6 Conclusões e considerações finais

A mecânica quântica, após um século de desenvolvimento, encontra finalmente aplicações práticas no nível de manipulação de estados quânticos individuais. A fusão dela com a teoria da informação abre inúmeras novas possibilidades bem como cria uma multidisciplinaridade jamais vista antes, já que o desenvolvimento de técnicas de processamento de informação quântica requer o trabalho conjunto de matemáticos, físicos, engenheiros, químicos, entre outros.

Se um dia realmente viermos a construir o tão sonhado computador quântico, nossas noções clássicas de informação serão muito aprofundadas. Com objetivos mais modestos, a criptografia quântica ainda tem muito a ser desenvolvida. Do ponto aonde nos encontramos até o dia em que todas as comunicações estejam empregando QKD, ainda há um longo caminho a ser percorrido.

Como foi visto, os sistemas de QKD ainda são extremamente limitados ambos em distância e em taxa de transmissão, especialmente se comparados aos modernos sistemas de comunicação ópticos alcançando milhares de quilômetros a taxas de muitos Gb/s. Para que haja um grande avanço em relação à sua performance dois saltos são necessários:

- Desenvolvimento de uma fonte que envie fótons unitários ao comando do usuário, isto é, não poissoniana. Isso permitirá a utilização de um fóton por pulso aumentando em dez vezes a taxa sem comprometer a segurança.
- SPADs melhores para a região de 1550nm. Os detectores de InGaAs utilizados atualmente têm uma eficiência quântica que mal beira os 10%, além de serem ruidosos. Eles são o principal fator limitante da distância. Uma crescente demanda por esses SPADs poderá estimular os fabricantes a melhorar seu desempenho.

Nesse trabalho, foi analisado em detalhes o sistema de QKD utilizando codificação por freqüência. Três possíveis esquemas de modulação (AM-AM, PM-PM e AM-PM) foram investigados. Foi demonstrado que os sistemas AM-AM (utilizando moduladores MZ *zero-chirp*) e PM-PM são na realidade equivalentes e só suportam o protocolo B92 ou BB84 modificado. Foi proposto

um novo sistema (AM-PM) que pode acomodar o protocolo BB84 clássico. Este protocolo apresenta vantagens sobre os outros dois, pois é mais seguro que o B92 [16] e consegue transmitir a uma taxa mais elevada do que o BB84 modificado. Finalmente foram feitas medidas do sistema operando em modos CW e pulsado com o intuito da comprovação da teoria apresentada.

Para a continuação deste trabalho, está prevista a utilização do sistema no regime quântico, utilizando SPADs. Com isto podem ser feitas comparações entre os diferentes protocolos, bem como estudos referentes à distância de transmissão.