Relatório Final de F809

Criptografia quântica: o Protocolo B92

13 de Junho de 2005

Aluno: Felipe Lourenço - R.A.: 016035

Orientador: Prof. Antonio Vidiella Barranco (DEQ)

1 Introdução

A criptografia quântica é um tema de estudos que vem se tornando cada vez mais recorrente nos dias de hoje. Desde a primeira proposta de um protocolo que tem a sua segurança baseada em princípios da física [1], diversas outras propostas e melhorias surgiram com o objetivo de tornar a distribuição quântica de chaves mais viável e confiável.

Distribuição de chave é o nome que se dá paras as técnicas que possibilitam a troca de sequências de bits entre duas partes com um alto nível de segurança, de forma que ninguém mais tenha informações significantes sobre elas. Tal chave secreta torna possível que as duas partes interessadas (**A***lice* e **B***ob*) se comuniquem, com segurança garantida, e atinjam os dois objetivos principais da criptografia: codificar uma mensagem para que ela se torne incompreensível à terceiros e garantir ao receptor que a mensagem não foi alterada durante a transmissão.

Se A e B não compartilham nenhuma informação secreta inicialmente, então uma das formas de se conseguir a troca de uma chave secreta são as transmissões quânticas, que em princípio não podem ser monitoradas sem alterações .

Vários tipos de transmissões quânticas já se mostraram suficientes, algumas delas são: uma sequência aleatória de partículas de spin $1/2$ ou fótons únicos em quatro estados não ortogonais de polarização , uma sequência análoga de pulsos de luz coerente e de baixa intensidade, uma sequência de dois fótons emaranhados (EPR) e etc. Neste projeto, por sua vez, escolhemos explorar o protocolo chamado de B92 [2]. Isso porque a sua implementação é relativamente mais simples que

a dos outros, o que facilita a compreensão para alguém que está vendo este assunto pela primeira vez. Este protocolo usa como base quaisquer dois estados quânticos não ortogonais.

Com esse projetos prentendemos explicar a proposta teórica do protocolo, o seu experimento e elaborar uma simulação do mesmo.

2 O Protocolo B92

Para introduzirmos o protocolo em si, devemos adotar dois estados quânticos não ortogonais:

$$|h\rangle \equiv bit\,0 \qquad |r\rangle \equiv bit\,1$$

Pensando em estados de fótons únicos (utilizados no experimento mostrado na próxima seção) esses estados podem ser: polarização horizontal $|h\rangle$, vertical $|v\rangle$, circular à direita $|r\rangle$ e circular à esquerda $|l\rangle$.

Alice, quem envia os bits, deve então gerar uma sequência arbitrária de bits 0 ou 1 (dos estados acima) e enviá-la à Bob. Já este, deve escolher, de forma aleatória também, com qual dos operadores de medida ele irá realizar as medidas dos estados enviados por Alice. Os operadores de medida são:

$$\hat{P}_v = |v\rangle\langle v| \qquad \hat{P}_l = |l\rangle\langle l|$$

Devemos notar que os operadores de medida $\hat{P}_v$ e $\hat{P}_l$ são formados por estados ortogonais aos estados que definem os bits 0 e 1, respectivamente. É válido dizer que dois estados $|a\rangle$ e $|b\rangle$ são ortogonais se $\langle a|b\rangle = 0$ e não-ortogonais se $\langle a|b\rangle \neq 0$. Utilizando isso podemos chegar na seguinte conclusão

$$\hat{P}_v|h\rangle = 0 \tag{1}$$

$$\hat{P}_v|r\rangle \neq 0 \tag{2}$$

$$\hat{P}_l|h\rangle \neq 0 \tag{3}$$

$$\hat{P}_l|r\rangle = 0 \tag{4}$$

A partir disso, chegamos que a aplicação 2 nos revela os bits 1 e a aplicação 3 os bits 0.

Com apenas esses elementos já é possível fazer uma primeira implementação do protocolo. Suponha que Alice tenha gerado a seguinte sequência aleatória de estados:

$$|h\rangle \quad |h\rangle \quad |r\rangle \quad |h\rangle \quad |r\rangle \quad |r\rangle \quad |h\rangle \quad |r\rangle$$

O que equivale a seguinte sequência de bits:

$$0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1$$

Esses estados devem então ser enviados para Bob através de um canal quântico (fibra óptica, ar...). Bob, por sua vez, escolhe a seguinte sequência arbitrária de medidas

$$\hat{P}_v \quad \hat{P}_l \quad \hat{P}_v \quad \hat{P}_l \quad \hat{P}_l \quad \hat{P}_v \quad \hat{P}_v \quad \hat{P}_l$$

O resultado obtido é

$$= 0 \quad \neq 0 \quad \neq 0 \quad \neq 0 \quad = 0 \quad \neq 0 \quad = 0 \quad = 0$$

A próxima etapa é a reconciliação dos bits (enviados e medidos) através da comunicação por um canal público. Bob diz à Alice qual foi a sua sequência de medidas. Veja bem, ele deve dizer apenas qual foi o operador usado em cada medida e não o resultado da mesma. Alice deve então responder quais medidas foram feitas com o operador correto (aquele não ortogonal ao estado enviado). Após essa reconciliação , Bob e Alice devem guardar apenas os bits para os quais o estado enviado e a medida feita concordam (ou seja, cuja medida resultou em $\neq 0$). Com isso, a sequência de bits compartilhados no exemplo acima é

$$0 \quad 1 \quad 0 \quad 1$$

Como podemos perceber, existe uma taxa de perda de bits mesmo que não haja nenhuma tentativa de espionagem. Vale dizer que nos protocolos de criptografia quântica a espionagem se torna uma tarefa árdua (se não praticamente impossível) devido à características do sistema físico envolvido. No caso das transmissões de fótons únicos, por exemplo, a indivisibilidade do fóton, a impossibilidade de clonagem e a não ortogonalidade dos estados usados, garantem que a espiã Eve não conseguirá clonar os bit enviados e nem mesmo realizar medidas em alguma amostra de bits sem ser detectada pela maior taxa de erro nas medidas de Bob que ela irá causar.

Dando sequência ao protocolo, é necessário que técnicas clássicas de detecção de erro sejam usadas para se obter uma chave "pura", que será usada para codificar a mensagem a ser transmitida entre Alice e Bob.

Para finalizar, é preciso dizer que esse protocolo requer um aparato que possibilite a detecção dos fótons com extrema sensibilidade, já que erros nessa discriminação poderiam tornar inviável troca de bits.

3 O Experimento

Nessa seção apesentaremos o experimento realizado em [3]. O experimento consiste em realizar uma distribuição quântica de chave (QKD, em inglês) pelo ar (ou espaço livre, traduzindo literalmente). Como os próprios autores do trabalho indicam, o sucesso dessa QKD depende da transmissão e da detecção de fótons únicos por um meio turbulento e de grande "background". Apesear disso, eles dizem que a combinação de medidas em subnanosegundos, filtragem espacial e óptica adaptativa podem tornar os problemas de detecção tratáveis. Ainda mais, dizem que a natureza não birrefringente da atmosfera em comprimentos de onda visíveis permite a transmissão segura de estados de polarização de fótons únicos usados no protocolo de QKD no espaço livre.

A primeira etapa é a emissão dos bits por Alice. O equipamento utilizado será descrito a seguir.

Na figura acima estão representados os seguintes componentes: um laser mono-modo de diodo, uma fibra que o conecta à um filtro interferômetro (IF) de 2.5nm de largura de banda, um atenuador óptico variável, um divisor de feixe de polarização (PBS), uma célula de Pockels e um expansor de feixe de 27 vezes. O laser é ajustado pela temperatura para 772 nm e é configurado para emitir pulsos de aproximadamente 1 ns, que contém aproximadamente 10^5 fótons.

Essa montagem deve ser usada da seguinte maneira: um sistema computacional de controle (Alice) inicia o protocolo emitindo pulsos de laser numa taxa já combinada anteriormente com o

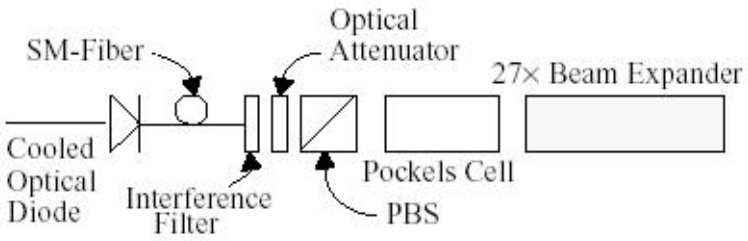

Figura 1: Aparato experimental de transmissão (Alice) para a distribuição quântica de chave.

receptor Bob. Cada pulso de laser é lançado no espaço livre pelo IF e é atenuado para ter em média menos de um fóton por pulso. Perceba que o pulso atenuado é apenas uma aproximação para o estado de um único fóton, nesse trabalho eles testaram o sistema com médias $< 0,1$ fóton por pulso, o que corresponde a uma probabilidade $< 0,5\%$ de se ter um estado de 2 fótons[1]. Os fótons que passam pelo atenuador são polarizados pelo PBS que transmite uma média de menos de um fóton $|h\rangle$ para a célula de Pockels. Essa célula tem um interruptor que aleatóriamente deixa o fóton passar sem mudaça no estado $|h\rangle$ ou no estado $|r\rangle$ com um retardo de $1/4$ de onda. Esse interruptor aleatório é controlado pela tensão gerada por uma fonte de ruído branco.

Com os fótons já enviados temos que analisar agora o receptor. O aparato experimental está esquematizado na figura abaixo.

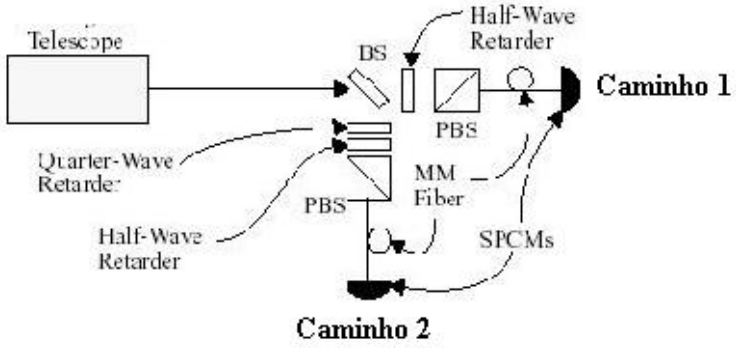

Figura 2: Aparato experimental do receptor (Bob) para a distribuição quântica de chave.

Ele consiste de um telescópio Cassegrain de 8,9 cm, seguido pelo receptor óptico e detectores. O primeiro deles contém um divisor de feixe (BS) de 50/50, que aleatóriamente dirige os fótons coletados em um dos dois caminhos ópticos. O caminho 1 (indicado na figura) é formado por uma placa de $1/2$ onda e um PBS para testar os fótons coletados para o estado $|r\rangle$, ou seja, esse caminho revela os bits 1 (equivale ao operador $\hat{P}_v$ da seção anterior). O caminho 2 consiste de uma placa de $1/4$ de onda, seguida por uma placa de $1/2$ onda e um PBS para testar o estado $|h\rangle$, ou seja, esse caminho revela os bits 0 (como o operador $\hat{P}_l$). Para coletar esses dados foram usadas fibras mulltimodos (MM) conectadas à um detetor de fótons individuais (SPCM). No trabalho [3] os au-

[1]Essa é uma falha que pode ser aproveitada pela espiã Eve, como dois fótons foram enviados ela pode medir um e deixar o outro passar para o Bob.

tores dizem que as fibras MM garantiam a filtragem espacial, reduzindo o background do ambiente, durante a noite, para níveis desprezíveis.

Para entendermos o que ocorre fisicamente com os fótons durante o experimento, vamos analisar os seguintes exemplos:

1. Alice emite um fóton $|r\rangle$. Ao chegar no telescópio de Bob ele pode fazer um dos dois caminhos:

   Caminho 1 Ao passar pela placa de $1/2$ onda esse fóton é convertido para $|l\rangle$ e é transmitido para o SPCM ou refletido com igual probabiliade pelo PBS. Para fazermos a ligação entre o experimento e a teoria devemos notar que essa medida é representada pela equação 2.

   Caminho 2 Ao passar pelas placas de $1/4$ de onda e de $1/2$ onda esse fóton é convertido para $|v\rangle$ e é refletido pelo PBS, ou seja, não é detectado pelo SPCM. Isso é representado pela equação 4.

2. Alice emite um fóton $|h\rangle$. Ao chegar no telescópio de Bob ele pode fazer um dos dois caminhos:

   Caminho 1 Ao passar pela placa de $1/2$ onda esse fóton é convertido para $|v\rangle$ e é refletido pelo PBS, ou seja, não é detectado. Esse fato aparece na equação 1

   Caminho 2 Ao passar pelas placas de $1/4$ de onda e de $1/2$ onda esse fóton é convertido para $|r\rangle$ e é transmitido para o SPCM ou refletido pelo PBS com igual probabilidade. Aqui temos o processo da equação 3.

Esse experimento foi realizado com distâncias de 240m, 500m e 950m entre o emissor e o receptor, durante a noite. O feixe emitido foi sempre refletido por um espelho de 25,4cm colocado na metade da distância de transmissão. A taxa de erro nos bits (razão entre os bits errados e os bits recebidos) para 950m foi $\sim 1,5\%$, com o sistema operando com menos de 1 fóton por pulso. Para 240m essa taxa foi de $\sim 0,7\%$ e para 500m $\sim 1.5\%$ também. Eles dizem que os erros causados pelo background do ambiente foram minimizados para menos de 1 a cada 9s pelo ajuste do tempo das janelas de emissão e de detecção (~ 5ns) e pela filtragem espacial. Além disso, dizem que o detector fazia uma medida errada (dark count) apenas a cada 125s. Com base nisso, argumentam que as taxas de erro apresentadas ocorreram devido à imperfeições e desalinhamento dos componentes ópticos (placas de onda e célula de Pockels).

Uma conclusão interessante apresentada pelo autores é a de que existe a possibilidade de se conseguir fazer uma QKD entre uma base terrestre e um satélite em órbita. Isso porque, segundo eles, a influência da turbulência é dominante nos primeiros 2 km de atmosfera. Então, os minutos nos quais o satélite está no campo de visão da base terrestre seriam suficientes para gerar uma chave com uma enorme quantidade de "raw bits", a partir dos quais poderia se obter uma chave menor (mas ainda sim com milhares de bits) que após correções de erros e amplificação da privacidade estaria pronta para ser usada.

4 Simulação

Para a simulação desse protocolo utilizou-se o software *Mathematica*. A notação usada aqui é um pouco diferente daquela usada na seção 2: P_1 se refere ao operador que revela os bits 1 (análago ao operador P_v da seção 2) e P_0 é o operador que revela os bits 0 (análago ao operador P_l).

A simulação do protocolo é dividida entra as seguintes etapas:

1. Alice gera uma sequência aleatória de bits 0 e 1 e os envia para Bob através do canal quântico.
2. A espiã (Eve) realiza o que é chamado de "ataque opaco". Ela realiza uma medida, aleatória, em alguns dos bits enviados por Alice e envia outro bit para que Bob possa medir. Se Eve conseguir detectar qual bit ela mediu, então ela envia o mesmo bit para o Bob, caso contrário ela envia um bit aleatório. Perceba que, dessa maneira, a espiã causa um aumento na taxa de bits errados e é a partir disso que ela pode ser detectada.
3. Bob escolhe aleatóriamente a sequência de medidas que ele ralizará nos bits (estados quânticos) enviados por Alice (ou Eve no caso de espionagem).
4. Bob comunica a Alice, publicamente, quais foram as suas medidas que tiveram resultado diferente de zero. Note que durante as medidas experimentais de Bob podem ocorrer erros e ele pode obter um resultado nulo mesmo que utilize o operador esperado, ou o contrário. Isso deve ser corrigido posteriormente, a partir de um tratamento adequado dos bits, no qual alguns bits são "sacrificados".
5. Após essa comunicação , Bob e Alice têm uma chave (sequência de bits) em comum. A partir dela, eles podem revelar publicamente alguns bits da chave, fazendo uma verificação estatística da taxa de erro. Uma taxa de erro elevada acusaria a presença da espião Eve.

4.1 O Algoritmo

O algoritmo desenvolvido permite que as seguintes quantidades sejam dadas como valores de entrada:

1. Números de bits enviados por Alice (n).
2. Opção para que a espiã ataque, ou não, o protocolo.
3. Taxa de acerto nas medidas de Bob (TAB). A probabilidade de Bob fazer uma medida errada é $1/(1+\text{TAB})$.
4. Taxa de acerto nas medidas da espiã (TAE). A probabilidade da espiã fazer uma medida errada é $1/(1+\text{TAE})$.
5. Taxa de atuação da espiã (TAtE). A probabilidade da espiã atacar é $1/(1+\text{TAtE})$.

A partir desses valores, o algoritmo gera uma sequência aleatória de bits (0 ou 1) que é enviada por Alice. A função usada para isso é a própia função "semi-aleatória"do Mathematica. Ela recebe esse nome porque, apesar da probabilidade do seu resultado ser 0 ou 1 ser sempre $1/2$, ela tem uma sequência determinada. Isso, porém, não afeta diretamente a simulação pois as diversas funções aleatórias usadas foram iniciadas em momentos distintos.

Após essa troca de bits pelo canal quântico, Bob se comunica publicamente com Alice para dizer em quais medidas ele obteve um resultado diferente de zero (que serão guardadas) e quais foram zero (descartadas). Perceba que Bob não revela o resultado da medida e apenas se ela foi nula ou não. Após essa comunicação , Alice e Bob possuem uma primeira chave, que a princípio é secreta.

Para dar continuidade ao protocolo, Alice e Bob devem realizar um tratamento adequado dos bits, visando a correção de erros experimentais e a minimização da informação obtida pela espi Eve.

Veja no Anexo **A** um exemplo de output da simulação .

Avaliação do Orientador

O estudante tem se mostrado bastante interessado no tema da criptografia quântica. No relatório apresentou de forma convincente os aspectos teóricos do protocolo de criptografia quântica conhecido como B92. Também descreveu adequadamente uma realização experimental do protocolo. Elaborou uma simulação visando a ilustração do funcionamento básico do protocolo. Em vista do desempenho do estudante em relação à execução do projeto, atribuo a nota 10 (dez) para o mesmo.

Prof. Antonio Vidiella Barranco

Referências

[1] C.H. Bennett and G. Brassard, Proceedings of the IEEE international conference on computers, systems and signal processing, Banglore, India, pp.175, (1984); uma versão eletrônica do artigo pode ser encontrada em: `http://quantum.bbn.com/dscgi/ds.py/get/file-18/BB84.pdf`

[2] C.H.Bennett, Phys. Rev. Lett. 68, 3121 (1992).

[3] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. 81, 3283 (1998).

[4] Exemplos de simulações encontradas na internet:
`http://www.columbia.edu/~mpj9/bb84.html`

[5] `http://monet.mercersburg.edu/henle/bb84/demo.php`

[6] `http://www.cki.au.dk/experiment/qrypto/doc/index.html`

Anexo A: Exemplo de Output

Os parâmetros escolhidos são: $n = 15$, opção de ataque da espiã ativada, $TAB = 3$, $TAE = 2$ e $TAtE = 2$. Os resultados marcados em vermelho indicam que ocorreu um erro durante a medida do bit. Perceba a alta taxa de bits errados, isso é um indício de que ocorreu ataque de espionagem.

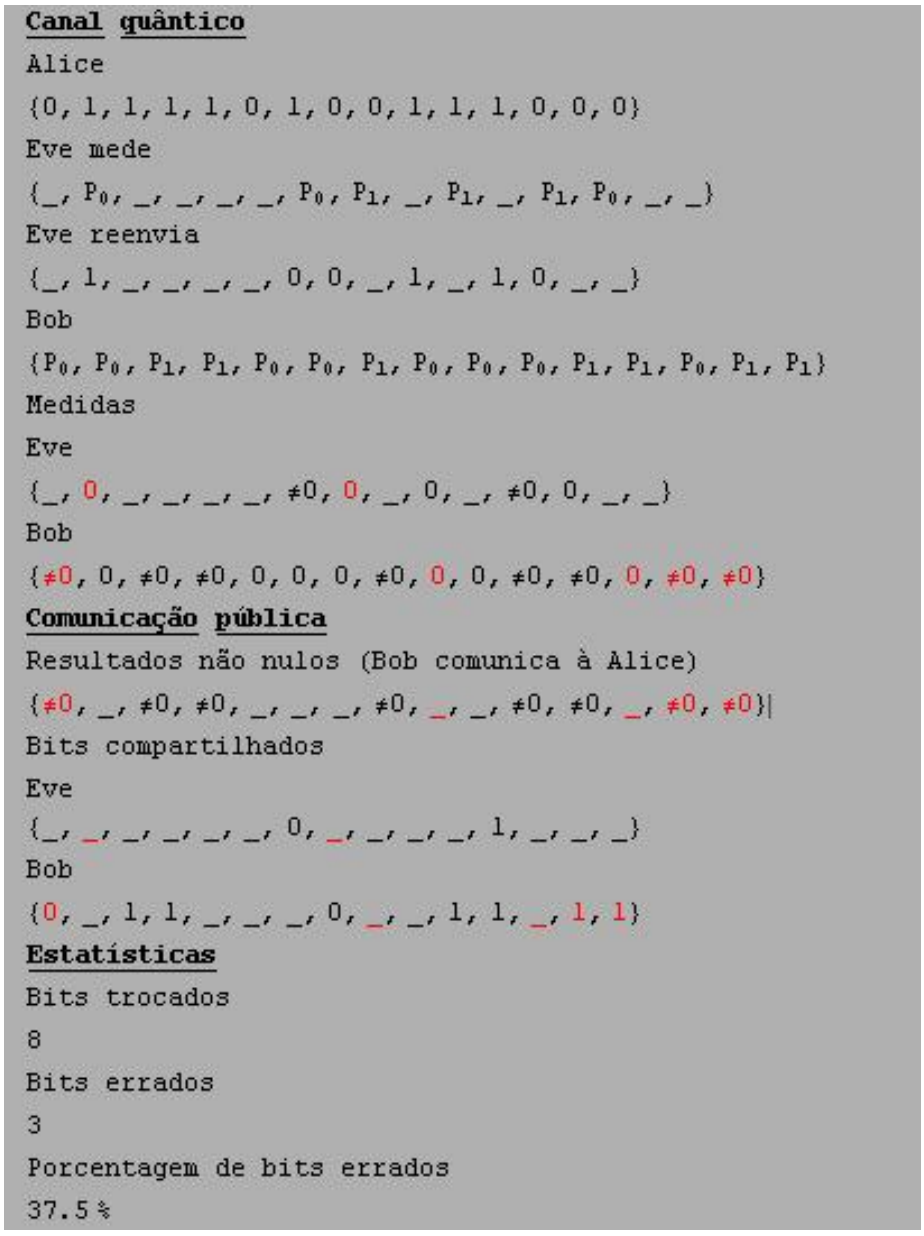

Figura 3: Exemplo de uma saída gerada pelo algoritmo.