1.
Introdução

Apesar de conhecida há bastante tempo, há pouco mais de vinte e cinco anos encontraram-se aplicações práticas para a mecânica quântica. O primeiro campo a surgir, a *Criptografia Quântica* tem como marco inicial o trabalho publicado por Bennett, Brassard, Breidbart e Wiesner em 1982 [1]. Entretanto, a idéia básica por trás desta área emergente nasceu na década de 1970, sob o nome de *Conjugate Coding*, tardiamente publicada por Wiesner em 1983, que dissertava a respeito do conceito abstrato de dinheiro quântico à prova de falsificação [1,2]. Na verdade, quando se pensa em criptografia quântica, está-se falando, mais especificamente, de *distribuição quântica de chaves* (QKD – *Quantum key distribution*), ou seja, como duas partes podem compartilhar, de forma segura, um segredo, que será utilizado posteriormente na encriptação da mensagem. Essa denominação foi introduzida por Bennett e Brassard em um artigo publicado em 1984 [1,3], dando origem ao protocolo de comunicação BB84 que estabeleceu os principais passos necessários para que haja uma seção de comunicação deste tipo, complementado pelas considerações apresentadas no protocolo B92 (Bennett 1992) [4]. Curiosamente, Ekert descobriu de forma independente a criptografia quântica em 1991, porém com estados quânticos emaranhados [6].

O primeiro sistema experimental fisicamente implementado, por Bennett, Bessette e Brassard, em 1989, apesar de cobrir uma distância de 32,5cm, foi fundamental para a aceitação por parte da comunidade científica destes novos conceitos [1]. Esforços vêm sendo feitos em vários centros de pesquisa e universidades ao redor do mundo no sentido de viabilizar um sistema capaz de distribuir chaves com taxas de transmissão altas e por grandes distâncias sem que se perca a condição de segurança. Há relato da ultrapassagem da barreira dos 100km com taxa de 166bit/s e de enlaces de alta taxa, como 2Mbit/s sobre 10km [5], além de sistemas do tipo *Plug&Play* [6].

Os fótons são as entidades quânticas especialmente atraentes para este tipo de comunicações. Suas principais características passíveis de codificação são a polarização e a fase, sendo que a escolha adequada depende, entre outros fatores, do tipo de canal pelo qual se deseja transmitir.

Para transmissão por canal cabeado, geralmente fibras ópticas monomodo padrão ou com dispersão deslocada (DS – *Dispersion shifted*), a codificação por fase pode se mostrar mais atraente, apesar da necessidade de estabilização precisa dos interferômetros requeridos, enquanto que a transmissão em espaço livre pode ser feita com codificação por polarização, sem as dificuldades impressas pelos efeitos da dispersão em fibra devido à polarização (PMD - *Polarization-mode dispersion*), gerada pela variação aleatória da birrefringência do meio.

Todavia, há ainda uma alternativa para codificação dos bits quânticos (qubits – *quantum bits*) introduzida por Merolla em 1999 [7] e adaptada para o protocolo BB84 por Xavier e von der Weid em 2005 [8]. O grau de liberdade do sistema utilizado para a codificação neste caso se refere à fase relativa entre as bandas laterais e a portadora óptica de um sinal óptico coerente modulado. É então proposta a montagem de um sistema de transmissão quântica por fibra-óptica com codificação de fótons em freqüência através de dupla-modulação em amplitude e fase. O sistema implementado se assemelha ao da referência [27], porém com as devidas correções para que seja compatível com o protocolo BB84 [8].

Os qubits a serem transmitidos serão modulados em amplitude com banda lateral dupla (DSB – *Dual Sideband*) por um sinal de rádio-freqüência (RF) cuja fase é escolhida por meio de um modulador de fase em quadratura (QPSK - *Quadrature Phase-Shift Keying*) dentre quatro possibilidades.

Na recepção, o sinal é novamente modulado, porém em fase, de acordo com o sinal de rádio-freqüência idêntico ao anterior, mas com nova fase, escolhida por meio de um segundo QPSK, agora dentre duas opções. Este sinal de RF, utilizado tanto na transmissão quanto na recepção, será sincronizado por meio de um canal adicional utilizando a técnica de multiplexação por divisão no comprimento de onda (WDM - *Wavelength-division multiplexing*).

Após este processo de codificação (primeira modulação), transmissão e decodificação (segunda modulação), deve-se extrair a informação do sinal óptico. Para isso, serão utilizados dois filtros de Fabry-Perot em série, formados, cada um, por duas redes de Bragg adequadamente espaçadas, possibilitando a filtragem da portadora óptica. De acordo com a combinação de fases da dupla-modulação, o sinal pode ter banda lateral única (SSB – *Single sideband*) ou dupla. Elas serão separadas segundo sua freqüência óptica por um interferômetro de Mach-Zehnder desbalanceado, para que possam ser entregues a um detector de fótons únicos e revelar o bit transmitido.

Este estudo apresenta na seção 2 o contexto clássico que motiva a pesquisa e desenvolvimento da área de criptografia quântica, que surge como solução para alguns problemas iminentes da distribuição de chaves.

A seção 3 enfoca a criptografia quântica como solução na distribuição de chaves privadas, seus fundamentos e elementos básicos, como os conceitos de qubits e emaranhamento, bem como os protocolos e as etapas de uma seção de comunicação.

A seção 4 trás os elementos constituintes de um sistema físico de distribuição quântica de chaves e considerações a respeito dos tipos de dispositivos de cada parte do enlace.

O sistema proposto é apresentado na seção 5, assim como o sistema implementado. Cada elemento relevante é analisado e caracterizado por meio de medições experimentais.

A seção 6 descreve os procedimentos e metodologia de medição do sistema, descritos em etapas, seguidos dos resultados obtidos.

Finalmente, na seção 7 apresentam-se as conclusões a respeito deste estudo e as perspectivas de continuação.