**Título:** Passeios quânticos em criptografia e transições de fase topológicas a temperature finita

**Nome:** Chrysoula Vlachou

**Doutoramento em:** Física

**Orientador:** Paulo Alexandre Carreira Mateus

**Co-Orientador:** Nikola Paunković

**Resumo**

A criptografia quântica é uma das mais ativas áreas de investigação, uma vez que se mostrou que a segurana de criptosistemas clássicos atualmente em utilização ficam comprometidos face a adversários com acesso a computadores quânticos. Na primeira parte desta tese, propomos novos e seguros criptosistemas quânticos baseados em passeios quânticos. Estes últimos têm-se vindo a revelar de grande utilidade para diversas tarefas de computação quântica. Em particular, apresentamos um criptosistema quântico de chave pública seguro, como alternativa aos análogos clássicos, cuja segurança cai por terra face a adversários quânticos. Propomos ainda três novos protocolos quânticos de distribuição de chave e analisamos as suas propriedades de segurança e robustez. A criação de memórias quânticas estáveis de longa duração  hoje em dia um dos maiores obstáculos tecnológicos na construção de computadores quânticos escaláveis, e a sua existência ou não tem consequências sérias em ambas a criptografia clássica e a criptografia quântica. Na segunda parte desta tese, estudamos o comportamento, a temperatura finita, de sistemas exibindo ordem topológica, já que possuem propriedades únicas que podem permitir a construção de memórias quânticas. Utilizando a fidelidade entre dois estados quânticos e a condição de transporte paralelo de Uhlmann no espaço das purificações de matrizes densidade, investigamos a existência de transições de fase topológicas a temperatura finita. Provamos ainda a robustez, em função da temperatura, dos estados de fronteira entre duas fases topológicas distintas. Esta análise mostra que não existem transições térmicas de fase e que as propriedades topológicas, presentes a temperatura zero, desaparecem gradualmente à medida que a temperatura sobe. O nosso estudo dos modos de Majorana (estados de fronteira de supercondutores topológicos), a temperatura baixa mas finita, sugere que podem ser realisticamente utilizados para produzir memórias quânticas. Aplicamos ainda a mesma análise aos Hamiltonianos efetivos provenientes de protocolos de passeios quânticos que se sabe simularem fases topológicas. Os resultados obtidos

condizem com os anteriores, indicando a não existência de transições térmicas de fase. Para mais, neste caso, a nossa análise revela a existência de transições paramétricas de fase a temperatura finita, devido à periodicidade temporal dos protocolos de passeios quânticos. Finalmente, investigamos a existência de transições de fase a temperatura finita em sistemas topológicos fora de equilíbrio. Ainda hoje existem duas formas de inferir a possibilidade de transições de fase a temperatura finita para tais sistemas, que levam a resultados contraditórios. Derivamos analiticamente as quantidades em causa e identificamos a origem do paradoxo. Discutimos ainda qual dos métodos melhor captura a natureza multi-corporal de sistemas topológicos e pode ser utilizado em implementações reais.

**Palavras-chave:** criptografia quântica, passeios quânticos, memórias quânticas, transições de fase topológicas, estados de fronteira

**Title:** Quantum walks in cryptography and finite-temperature topological phase transitions

**Abstract**

Quantum cryptography is an active area of research, since it was shown that the security of some of the classical cryptosystems currently used can be compromised by adversaries with access to quantum computers. In the first part of this thesis, we propose new secure quantum cryptosystems based on quantum walks, which have been proved very useful in several quantum computation tasks. In particular, we design a secure quantum public-key cryptosystem, as an alternative to the classical counterparts, whose security can be jeopardised by quantum adversaries. Moreover, we propose three new quantum key distribution protocols and analyse their security and robustness properties.

The design of long-term stable quantum memories is currently one of the biggest technological challenges towards the construction of operational and scalable quantum computers, and their existence or absence has serious implications in both classical and quantum cryptography. In the second part of this thesis, we study the finite-temperature behaviour of systems exhibiting topological order, as they possess some unique properties which could be used to construct quantum memories. By means of the fidelity between two quantum states and the Uhlmann parallel transport condition in the space of the purifications of density matrices, we investigate the existence of topological phase transitions at finite temperatures. We also probe the robustness of the edge states on the boundary between two different symmetry-protected topological phases with respect to the temperature. This analysis shows that there exist no thermal phase transitions and the topological features, present at zero temperature, are gradually smeared out as the temperature increases. Our study of the Majorana modes (edge states of topological superconductors) at low but finite temperatures, suggests that they could be used to achieve realistic quantum memories.

We also performed the same analysis for the effective Hamiltonians resulting from quantum walk protocols that have been shown to simulate symmetry-protected topological phases. The results that we obtained are consistent with the previous, indicating the absence of thermally-driven phase transitions. Moreover, in this case, our analysis revealed the existence of finite-temperature parameter-driven phase transitions.

Finally, we investigated the existence of finite-temperature phase transitions in topological systems out of equilibrium. So far, there exist two different approaches to infer the possibility of phase transitions at finite temperatures for such systems, which were giving

opposite predictions. We analytically derived the relevant quantities and showed the origin of such different behaviours. Moreover, we argued which is the most suitable approach that better captures the many-body nature of topological systems and can be used in realistic implementations.

**Key-words:** quantum cryptography, quantum walks, quantum memories, topological phase transitions, edge states

**Título:** Passeios quânticos em criptografia e transições de fase topológicas a temperatura finita


**Resumo alargado em Português**

Na primeira parte desta tese, apresentamos o nosso trabalho em criptografia quântica baseada em passeios quânticos. Propomos um novo e seguro sistema quântico de chave pública, no qual a chave pública utilizada para a encriptação de mensagens é um estado quântico gerado por um passeio quântico. Uma vez que a segurança de muitos dos sistemas de chave pública clássicos atualmente utilizados fica comprometida face a adversários com acesso a computadores quânticos, cremos que o nosso protocolo oferece uma alternativa útil para as comunicacões quânticos emergentes. Para mais, a nossa proposta apresenta uma melhoria em relação a propostas anteriores, em que a chave pública é gerada via rotações de qubits, um de cada vez, em estados separáveis. Os estados resultantes de um passeio quântico são, em geral, estados entrelaçados, pelo que uma terceira parte que escute a comunicação necessita, em princípio, de aplicar operações substancialmente mais complexas para inferir a chave privada e/ou a mensagem. Consequentemente, a segurança, em termos práticos, do nosso protocolo é maior.

Utilizamos ainda passeios quânticos para desenhar e analisar novos protocolos seguros de distribuição quântica de chaves. Nessa perspetiva, propomos dois novos protocolos de distribuição quântica de chaves, em que as partes trocam chaves geradas a partir dos estados obtidos de certos passeios quânticos para establecer uma chave simétrica que poderão utilizar para a troca de mensagens cifradas ou para fins de autenticação. Também apresentamos uma variação semi-quântica de distribuição quântica de chaves, em que uma das partes pode utilizar exclusivamente operações clássicas. Mostramos que este protocolo, que pode ser considerado mais prático já que necessita de menos hardware quântico, é robusto contra adversários que escutem ou manipulem a comunicação. De facto, se um adversário tentar interferir, será detetado pelas partes legítimas, que poderão abortar o protocolo. Até ao momento, a distribuição quântica de chaves é a instncia mais prática e segura de criptografia quântica, e será portanto de interesse estudar, um futuro, implementações reais das nossas propostas teóricas. Em particular, poder-se-á fazer uma análise detalhada das diversas estratégias de ataque que um terceiro possa ter na presença de ruído, tal como se poderá adaptar os ataques e defesas genéricos que apresentamos para o caso de implementações específicas. Nesta linha, mostramos que o nosso protocolo de distribuição quântica de chaves unidirecional tolera bastante ruído devido á alta dimensão do espaço de posições, o que

vai de encontro a vários estudos recentes. Assim, a aplicação de passeios quânticos para a distribuição quântica de chaves revela-se ser muito promissor para aplicações práticas.

Em suma, a contribuição mais relevante do nosso trabalho é o facto de introduzirmos, pelo que nos parece ser a primeira vez, a utilização de passeios quânticos em criptografia assimétrica e distribuição de chaves, e a prova de que muitas das propriedades dos passeios se traduzem em propriedades significativas de segurança dos protocolos criptográficos. No seguimento deste trabalho, seria particularmente relevante estudar a possibilidade de criar protocolos criptográficos diferentes, tais como transferência oblívia e esquemas de compromisso, ou outras primitivas como autenticação de mensagens e assinaturas digitais, a partir de passeios quânticos.

Na segunda parte da tese, explicamos por que a existência ou ausência de memórias quânticas de longo prazo tem sérias implicações em ambas criptografia clássica e criptografia quântica. Assim, estudamos o comportamento, a temperaturas finitas, de sistemas exibindo ordem topológica, que estão entre os melhores candidatos para o desenho de memórias quânticas. Estudamos as transições de fase de sistemas topológicos a temperaturas finitas recorrendo á fidelidade, como é de uso comum, assim como recorrendo a uma quantidade distinta, associada conexão de Uhlmann e a fidelidade via a métrica de Bures. Aplicamos esta análise a modelos paradigmáticos de insuladores topológicos e supercondutores, e mostramos que as propriedades topológicas presentes a termperatura zero desaparecem gradualmente á medida que a temperatura aumenta. Analisamos ainda um supercondutor topológico trivial, descrito pela teoria BCS. Contrariamente ao caso do supercondutor topológico, ambas as quantidades indicam a existência de transições térmicas de fase, já que o Hamiltoniano BCS efetivo depende explicitamente da temperatura. Explicamos esta divergência comportamental identificando a significância das contribuições térmicas e puramente quânticas para as transições de fase. Acreditamos que o nosso estudo, que revela esta diferença e clarifica o porquê da sua existência, possa ser utilizado para examinar diversas propriedades dos sistemas mencionados em experiências reais. Confirmamos ainda a ausência de transições térmicas de fase em insuladores topológicos e supercondutores, investigando para isso o comportamento de estados de fronteira.

O estudo dos modos de Majorana (estados de fronteira do supercondutor topológico) a temperatura finita sugere que possam ser realisticamente utilizados para obter memórias quânticas. Assim, uma parte relevante do trabalho futuro será um estudo quantitativo aprofundado robustez destes modos face á temperatura no método que propomos.

Fazemos ainda a mesma análise para os Hamiltonianos efetivos resultantes de passeios

quânticos específicos de uma só partícula, que se veio a saber recentemente, simularem todas as fases topológicas em uma e duas dimensões. Em particular, estudamos representantes de duas classes simétricas de insuladores topológicos e chegamos á mesma conclusão: a temperatura efetiva apenas apaga propriedades topológicas exibidas a temperatura zero, sem causar qualquer transição térmica de fase. Para mais, a periodicidade temporal dos protocolos de passeios quânticos revela transições paramétricas de fase a temperatura finita, um comportamento emergente em sistemas periódicos. Fazemos o nosso estudo para estados de Boltzmann-Gibbs com uma só partícula com respeito ao Hamiltoniano efetivo de passeios quânticos de uma só partícula, e também aos seus análogos multi-partículas, e mostramos que o seu comportamento é consistente. Assim, a análise de partículas únicas pode-se vir a revelar uma ferramenta matemática muito útil no estudo dos sistemas multi-partículas correspondentes. Os parâmetros que descrevem passeios quânticos tambêm podem ser facilmente controlados em testes experimentais, oferecendo uma plataforma de simulação para sistemas topologicamente ordenados. Consequentemente, será interessante estudar os efeitos realistas de ruído que possam gerar estes passeios com partículas únicas em estados de Boltzmann-Gibbs, e utilizar a nossa análise para investigar as propriedades topológicas dessas experiências a temperaturas finitas.

Finalmente, estudamos o comportamento da ordem topológica com respeito á temperatura para sistemas fora de equilíbrio. O protagonista no estudo das transições de fase correspondentes para estados puros é o eco de Loschmidt, para o qual existem várias propostas de generalização para estados mistos: o eco da fidelidade de Loschmidt e o eco interferométrico de Loschmidt. Contudo, estas duas quantidades geram previsões paradoxais: o eco da fidelidade de Loschmidt não prevê transições de fase a temperatura finita (o que bate certo com o nosso resultado no caso de transições topológicas de fase em sistemas em equilíbrio), enquanto que o eco interferométrico de Loschmidt mostra a permanência de transições topológicas de fase a temperaturas finitas. De maneira a clarificar a origem desta incongruência, derivamos analiticamente a forma das suscetibilidades dinâmicas associadas. O eco da fidelidade de Loschmidt quantifica o nível de distinção entre estados em termos de medições de propriedades físicas, induzindo uma métrica no espaço de estados quânticos, enquanto que o eco interferométrico de Loschmidt quantifica os efeitos de canais quânticos que agem sobre um estado, induzindo uma métrica de pullback sobre o espaço dos unitários. Assim, argumentamos que o eco da fidelidade de Loschmidt e a sua suscetibilidade dinâmica associada são uma melhor medida a utilizar no estudo de sistemas multi-partículas, enquanto que o caminho interferométrico é preferível quando se consideram sistemas quânticos genuinamente

microscópicos. Para mais, experiências interferométricas involvem a sobreposição coerente de dois estados, o que, no caso de sistemas macroscópicos multi-partículas, é experimentalmente impossível de conretizar com a tecnologia atual.

**Palavras-chave:** criptografia quântica, passeios quânticos, memórias quânticas, transições de fase topológicas, estados de fronteira