7.
Conclusões

Há várias pesquisas ativas sobre as possibilidades das telecomunicações quânticas, destacando-se a criptografia. Fundamentada na física quântica, a distribuição quântica de chaves se apresenta como solução para o principal problema da criptografia clássica de chave privada, ou seja, soluciona o problema do compartilhamento da chave entre as partes comunicantes sem a necessidade de contato direto e de forma comprovadamente segura. Tal chave será posteriormente empregada na codificação da mensagem a ser transmitida, com a restrição de que seja utilizada uma única vez (*one-time pad*). Tal sistema apresenta vantagens em relação ao de chave pública, para qual há a possibilidade de descoberta de um algoritmo de fatoração que agilize a quebra da chave, agravada pelo iminente surgimento do computador quântico (para o qual já há tal algoritmo).

Os sistemas QKD já chegam a implementações comerciais do tipo P*lug&Play* [6]. Os avanços nesta área são claros e os enlaces já ultrapassam uma centena de quilômetros [5], um aumento significativo em relação à primeira transmissão, efetuada em 1989, de 32,2cm [1]. As taxas de transmissão também apresentam desenvolvimento significativo, podendo-se citar o valor de 2Mbit/s sobre 10km [5]. Novas técnicas vêm sendo desenvolvidas, como a utilização de detecção homódina [24], codificação por fase diferencial [25] ou conversão de freqüência óptica através de guias de onda PPLN para utilização de detectores de silício [5].

É fato a dificuldade em se manter as polarizações corretas nos sistemas cabeados com fibras convencionais ao se utilizar a codificação por polarização, necessitando de controle ativo de polarização. Além disso, no esquema de codificação por fase, há a necessidade de estabilização térmica tanto do interferômetro de Alice quanto do interferômetro de Bob. Como eles se encontram afastados, os controles individuais devem ser interdependentes, necessitando de um canal extra de sincronismo. Portanto, pode não ser tão fácil manter a temperatura de ambos devidamente ajustadas, sendo que variações mínimas nas temperaturas podem resultar em variações críticas de fase no sistema.

Justifica-se, então, a opção pela codificação em freqüência dos pulsos ópticos altamente atenuados. O experimento implementado apresentou os resultados qualitativos corretos, demonstrando a possibilidade de codificação e decodificação dos qubits nas bandas laterais do sinal óptico de acordo com a fase relativa à portadora, com a devida recuperação dos bits enviados. Quantitativamente, observa-se que a QBER está abaixo do limite de 15% [6] (quando assumidos ataques individuais por parte de Eva), atestando a viabilidade do sistema. Na medição do sistema com escolha de fase pelos moduladores QPSK sem o enlace de sincronismo, obtém-se QBER inferior a 11% (caso seja realizado um pré-processamento dos bits por Alice, este valor se eleva para 12,4%), o que mostra a possibilidade de se implementar um sistema absolutamente seguro, mesmo contra ataque coerentes [11]. A utilização de um detector de fótons únicos com maior eficiência e menos ruído possibilitaria a melhora deste parâmetro, permitindo maior contagem de fótons e menor contagem de escuro. Com isso, o ruído pode ser reduzido em pelo menos uma ordem de grandeza, resultando em maior visibilidade e redução de sua contribuição para a QBER do sistema.

A diferença entre as razões de contraste obtidas para as diferentes fases de Alice, quando Bob os decodifica na base correta, deve-se em parte ao interferômetro de Mach-Zehnder, já que, de acordo com a caracterização, suas saídas não são exatamente idênticas em relação à potência do sinal, e em parte pelo desvio de fase dos moduladores QPSK, de até 6,42°. Esses fatores também justificam a assimetria de contagens nos casos em que há ambigüidade de bandas laterais. Apesar de inicialmente poderem revelar à Eva qual base foi escolhida por Alice, esses qubits serão descartados, não comprometendo a confidenciabilidade da chave.

O alargamento espectral experimentado pelo sinal óptico ao ser modulado em fase pelo sinal de rádio-freqüência recuperado por Bob através do enlace de sincronismo poderia ser minimizado com a utilização de amplificadores de RF com menor figura de ruído. Esse fator influencia severamente, como foi verificado com diversas combinações de dispositivos disponíveis, até se chegar à configuração que gerou os resultados apresentados no terceiro grupo de medições. Além disso, o orçamento de potência para a modulação em Alice e em Bob ficou ligeiramente deficiente, ou seja, ao se enviar o sinal de RF para Bob por WDM através do canal de sincronismo, não houve a restauração eficiente da potência ótima para que fossem reproduzidas as condições do

sistema das medições anteriores, o que resultou em prejuízo nas taxas de contagem.

Desde o ajuste dos moduladores AM e PM para obter-se a razão de contraste ótima da supressão de banda lateral, passando pelos filtros de Fabry-Perot com redes de Bragg e o interferômetro de Mach-Zehnder, verificou-se uma grande dependência da polarização no sistema experimentalmente implementado. Tal dependência torna difícil o ajuste correto de tantos parâmetros, já que os dispositivos devem operar simultaneamente. Apesar de não ser impeditiva no caso de demonstração experimental, uma vez que os ajustes se mantêm por tempo suficiente para que sejam feitas as medições, essa dependência pode tornar inviável a aplicação comercial do sistema, a menos que sejam utilizados dispositivos menos sensíveis à polarização, luz despolarizada ou compensação ativa de polarização.

No caso do sistema de codificação por dupla modulação em amplitude e fase, a polarização interfere diretamente na profundidade de modulação, já que os dispositivos utilizados são constituídos de guias de onda em niobato de lítio, e apenas o componente não-ortogonal do campo da portadora em relação à geometria do guia será modulado. A utilização de luz despolarizada levaria a uma profundidade de modulação média, que tornaria o sistema estável, apesar de se perder o ponto ótimo de operação.

Os filtros de Fabry-Perot apresentaram grande dependência da polarização devido ao tipo de fibra utilizado para a marcação holográfica das redes de Bragg.

O interferômetro de Mach-Zehnder depende da polarização da luz para que haja a interferência entre os campos, problema semelhante ao dos moduladores.

Esforços têm sido feitos no sentido de tornar este sistema comercial. Há relatos de implementação experimental em campo atingindo distância de 10km com QBER igual a 3% e taxa de transmissão de qubits de 400Hz, estável por 30 minutos [27].

Pode ser dada continuidade ao trabalho realizado, com foco em dois pontos: a interface de comunicação de um computador com o sistema, para a transmissão da chave propriamente dita, e a construção do detector de fótons únicos.

A interface deve ser tal que os bits possam ser gerados, mesmo que pseudo-aleatoriamente por um computador e transmitidos ao sistema, seja diretamente aos moduladores QPSK ou por intermédio de um microcontrolador

tipo PIC ou por FPGA, como na figura 60. Além disso, deve ser enviado um sinal de *clock* de Alice para Bob (ou de Bob para Alice), um sinal de gatilho para o gerador de pulsos de Alice e um sinal de gatilho para o detector de Bob, ajustando-se os tempos e atrasos corretos. Também é necessária a aquisição das detecções dos SPAD, para que possa ser feito o processo de reconciliação, correção de erro, amplificação de privacidade e estatísticas necessárias.

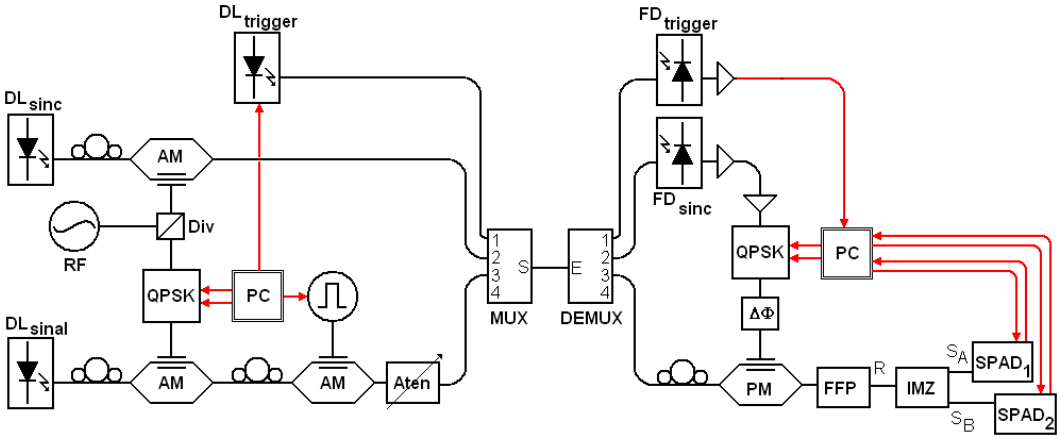

Figura 60: Sugestão de sistema para continuação do trabalho.

Em relação ao detector de fótons únicos, tentou-se construir um par destes dispositivos, porém sem obterem-se resultados satisfatórios. Acredita-se que o problema encontrado seja de caráter elétrico e esteja concentrado no circuito de subtração utilizado no modo gatilhado. Apesar de a eficiência do fotodiodo de avalanche estar de acordo com o esperado, é necessário que incida uma potência óptica relativamente alta para que a contagem seja satisfatória.

Há, portanto, a possibilidade de desenvolvimento de um SPAD, que envolveria sua estabilização térmica e o circuito de compensação de capacitância e subtração dos pulsos derivados. O dispositivo, construído em par, poderia, além de sua já citada utilização em distribuição quântica de chaves, poderia ser utilizado em outras em aplicações, como refletometria óptica no domínio do tempo ou espectroscopia [28].