1.
Introdução

"Teoria da Informação Quântica" é o nome dado a uma nova área do conhecimento que vive na interseção da física quântica, teoria da informação e ciência da computação. Mais do que isso, é a primeira manifestação, após quase um século de existência, dos princípios mais fundamentais da física quântica em outras áreas científicas.

As origens dessa teoria se estendem até o início da década de 60, quando o então jovem Stephen Wiesner comentou com seu colega de faculdade Charles Bennett sobre uma idéia não-ortodoxa que ele havia tido: o "*dinheiro quântico*"[1] [1]. Essa idéia foi a semente do brilhante advento da *criptografia quântica*, quase duas décadas depois, por uma parceria entre Charles Bennett e Gilles Brassard. Ambas as idéias se baseiam em um mesmo princípio fundamental da física quântica: o *princípio da não-clonagem*, que garante que não há meios de se realizar uma cópia idêntica de um estado quântico desconhecido. Essa foi a primeira constatação de que existem aplicações *clássicas* que podem ser realizadas de forma mais eficiente usando sistemas quânticos.

Ainda na década de 80, Richard Feynman observou que simulações de sistemas quânticos complexos em computadores seriam inviáveis, e cogitou a existência de um *computador quântico* para realizar tais tarefas. Supostamente, um computador quântico levaria um tempo exponencialmente menor que um computador clássico para realizar a simulação de um sistema quântico. Descobriu-se em seguida que não apenas isso é verdade como o computador quântico é capaz de realizar diversas tarefas *clássicas* que seriam inconcebíveis para um computador clássico, como por exemplo o famoso algoritmo de Shor para fatoração de números inteiros muito grandes [2]. Todos esses eventos, juntamente com o desenvolvimento tecnológico e o aumento de maturidade da comunidade científica, levaram à explosão de pesquisas nessa área.

[1] Basicamente, tratava-se de uma idéia de aplicar conceitos fundamentais da física quântica para evitar falsificação de cédulas monetárias.

Hoje em dia, a produção científica e o desenvolvimento de aplicações em informação quântica é tão grande que está surgindo, paulatinamente, uma necessidade de adaptação do mercado de telecomunicações à nova realidade. A criptografia quântica, por exemplo, já pode ser encontrada comercialmente disponível, mas foram necessários alguns anos para que os dispositivos ópticos e eletrônicos necessários se tornassem realidade. Como a informação é codificada em fótons individuais[2], surgiu uma enorme demanda por detectores ultra-sensíveis que sejam capazes de detectar a presença de apenas um fóton. Um dispositivo que utiliza um desses detectores e que é indispensável para qualquer sistema de comunicações quânticas é o chamado Módulo de Contagem de Fótons Únicos (SPCM, *Single Photon Counting Module*), que é capaz de dizer o número de fótons presentes em um pulso de luz[3].

Já existe uma grande variedade de SPCMs, disponíveis para diferentes comprimentos de onda, principalmente aqueles que coincidem com as freqüências de telecomunicações utilizadas em transmissão atmosférica ou via fibras ópticas. No entanto, a busca por melhores detectores está longe de terminar, e envolve diversos centros de pesquisa no mundo todo.

O objetivo dessa tese é desenvolver dois novos tipos de detectores que possam ser utilizados para contagem de fótons que utilizam a mesma idéia básica: explorar a rapidez e eficiência dos detectores de silício. Sensíveis apenas a uma faixa restrita do espectro, entre 400 e 1000 nm, os fotodiodos avalanche de silício (Si APD) não podem ser utilizados em outros comprimentos de onda, a não ser que os fótons que desejamos detectar sejam previamente convertidos em freqüência para essa faixa espectral. Isso pode ser realizado utilizando um processo conhecido desde o fim da década de 50, chamado de *frequency up-conversion*, na qual um fóton interage com um feixe intenso de luz em um meio não-linear e tem sua freqüência alterada.

---

[2] O termo em inglês *single photon* foi traduzido, ao longo da tese, de diversas formas, tais como "fóton único", "fóton individual", "fóton isolado" ou até mesmo "fóton simples". Todas as denominações, portanto, são equivalentes.

[3] No entanto, se dois ou mais fótons chegam ao dispositivo em um intervalo de tempo inferior à sua resolução temporal, apenas um pulso de contagem é produzido. Uma nova geração de contadores de fótons, chamada de *photon number resolving*, está sendo desenvolvida para superar essa limitação [3].

Devido à grande diferença e aplicabilidade dos dois detectores, cada um deles será considerado um *projeto* independente. Cronologicamente, o primeiro deles consiste em implementar um contador de fótons no infravermelho médio, que é a região do espectro que se estende de ~ 3 a ~ 20 μm, e realizar um estudo de viabilidade de criação de um sistema de criptografia quântica no espaço livre que utilize um comprimento de onda nessa faixa. O segundo projeto prevê a construção de um contador de fótons para o comprimento de onda de telecomunicações de 1.55 μm que apresente maior rapidez que os existentes no mercado e menor ruído que os recentes projetos apresentados pela comunidade científica nos últimos anos.

Esta tese encontra-se estruturada da seguinte forma: o capítulo 2 apresenta os conceitos fundamentais da teoria de informação quântica, incluindo uma introdução à criptografia quântica. O capítulo 3 se concentra em classificar e explicar o comportamento não-linear de alguns materiais, e como esses fenômenos podem ser utilizados para realizar a conversão de freqüências dos fótons únicos que desejamos detectar. Os capítulos 4 e 5 se dedicam, cada um, a descrever um dos projetos. Por motivos meramente didáticos, a ordem cronológica não foi respeitada, e começamos a discussão pelo projeto de contagem de fótons a 1.55 μm no capítulo 4. Finalmente, uma conclusão do trabalho realizado é fornecida no capítulo 6.