve $[0,1] \ni s \mapsto \lambda(s) \in U$, with initial condition $\lambda(0) = \lambda_0$, such that $\lambda(s_0) = \lambda_i$ for some $s_0 \in [0,1]$. The family of Hamiltonians $H(s) := H(\lambda(s))$ is well-defined for every $s \in [0,1]$. The family of states $|\psi(s)\rangle \equiv |\psi(\lambda(s))\rangle$ is well-defined for $s \neq s_0$ and so is the ground state energy

$$E(s) := \langle\psi(s)| H(s) |\psi(s)\rangle .$$

The overlap,

$$\mathcal{A}(s) := \langle\psi(0)| \exp(-itH(s)) |\psi(0)\rangle ,$$

is well-defined. We can write

$$\exp(-itH(s)) = \exp(-itH(0))T \exp\left\{-i \int_0^t d\tau V(s,\tau)\right\} .$$

If we take the derivative with respect to t, we find

$$H(s) = H(0) + \exp(-itH(0))V(s,t)\exp(itH(0))$$

so,

$$V(s,t) = \exp(itH(0))(H(s) - H(0))\exp(-itH(0)).$$

We can now write, since $|\psi(0)\rangle$ is an eigenvector of $H(0)$,

$$\mathcal{A}(s) = e^{-itE(0)} \langle\psi(0)| T\exp\left\{-i\int_0^t d\tau V(s,\tau)\right\} |\psi(0)\rangle .$$

We now perform an expansion of the overlap

$$\langle\psi(0)| T\exp\left\{-i\int_0^t d\tau V(s,\tau)\right\} |\psi(0)\rangle$$

in powers of s. Notice that

$$T\exp\left\{-i\int_0^t d\tau V(s,\tau)\right\} = I - i\int_0^t d\tau V(s,\tau) - \frac{1}{2}\int_0^t\int_0^t d\tau_2 d\tau_1 T\{V(s,\tau_2)V(s,\tau_1)\} + \dots$$

and hence

$$\frac{d}{ds}\left(T\exp\left\{-i\int_0^t d\tau V(s,\tau)\right\}\right)\Big|_{s=0} = -i\int_0^t d\tau \frac{\partial V}{\partial s}(0,\tau)$$

and

$$\frac{d^2}{ds^2}\left(T\exp\left\{-i\int_0^t d\tau V(s,\tau)\right\}\right)\Big|_{s=0} = -i\int_0^t d\tau \frac{\partial^2 V}{\partial s^2}(0,\tau) - \int_0^t\int_0^t d\tau_2 d\tau_1 T\left\{\frac{\partial V}{\partial s}(0,\tau_2)\frac{\partial V}{\partial s}(0,\tau_1)\right\}.$$

Therefore,

$$\langle\psi(0)| T\exp\left\{-i\int_0^t d\tau V(s,\tau)\right\} |\psi(0)\rangle = 1 - is\langle\psi(0)|\int_0^t d\tau \tfrac{\partial V}{\partial s}(0,\tau)|\psi(0)\rangle$$
$$+\tfrac{s^2}{2}\left[-i\langle\psi(0)|\int_0^t d\tau \tfrac{\partial^2 V}{\partial s^2}(0,\tau)|\psi(0)\rangle - \langle\psi(0)|\int_0^t\int_0^t d\tau_2 d\tau_1 T\left\{\tfrac{\partial V}{\partial s}(0,\tau_2)\tfrac{\partial V}{\partial s}(0,\tau_1)\right\}|\psi(0)\rangle\right] + \mathrm{O}(s^3).$$

Thus, by using the identity $\theta(\tau)+\theta(-\tau) = 1$ of the Heaviside theta function, we obtain

$$\begin{aligned}|\mathcal{A}(s)|^2 = \quad & 1 - s^2\big(\int_0^t\int_0^t d\tau_2 d\tau_1 \langle\psi(0)|\tfrac{1}{2}\left\{\tfrac{\partial V}{\partial s}(0,\tau_2), \tfrac{\partial V}{\partial s}(0,\tau_1)\right\}|\psi(0)\rangle \\ & - \langle\psi(0)|\tfrac{\partial V}{\partial s}(0,\tau_2)|\psi(0)\rangle\langle\psi(0)|\tfrac{\partial V}{\partial s}(0,\tau_1)|\psi(0)\rangle\big) + \mathrm{O}(s^3).\end{aligned}$$

If we denote the expectation value $\langle\psi(0)| * |\psi(0)\rangle \equiv \langle * \rangle$ we can write,

$$\begin{aligned}|\mathcal{A}(s)|^2 = \quad & 1 - s^2\int_0^t\int_0^t d\tau_2 d\tau_1 \left[\langle\tfrac{1}{2}\left\{\tfrac{\partial V}{\partial s}(0,\tau_2), \tfrac{\partial V}{\partial s}(0,\tau_1)\right\}\rangle - \langle\tfrac{\partial V}{\partial s}(0,\tau_2)\rangle\langle\tfrac{\partial V}{\partial s}(0,\tau_1)\rangle\right] + \mathrm{O}(s^3) \\ & = 1 - \chi s^2 + \mathrm{O}(s^3),\end{aligned}$$

where

$$\chi \equiv \int_0^t \int_0^t d\tau_2 d\tau_1 \left[\langle \frac{1}{2} \left\{ \frac{\partial V}{\partial s}(0,\tau_2), \frac{\partial V}{\partial s}(0,\tau_1) \right\} \rangle - \langle \frac{\partial V}{\partial s}(0,\tau_2) \rangle \langle \frac{\partial V}{\partial s}(0,\tau_1) \rangle \right]$$

is the dynamical susceptibility and is naturally nonnegative. In fact, defining $V_a(\tau) = e^{i\tau H(0)} \partial H / \partial \lambda^a(\lambda_0) e^{-i\tau H(0)}$ such that, by the chain rule,

$$\frac{\partial V}{\partial s}(0,\tau) = V_a(\tau) \frac{\partial \lambda^a}{\partial s}(0),$$

we can write,

$$\chi = g_{ab}(\lambda_0) \frac{\partial \lambda^a}{\partial s}(0) \frac{\partial \lambda^b}{\partial s}(0),$$

with the metric tensor given by

$$g_{ab}(\lambda_0) = \int_0^t \int_0^t d\tau_2 d\tau_1 \left[\langle \frac{1}{2} \{ V_a(\tau_2), V_b(\tau_1) \} \rangle - \langle V_a(\tau_2) \rangle \langle V_b(\tau_1) \rangle \right]. \tag{19}$$

Dynamical fidelity susceptibility χ at finite temperature

A possible generalisation of the zero-temperature LE to finite temperatures is through the Uhlmann fidelity, since the zero temperature $|\mathcal{A}(s)|$ is precisely the fidelity between the states $|\psi(0)\rangle$ and $\exp(-itH(s))\,|\psi(0)\rangle$. Since the Uhlmann fidelity between two close mixed states is determined by the Bures metric, we begin by revisiting the derivation of the latter for the case of interest, i.e., two-level systems.

Bures metric for a two-level system

Take a curve of full-rank density operators $t \mapsto \rho(t)$ and an horizontal lift $t \mapsto W(t)$, with $W(0) = \sqrt{\rho(0)}$. Then the Bures metric is given by

$$g_{\rho(t)}(\frac{d\rho}{dt}, \frac{d\rho}{dt}) = \mathrm{tr} \left\{ \frac{dW^\dagger}{dt} \frac{dW}{dt} \right\}.$$

The horizontality condition is given by

$$W^\dagger \frac{dW}{dt} = \frac{dW^\dagger}{dt} W,$$

for each t. In the full-rank case, we can find a unique Hermitian matrix $G(t)$, such that

$$\frac{dW}{dt} = G(t)W$$

solves the horizontality condition

$$W^\dagger \frac{dW}{dt} = W^\dagger G W = \frac{dW^\dagger}{dt} W.$$

Also, G is such that

$$\frac{d\rho}{dt} = \frac{d}{dt}(WW^\dagger) = G\rho + \rho G.$$

If L_ρ (R_ρ) is left (right) multiplication by ρ, we have, formally,

$$G = (L_\rho + R_\rho)^{-1} \frac{d\rho}{dt}.$$

Therefore,

$$\begin{aligned} g_{\rho(t)}(\frac{d\rho}{dt}, \frac{d\rho}{dt}) &= \operatorname{tr}\left\{\tfrac{dW^\dagger}{dt}\tfrac{dW}{dt}\right\} = \operatorname{tr}\{G^2\rho\} \\ &= \tfrac{1}{2}\operatorname{tr}\{G(\rho G + G\rho)\} \\ &= \tfrac{1}{2}\operatorname{tr}\{G\tfrac{d\rho}{dt}\} = \tfrac{1}{2}\operatorname{tr}\left\{(L_\rho + R_\rho)^{-1}\tfrac{d\rho}{dt}\tfrac{d\rho}{dt}\right\}. \end{aligned}$$

If we write $\rho(t)$ in the diagonal basis,

$$\rho(t) = \sum_i p_i(t) \left|i(t)\right\rangle \left\langle i(t)\right|$$

we find

$$g_{\rho(t)}(\frac{d\rho}{dt}, \frac{d\rho}{dt}) = \frac{1}{2}\operatorname{tr}\left\{(L_\rho + R_\rho)^{-1}\frac{d\rho}{dt}\frac{d\rho}{dt}\right\} = \frac{1}{2}\sum_{i,j}\frac{1}{p_i(t) + p_j(t)} \left\langle i(t)\right| \frac{d\rho}{dt} \left|j(t)\right\rangle \left\langle j(t)\right| \frac{d\rho}{dt} \left|i(t)\right\rangle.$$

Hence, using the diagonal basis of ρ, we can read off the metric tensor at ρ as

$$g_\rho = \frac{1}{2}\sum_{i,j}\frac{1}{p_i + p_j} \left\langle i\right| d\rho \left|j\right\rangle \left\langle j\right| d\rho \left|i\right\rangle.$$

This is the result for general full rank density operators. For two-level systems, writing

$$\rho = \frac{1}{2}(1 - X^\mu \sigma_\mu),$$

and defining variables $|X| = r$ and $n^\mu = X^\mu/|X|$, we can express g_ρ as

$$g_\rho = \left[\frac{1}{1+r} + \frac{1}{1-r}\right] d\rho_{11}^2 + d\rho_{12}d\rho_{21} = \frac{1}{1-r^2} d\rho_{11}^2 + d\rho_{12}d\rho_{21},$$

where we used $d\rho_{11} = -d\rho_{22}$. Notice that

$$d\rho_{11} = \frac{1}{2}\operatorname{tr}\{d\rho U\sigma_3 U^{-1}\} = \frac{1}{2}\operatorname{tr}\{d\rho n^\mu \sigma_\mu\},$$

where U is a unitary matrix diagonalising ρ, $U\sigma_3 U^{-1} = n^\mu\sigma_\mu$. Now,

$$d\rho = -\frac{1}{2} dX^\mu \sigma_\mu,$$

and hence

$$d\rho_{11} = -\frac{1}{2} dX^\mu n_\mu = -\frac{1}{2} dr.$$

On the other hand,

$$\begin{aligned} d\rho_{12}d\rho_{21} &= \tfrac{1}{4}\operatorname{tr}\{d\rho U(\sigma_1 - i\sigma_2)U^{-1}\}\operatorname{tr}\{d\rho U(\sigma_1 - i\sigma_2)U^{-1}\} \\ &= \tfrac{1}{4}\left[\operatorname{tr}\{d\rho U\sigma_1 U^{-1}\}\operatorname{tr}\{d\rho U\sigma_1 U^{-1}\} + \operatorname{tr}\{d\rho U\sigma_2 U^{-1}\}\operatorname{tr}\{d\rho U\sigma_2 U^{-1}\}\right] \\ &= \tfrac{1}{4}\delta_{\mu\nu}(dX^\mu - n^\mu n_\lambda dX^\lambda)(dX^\nu - n^\nu n_\sigma dX^\sigma) = \tfrac{1}{4} r^2 dn^\mu dn_\mu, \end{aligned}$$

where we used the fact that the vectors (u, v) defined by the equations $U\sigma_1 U^{-1} = u^\mu\sigma_\mu$ and $U\sigma_2 U^{-1} = v^\mu\sigma_\mu$ form an orthonormal basis for the orthogonal complement in $\mathbb{R}^3$ of the line generated by n^μ (which corresponds to the tangent space to the unit sphere S^2 at n^μ). Thus, we obtain the final expression for the squared line element

$$ds^2 = \frac{1}{4}\left(\frac{dr^2}{1-r^2} + r^2\delta_{\mu\nu}dn^\mu dn^\nu\right). \tag{20}$$

The above expression is ill-defined for the pure state case of $r = 1$. Nevertheless, the limiting case of $r \to 1$ as the metric is smooth as we will now show by introducing another coordinate patch. The set of pure states is defined by $r = 1$, i.e., they correspond to the boundary of the 3-dimensional ball $B = \{X \ : \ |X| = r \leq 1\}$ which, topologically, is the set of all density matrices in dimension 2. Introducing the change of variable $r = \cos u$, with $u \in [0, \pi/2)$, the metric becomes

$$ds^2 = \frac{1}{4}\left(du^2 + (\cos u)^2\delta_{\mu\nu}dn^\mu dn^\nu\right),$$

which is well defined also for the pure-state case of $r = \cos(0) = 1$. Restricting it to the unit sphere, the metric coincides with the Fubini-Study metric, also known as the

quantum metric, on the space of pure states $\mathbb{C}P^1 \cong S^2$, i.e., the Bloch sphere. Therefore, there is no problem on taking the pure-state limit of this metric on the space of states, since it reproduces the correct result.

The pullback of the Bures metric

We have a map

$$M \ni \lambda \mapsto \rho(\lambda) \quad = U(\lambda)\rho_0 U(\lambda)^{-1} = \tfrac{1}{2}U(\lambda)\left(I - X^\mu \sigma_\mu\right)U(\lambda)^{-1},$$

with

$$U(\lambda) = \exp(-itH(\lambda)),$$

and we take

$$\rho_0 = \frac{\exp(-\beta H(\lambda_0))}{\mathrm{tr}\left\{\right.}$$

, for some $\lambda_0 \in M$.We use the curve $[0,1] \ni s \mapsto \lambda(s)$, with $\lambda(0) = \lambda_0$, to obtain a curve of density operators

$$s \mapsto \rho(s) := \rho(\lambda(s)).$$

Notice that $\rho(0) = \rho_0$. The fidelity we consider is then

$$F(\rho(0), \rho(s)) = \mathrm{tr}\left(\sqrt{\sqrt{\rho(0)}\rho(s)\sqrt{\rho(0)}}\right).$$

Recall that for 2×2 density operators of full rank the Bures line element reads

$$ds^2 = \frac{1}{4}\left(\frac{dr^2}{1-r^2} + r^2 \delta_{\mu\nu} dn^\mu dn^\nu\right),$$

where

$$n^\mu = X^\mu/|X| \text{ and } r = |X|,$$

with

$$\rho = \frac{1}{2}\left(I - X^\mu \sigma_\mu\right).$$

Now,

$$\rho(\lambda) = \frac{1}{2}\left(I - R^\mu{}_\nu(\lambda) X^\nu \sigma_\mu\right),$$

with $R^\mu{}_\nu(\lambda)$ being the unique SO(3) element satisfying

$$U(\lambda)\sigma_\mu U(\lambda)^{-1} = R^\nu{}_\mu(\lambda)\sigma_\nu.$$

We then have, pulling back the coordinates,

$$r(\lambda) = |X| = \text{constant} \quad \text{and} \quad n^\mu(\lambda) = R^\mu{}_\nu(\lambda) n^\nu.$$

Therefore,

$$ds^2 = \frac{1}{4} r^2 \delta_{\mu\nu} \frac{\partial n^\mu}{\partial \lambda^a} \frac{\partial n^\nu}{\partial \lambda^b} d\lambda^a d\lambda^b = \frac{1}{4} r^2 \delta_{\mu\nu} n^\sigma n^\tau \frac{\partial R^\mu{}_\sigma}{\partial \lambda^a} \frac{\partial R^\nu{}_\tau}{\partial \lambda^b} d\lambda^a d\lambda^b,$$

which in terms of the Euclidean metric on the tangent bundle of $\mathbb{R}^3$, denoted by $\langle *, * \rangle$, takes the form

$$g_{ab}(\lambda) = \frac{1}{4} r^2 \langle R^{-1} \frac{\partial R}{\partial \lambda^a} n, R^{-1} \frac{\partial R}{\partial \lambda^b} n \rangle,$$

written in terms of the pullback of the Maurer-Cartan form in SO(3), $R^{-1}dR$. We can further pullback by the curve $s \mapsto \lambda(s)$ and evaluate at $s = 0$

$$\chi = g_{ab}(\lambda_0) \frac{\partial \lambda^a}{\partial s}(0) \frac{\partial \lambda^b}{\partial s}(0) = \frac{1}{4} r^2 \langle R^{-1} \frac{\partial R}{\partial \lambda^a} n, R^{-1} \frac{\partial R}{\partial \lambda^b} n \rangle \frac{\partial \lambda^a}{\partial s}(0) \frac{\partial \lambda^b}{\partial s}(0),$$

which gives us the expansion of the fidelity

$$F(s) \equiv F(\rho(0), \rho(s)) = 1 - \frac{1}{2} \chi s^2 + \dots$$

We now evaluate χ. Note that

$$dU \sigma_\mu U^{-1} + U \sigma_\mu dU^{-1} = U[U^{-1} dU, \sigma_\mu] U^{-1} = dR^\nu{}_\mu \sigma_\nu.$$

Now, we can parameterise

$$U = y^0 I + i y^\mu \sigma_\mu, \text{ with } |y|^2 = 1.$$

Therefore,

$$U^{-1} dU = (y^0 - i y^\mu \sigma_\mu)(dy^0 + i dy^\nu \sigma_\nu) = i(y^0 dy^\mu - y^\mu dy^0)\sigma_\mu + \frac{i}{2}(y^\mu dy^\nu - y^\nu dy^\mu) \varepsilon^\lambda_{\mu\nu} \sigma_\lambda;$$

,

$$\begin{aligned}
[U^{-1} dU, \sigma_\kappa] &= -2 \left[(y^0 dy^\mu - y^\mu dy^0) \varepsilon^\tau_{\mu\kappa} + \tfrac{1}{2} (y^\mu dy^\nu - y^\nu dy^\mu) \varepsilon^\lambda_{\mu\nu} \varepsilon^\tau_{\lambda\kappa} \right] \sigma_\tau \\
&= -2 \left[(y^0 dy^\mu - y^\mu dy^0) \varepsilon_{\mu\kappa}{}^\tau + \tfrac{1}{2} (y^\mu dy^\nu - y^\nu dy^\mu)(\delta_{\mu\kappa} \delta^\tau_\nu - \delta^\tau_\mu \delta^\nu_\kappa) \right] \sigma_\tau \\
&= -2 \left[(y^0 dy^\mu - y^\mu dy^0) \varepsilon_{\mu\kappa}{}^\tau + (y^\kappa dy^\tau - y^\tau dy^\kappa) \right] \sigma_\tau \\
&= 2 \left[(y^0 dy^\mu - y^\mu dy^0) \varepsilon_\mu{}^\tau{}_\kappa + (y^\tau dy^\kappa - y^\kappa dy^\tau) \right] \sigma_\tau \equiv (R^{-1} dR)^\tau{}_\kappa \sigma_\tau.
\end{aligned}$$

Observe that for $H(\lambda) = x^\mu(\lambda)\sigma_\mu$ we have,

$$y^0(\lambda) = \cos(|x(\lambda)|t) \text{ and } y^\mu = -\sin(|x(\lambda)|t)\frac{x^\mu(\lambda)}{|x(\lambda)|}.$$

Therefore,

$$\begin{aligned} dy^0 &= -\sin(|x(\lambda)|t)d|x(\lambda)|, \\ dy^\mu &= -\cos(|x(\lambda)|t)\tfrac{x^\mu(\lambda)}{|x(\lambda)|}d|x(\lambda)| - \sin(|x(\lambda)|t)d\left(\tfrac{x^\mu(\lambda)}{|x(\lambda)|}\right). \end{aligned}$$

After a bit of algebra, we get

$$\begin{aligned} y^0dy^\mu - y^\mu dy^0 &= \tfrac{x^\mu(\lambda)}{|x(\lambda)|}d|x(\lambda)| - \sin(|x(\lambda)|)\cos(|x(\lambda)|)d\left(\tfrac{x^\mu(\lambda)}{|x(\lambda)|}\right), \\ y^\mu dy^\nu - y^\nu dy^\mu &= 2\sin^2(|x(\lambda)|t)\tfrac{x^{[\mu}(\lambda)}{|x(\lambda)|}d\left(\tfrac{x^{\nu]}(\lambda)}{|x(\lambda)|}\right). \end{aligned}$$

Thus,

$$(R^{-1}dR)^\tau_\kappa = 2\frac{x^\mu(\lambda)}{|x(\lambda)|}d|x(\lambda)|\varepsilon^{\ \tau}_{\mu\kappa} - \sin(2|x(\lambda)|t)d\left(\frac{x^\mu(\lambda)}{|x(\lambda)|}\right)\varepsilon^{\ \tau}_{\mu\kappa} + 4\sin^2(|x(\lambda)|t)\frac{x^{[\tau}(\lambda)}{|x(\lambda)|}d\left(\frac{x^{\kappa]}(\lambda)}{|x(\lambda)|}\right).$$

At $s = 0$, $\lambda(0) = \lambda_0$ and the coordinate $n^\mu(\lambda(0)) = x^\mu(\lambda_0)/|x(\lambda_0)|$, so the previous expression reduces to

$$\begin{aligned} (R^{-1}dR(\lambda_0))^\tau{}_\kappa n^\kappa &= 6(R^{-1}dR(\lambda_0))^\tau{}_\kappa \tfrac{x^\kappa(\lambda_0)}{|x(\lambda_0)|} \\ &= -\sin(2|x(\lambda_0)|t)\tfrac{1}{|x(\lambda_0)|^2}\varepsilon^\tau{}_{\mu\kappa}x^\mu(\lambda_0)dx^\kappa(\lambda_0) - (1-\cos(2|x(\lambda_0)|t))d\left(\tfrac{x^\mu}{|x|}\right)(\lambda_0). \end{aligned}$$

Notice that the first term is perpendicular to the second. Therefore, we find

$$\begin{aligned} \chi ds^2 &= \tfrac{1}{4}r^2|R^{-1}dRn|^2 \\ &= \tfrac{1}{4}r^2\left[\sin^2(2|x(\lambda_0)|t)\tfrac{1}{|x(\lambda_0)|^4}\left(\delta^\lambda_\mu\delta^\sigma_\kappa - \delta^\sigma_\mu\delta^\lambda_\kappa\right)x^\mu(\lambda)dx^k(\lambda)x_\lambda(\lambda_0)dx_\sigma(\lambda_0) + \left(1-\cos\left(2|x(\lambda_0|t)^2\langle Pdx(\lambda_0), Pdx(\lambda_0)\rangle\right)\right)\right] \\ &= r^2\tfrac{\sin^2(|x(\lambda_0)|t)}{|x(\lambda_0)|^2}\langle P\tfrac{\partial x}{\partial\lambda^a}(\lambda_0), P\tfrac{\partial x}{\partial\lambda^b}(\lambda_0)\rangle\tfrac{\partial\lambda^a}{\partial s}(0)\tfrac{\partial\lambda^b}{\partial s}(0)ds^2, \end{aligned}$$

where we have introduced the projector $P : T_x\mathbb{R}^3 = T_xS^2_{|x|} \oplus N_xS^2_{|x|} \to T_xS^2_{|x|}$ onto the tangent space of the sphere of radius $|x|$ at x. In other words, the pullback metric by ρ of the Bures metric at λ_0 is given by

$$\begin{aligned} g_{ab}(\lambda_0) &= r^2\tfrac{\sin^2(|x(\lambda_0)|t)}{|x(\lambda_0)|^2}\langle P\tfrac{\partial x}{\partial\lambda^a}(\lambda_0), P\tfrac{\partial x}{\partial\lambda^b}(\lambda_0)\rangle \\ &= \tanh^2(\beta|x(\lambda_0)|)\tfrac{\sin^2(|x(\lambda_0)|t)}{|x(\lambda_0)|^2}\langle P\tfrac{\partial x}{\partial\lambda^a}(\lambda_0), P\tfrac{\partial x}{\partial\lambda^b}(\lambda_0)\rangle. \end{aligned}$$

Dynamical interferometric susceptibility $\tilde{\chi}$ at finite temperature

We can replace the average $\langle e^{-itH(s)}\rangle \equiv \langle\psi(0)|\, e^{-itH(s)}\, |\psi(0)\rangle$ by the corresponding average of $e^{itH(0)}e^{-itH(s)}$ on the mixed state $\rho(\lambda_0) = \rho(0) = \exp(-\beta H(0))/\operatorname{tr}\{\exp(-\beta H(0))\}$ (note its implicit temperature dependence):

$$\mathcal{A}(s) = \operatorname{tr}\left\{\rho(0)T\exp\left\{-i\int_0^t d\tau V(s,\tau)\right\}\right\}.$$

It is easy to see that $|\mathcal{A}(s)|^2$ has the same expansion as before with the average on $|\psi(0)\rangle$ replaced by the average on $\rho(0)$.

We now proceed to compute $\tilde{\chi}$, or equivalently $\tilde{g}_{ab}(\lambda_0)$, in the case of a two-level system, where we can write

$$\rho(\lambda) = \frac{e^{-\beta H(\lambda)}}{\operatorname{tr}\{e^{-\beta H(\lambda)}\}} = \frac{1}{2}(I - X^\mu(\lambda)\sigma_\mu),$$

and define variables $r(\lambda) = |X(\lambda)|$ and $n^\mu(\lambda) = X^\mu(\lambda)/|X(\lambda)|$. Writing $H(\lambda) = x^\mu(\lambda)\sigma_\mu$ (and $H(s) \equiv H(\lambda(s))$), we have

$$V_a(\tau) = \frac{\partial x^\mu}{\partial\lambda^a}(\lambda_0)e^{i\tau H(0)}\sigma_\mu e^{-i\tau H(0)}.$$

Hence, its expectation value is

$$\langle V_a(\tau)\rangle = \frac{1}{\operatorname{tr}\{e^{-\beta H(\lambda)}\}}\operatorname{tr}\left\{e^{-\beta H(0)}\sigma_\mu\right\}\frac{\partial x^\mu}{\partial\lambda^a}(\lambda_0) = r(\lambda_0)n_\mu(\lambda_0)\frac{\partial x^\mu}{\partial\lambda^a}(\lambda_0) = X_\mu(\lambda_0)\frac{\partial x^\mu}{\partial\lambda^a}(\lambda_0),$$

which is independent of τ. We then have

$$\begin{aligned}\langle V_a(\tau_2)\rangle\langle V_b(\tau_1)\rangle &= (r(\lambda_0))^2 n_\mu(\lambda_0)\tfrac{\partial x^\mu}{\partial\lambda^a}(\lambda_0)n_\nu(\lambda_0)\tfrac{\partial x^\nu}{\partial\lambda^b}(\lambda_0)\\ &= \tanh^2(\beta|x(\lambda_0)|)\tfrac{x_\mu}{|x(\lambda_0)|}\tfrac{\partial x^\mu}{\partial\lambda^a}(\lambda_0)\tfrac{x_\nu}{|x(\lambda_0)|}\tfrac{\partial x^\nu}{\partial\lambda^b}(\lambda_0),\end{aligned}$$

where we used $X^\mu(\lambda_0) = \tanh(\beta|x(\lambda_0)|)x^\mu(\lambda_0)/|x(\lambda_0)|$. Now, using the cyclic property of the trace, we get

$$\begin{aligned}\frac{1}{2\operatorname{tr}\{e^{-\beta H(0)}\}}\operatorname{tr}\left\{e^{-\beta H(\lambda)}\{V_a(\tau_2),V_b(\tau_1)\}\right\} &= \tfrac{1}{2\operatorname{tr}\{e^{-\beta H(0)}\}}\operatorname{tr}\left\{e^{-\beta H(0)}\{\sigma_\mu,\sigma_\nu\}\right\}R^\mu{}_\lambda(\tau_2)R^\nu{}_\sigma(\tau_1)\tfrac{\partial x^\lambda}{\partial\lambda^a}(\lambda_0)\tfrac{\partial x^\sigma}{\partial\lambda^b}(\lambda_0)\\ &= \delta_{\mu\nu}R^\mu{}_\lambda(\tau_2)R^\nu{}_\sigma(\tau_1)\tfrac{\partial x^\lambda}{\partial\lambda^a}(\lambda_0)\tfrac{\partial x^\sigma}{\partial\lambda^b}(\lambda_0), \qquad (21)\end{aligned}$$

where $R^\mu{}_\nu(\tau)$ is the rotation matrix defined by the equation

$$e^{i\tau H(0)}\sigma_\nu e^{-i\tau H(0)} = R^\mu{}_\nu(\tau)\sigma_\mu. \qquad (22)$$

We can explicitly write $R^{\mu}{}_{\nu}(\tau)$ as

$$R^{\mu}_{\nu}(\tau) = \cos(2\tau|x(\lambda_0)|)\delta^{\mu}_{\nu} + (1-\cos(2\tau|x(\lambda_0)|))n^{\mu}(\lambda_0)n_{\nu}(\lambda_0) + \sin(2\tau|x(\lambda_0)|)n^{\lambda}(\lambda_0)\varepsilon^{\mu}_{\lambda\nu}.$$

Using the previous equation, and because $\{R(\tau)\}$ forms a one-parameter group, we can write

$$\delta_{\mu\nu}R^{\mu}{}_{\lambda}(\tau_2)R^{\nu}{}_{\sigma}(\tau_1) = \delta_{\kappa\lambda}R^{\kappa}{}_{\sigma}(\tau_2-\tau_1).$$

Since $\tilde{\chi}$ (i.e., the metric $\tilde{g}_{ab}$; recall its zero-temperature expression from Equation (19)) has to be symmetric under the label exchange $a \leftrightarrow b$, the relevant symmetric part of Equation (21) is

$$\cos\left[2(\tau_2-\tau_1)|x(\lambda_0)|\right]\delta_{\mu\nu}\frac{\partial x^{\mu}}{\partial\lambda^{a}}(\lambda_0)\frac{\partial x^{\nu}}{\partial\lambda^{b}}(\lambda_0)+(1-\cos\left[2(\tau_2-\tau_1)|x(\lambda_0)|\right])\frac{x_{\mu}}{|x(\lambda_0)|}\frac{\partial x^{\mu}}{\partial\lambda^{a}}(\lambda_0)\frac{x_{\nu}}{|x(\lambda_0)|}\frac{\partial x^{\nu}}{\partial\lambda^{b}}(\lambda_0).$$

Putting everything together gives

$$\begin{aligned}\langle\frac{1}{2}\{V_a(\tau_2),V_b(\tau_1)\}\rangle - \langle V_a(\tau_2)\rangle\langle V_b(\tau_1)\rangle = \quad & \cos\left[2(\tau_2-\tau_1)|x(\lambda_0)|\right]\langle P\tfrac{\partial x}{\partial\lambda^{a}}(\lambda_0), P\tfrac{\partial x}{\partial\lambda^{b}}(\lambda_0)\rangle \\ & +(1-\tanh^2(\beta|x(\lambda_0)|))\langle\tfrac{x(\lambda_0)}{|x(\lambda_0)|},\tfrac{\partial x}{\partial\lambda^{a}}(\lambda_0)\rangle\langle\tfrac{x(\lambda_0)}{|x(\lambda_0)|},\tfrac{\partial x}{\partial\lambda^{b}}(\lambda_0)\rangle.\end{aligned}$$

The integral on τ_1 and τ_2 can now be performed, using

$$\begin{aligned}&\int_0^t\int_0^t d\tau_2 d\tau_1\cos[2(\tau_2-\tau_1)\varepsilon] = \int_0^t\int_0^t d\tau_2 d\tau_1\left(\cos(2\tau_2\epsilon)\cos(2\tau_1\epsilon)+\sin(2\tau_2\epsilon)\sin(2\tau_1\epsilon)\right)\\ &\quad = \tfrac{1}{4\epsilon^2}\left[\sin^2(2t\epsilon)+(\cos(2t\epsilon)-1)(\cos(2t\epsilon)-1)\right] = \tfrac{1}{4\epsilon^2}\left[2-2\cos(2t\epsilon)\right] = \tfrac{\sin^2(t\epsilon)}{\epsilon^2}.\end{aligned}$$

So, the interferometric metric is

$$\tilde{g}_{ab}(\lambda_0) = \frac{\sin^2(|x(\lambda_0)|t)}{|x(\lambda_0)|^2}[\langle P\frac{\partial x}{\partial\lambda^{a}}(\lambda_0), P\frac{\partial x}{\partial\lambda^{b}}(\lambda_0)\rangle]+t^2(1-\tanh^2(\beta|x(\lambda_0|))\langle\frac{x(\lambda_0)}{|x(\lambda_0)|},\frac{\partial x}{\partial\lambda^{a}}(\lambda_0)\rangle\langle\frac{x(\lambda_0)}{|x(\lambda_0)|},\frac{\partial x}{\partial\lambda^{b}}(\lambda_0)\rangle.$$

The dynamical interferometric susceptibility is then given by

$$\begin{aligned}\tilde{\chi} \quad & = \tilde{g}_{ab}(\lambda_0)\tfrac{\partial\lambda^{a}}{\partial s}(0)\tfrac{\partial\lambda^{b}}{\partial s}(0) = \int_0^t\int_0^t d\tau_2 d\tau_1\left[\langle\tfrac{1}{2}\left\{\tfrac{\partial V}{\partial s}(0,\tau_2),\tfrac{\partial V}{\partial s}(0,\tau_1)\right\}\rangle - \langle\tfrac{\partial V}{\partial s}(0,\tau_2)\rangle\langle\tfrac{\partial V}{\partial s}(0,\tau_1)\rangle\right]\\ &= \{\tfrac{\sin^2(|x(\lambda_0)|t)}{|x(\lambda_0)|^2}[\langle P\tfrac{\partial x}{\partial\lambda^{a}}(\lambda_0), P\tfrac{\partial x}{\partial\lambda^{b}}(\lambda_0)\rangle] + t^2(1-\tanh^2(\beta|x(\lambda_0|))\langle\tfrac{x(\lambda_0)}{|x(\lambda_0)|},\tfrac{\partial x}{\partial\lambda^{a}}(\lambda_0)\rangle\langle\tfrac{x(\lambda_0)}{|x(\lambda_0)|},\tfrac{\partial x}{\partial\lambda^{b}}(\lambda_0)\rangle\}\tfrac{\partial\lambda^{a}}{\partial s}(0)\tfrac{\partial\lambda^{b}}{\partial s}(0),\end{aligned}$$

with the average taken with respect to the thermal state $\rho_0 = \rho(0) \equiv \rho(\lambda_0)$. Also, as mentioned previously, we have the expansion

$$|\mathcal{A}(s)|^2 = |\operatorname{tr}\left[\rho(0)\exp(itH(0))\exp(-itH(s))\right]|^2 = \left|\operatorname{tr}\left[\rho(0)T\exp\left(-i\int_0^t d\tau V(s,\tau)\right)\right]\right|^2 = 1-\tilde{\chi}s^2+\ldots$$

The difference between the two susceptibilities is given by:

$$\tilde{\chi} - \chi =$$
$$(1 - \tanh^2(\beta|x(\lambda_0)|))\{\tfrac{\sin^2(|x(\lambda_0)|t)}{|x(\lambda_0)|^2}[\langle P\tfrac{\partial x}{\partial\lambda^a}(\lambda_0), P\tfrac{\partial x}{\partial\lambda^b}(\lambda_0)\rangle] + t^2\langle\tfrac{x(\lambda_0)}{|x(\lambda_0)|}, \tfrac{\partial x}{\partial\lambda^a}(\lambda_0)\rangle\langle\tfrac{x(\lambda_0)}{|x(\lambda_0)|}, \tfrac{\partial x}{\partial\lambda^b}(\lambda_0)\rangle\}\tfrac{\partial\lambda^a}{\partial s}(0)\tfrac{\partial\lambda^b}{\partial s}(0).$$

As $\beta \to +\infty$, i.e., as the temperature goes to zero, the two susceptibilities are equal. Now, the function

$$f(t) = \frac{\sin^2(\epsilon t)}{\epsilon^2}$$

is well approximated by t^2 for small enough ϵ. In that case the sum of the two terms appearing in the difference between susceptibilities is just proportional the pull-back Euclidean metric on $T\mathbb{R}^3$.

The pullback of the interferometric (Riemannian) metric on the space of unitaries

We first observe that each full rank density operator ρ defines a Hermitian inner product in the vector space of linear maps of a Hilbert space $\mathscr{H}$, i.e., $\mathrm{End}(\mathscr{H})$, given by,

$$\langle A, B\rangle_\rho \equiv \mathrm{tr}\{\rho A^\dagger B\}.$$

This inner product then defines a Riemannian metric on the trivial tangent bundle of the vector space $\mathrm{End}(\mathscr{H})$. Since the unitary group $\mathrm{U}(\mathscr{H}) \subset \mathrm{End}(\mathscr{H})$, by restriction we get a Riemannian metric on $\mathrm{U}(\mathscr{H})$. If we choose ρ to be $e^{-\beta H(\lambda)}/\,\mathrm{tr}\{e^{-\beta H(\lambda)}\}$, then take the pullback by the map $\Phi_t : M \ni \lambda_f \mapsto e^{-itH(\lambda_f)} \in \mathrm{U}(\mathscr{H})$ and evaluate at $\lambda_f = \lambda$, to obtain the desired metric.

Next, we show that this version of LE is closely related to the interferometric geometric phase introduced by Sjöqvist *et. al* [**?** **?**]. To see this, consider the family of distances in $\mathrm{U}(\mathscr{H})$, d_ρ, parametrised by a full rank density operator ρ, defined as

$$d^2_\rho(U_1, U_2) = \mathrm{tr}\{\rho(U_1 - U_2)^\dagger(U_1 - U_2)\} = 2(1 - \mathrm{Re}\langle U_1, U_2\rangle_\rho),$$

where $\langle *, *\rangle_\rho$ is the Hermitian inner product defined previously. In terms of the spectral representation of $\rho = \sum_j p_j \left|j\right\rangle \left\langle j\right|$, we have

$$\langle U_1, U_2\rangle_\rho = \sum_j p_j \left\langle j\right| U_1^\dagger U_2 \left|j\right\rangle .$$

The Hermitian inner product is invariant under $U_i \mapsto U_i \cdot D$, $i = 1, 2$, where D is a phase

matrix

$$D = e^{i\alpha} \sum_j |j\rangle \langle j| .$$

For the interferometric geometric phase, one enlarges this gauge symmetry to the subgroup of unitaries preserving ρ, i.e., the gauge degree of freedom is $U(1) \otimes \cdots \otimes U(1)$. However, since we are interested in the interferometric LE previously defined, we choose not to do that, as we only need the diagonal subgroup, i. e., we only have a global phase. Next, promoting this global U(1)-gauge degree of freedom to a local one, i.e., demanding that we only care about unitaries modulo a phase, we see that, upon changing $U_i \mapsto U_i \cdot D_i$, $i = 1, 2$, we have

$$\langle U_1, U_2\rangle_\rho \mapsto \quad \langle U_1 \cdot D_1, U_2 \cdot D_2\rangle_\rho = \textstyle\sum_j p_j \langle j| U_1^\dagger U_2 |j\rangle e^{i(\alpha_2 - \alpha_1)}.$$

We can choose gauges, i.e., D_1 and D_2, minimising $d_\rho^2(U_1 \cdot D_1, U_2 \cdot D_2)$, obtaining

$$d_\rho^2(U_1 \cdot D_1, U_2 \cdot D_2) = 2(1 - |\langle U_1 \cdot D_1, U_2 \cdot D_2\rangle_\rho|) = 2(1 - |\langle U_1, U_2\rangle_\rho|).$$

Now, if $\{U_i = U(t_i)\}_{1 \leq i \leq N}$ were the discretisation of a path of unitaries $t \mapsto U(t)$, $t \in [0, 1]$, applying the minimisation process locally, i.e., between adjacent unitaries U_{i+1} and U_i, in the limit $N \to \infty$ we get a notion of parallel transport on the principal bundle $\mathrm{U}(\mathscr{H}) \to \mathrm{U}(\mathscr{H})/\mathrm{U}(1)$. In particular, the parallel transport condition reads as

$$\mathrm{tr}\left\{\rho U^\dagger(t) \frac{dU}{dt}(t)\right\} = 0, \text{ for all } t \in [0, 1].$$

If we take $\rho = \exp(-\beta H(\lambda_i))/\,\mathrm{tr}\{e^{-\beta H(\lambda_i)}\}$, $U_1 = \exp(-itH(\lambda_i))$ and $U_2 = \exp(-itH(\lambda_f))$, then the interferometric LE is

$$\mathcal{L}(t, \beta; \lambda_f, \lambda_i) = |\langle U_1, U_2\rangle_\rho| = \langle \widetilde{U}_1, \widetilde{U}_2\rangle_\rho,$$

where $\widetilde{U}_i = U_i \cdot D_i$ $(i = 1, 2)$ correspond to representatives satisfying the discrete version of the parallel transport condition.