Chapter 1

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 [1], 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 dimension of the positions space, in agreement with several recent studies [2–7]. 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. Furthermore, during the completion of this thesis, we also performed the same analysis for 2D topological insulators and superconductors and we obtained qualitatively similar results [8]. The edge states of 2D topological superconductors are used to achieve fault-tolerant topological quantum computing [9,10]. Thus it would be interesting to specialise the general study of the robustness of the edge states presented in [8] in specific models of thermal noise.

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 [11,12]. 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.

Bibliography

[1] G. Nikolopoulos. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A*, 77:032348, Mar 2008.

[2] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61:062308, May 2000.

[3] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:127902, Mar 2002.

[4] D. Bruss, M. Christandl, A. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello. Tomographic quantum cryptography: Equivalence of quantum and classical key distillation. *Phys. Rev. Lett.*, 91:097901, Aug 2003.

[5] G. M. Nikolopoulos and G. Alber. Security bound of two-basis quantum-key-distribution protocols using qudits. *Phys. Rev. A*, 72:032320, Sep 2005.

[6] L. Sheridan and V. Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A*, 82:030301, Sep 2010.

[7] H. F. Chau. Quantum key distribution using qudits that each encode one bit of raw key. *Phys. Rev. A*, 92:062324, Dec 2015.

[8] S. T. Amin, B. Mera, C. Vlachou, N. Paunkovic, and V. R. Vieira. Fidelity and uhlmann connection analysis of topological phase transitions in two dimensions. *arXiv preprint arXiv:1803.05021*, 2018.

[9] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma. Non-abelian anyons and topological quantum computation. *Rev. Mod. Phys.*, 80:1083–1159, Sep 2008.

[10] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2 – 30, 2003.

[11] T. Kitagawa, M. S. Rudner, E. Berg, and E. Demler. Exploring topological phases with quantum walks. *Phys. Rev. A*, 82:033429, Sep 2010.

[12] T. Kitagawa. Topological phenomena in quantum walks: elementary introduction to the physics of topological phases. *Quantum Information Processing*, 11(5):1107–1148, 2012.