*Resumo

tocsectionResumo 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.

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