Simulação do protocolo BB84 de criptografia quântica utilizando um feixe laser intenso

A.L.P. Camargo[1,3], L.O. Pereira[1], W.F. Balthazar[2] J.A.O. Huguenin[1,3*]
[1] *Instituto de Ciências Exatas, Universidade Federal Fluminense, 27213-145 Volta Redonda - RJ, Brazil*
[2] *Instituto Federal de Educação, Ciência e Tecnologia do Estado do Rio de Janeiro, Campus Volta Redonda, 27215-350 Volta Redonda - RJ, Brazil. and*
[3] *Programa de Pós Graduação em Física, Instituto de Física, Universidade Federal Fluminense, 24210-346 Niterói - RJ, Brazil.*

Neste trabalho apresentamos um experimento muito simples explorando polarização de um feixe laser intenso para simular a distribuição de uma chave criptográfica através do protocolo $BB84$ de criptografia quântica. Nossa proposta está baseada na analogia entre graus de liberdade de um feixe laser com estados quânticos da luz, muito discutida atualmente. A proposta utiliza duas bases de polarização linear, que é o ingrediente original do protocolo proposto por Bennet e Brassard. Dessa forma, o experimento permite um entendimento direto do princípio de funcionamento do protocolo. O experimento pode ser realizado em laboratórios didáticos dos cursos de graduação em Física e Engenharias bem como em espaços de divulgação científica. Além disso, os resultados mostram que o experimento apresenta um ambiente muito propício para discussão sobre a diferença entre propriedades clássicas e quânticas da luz.

We present a very simple experiment exploring the polarization of an intense laser beam in order to perform an emulation of a cryptographic key distribution by the well known BB84 protocol. Our work relies on the analogy between classical degrees of freedom of a laser beam and quantum states, very discussed nowadays. Our analogue of a key distribution is made by using two polarization basis, the original ingredient used by Bennet and Brassard, which allow us a direct understanding of the protocol. The experiment can be performed in didactic laboratories or can be demonstrated in a classroom. In addition, the results show a very proper ambient to discuss the difference between classical and quantum measurement of light.

I. INTRODUÇÃO

Em mundo cada vez mais digital é preciso confiar nos canais de transmissão de informação. A criptografia moderna é baseada na distribuição de chaves criptográficas (uma longa sequência de zeros e uns - 0 e 1). Para encriptar uma mensagem digital (também uma sequência de zeros e uns) que se deseja enviar em segredo, deve-se utilizar técnicas seguras de encriptação. Uma delas é a conhecida técnica "*One-Time pad*"[1], onde bits da mensagem são combinados com os bits da chave criptográfica em uma operação modular. Uma nova sequência binária será produzida com significado ininteligível para quem interceptar. Este procedimento é seguro desde que a chave seja randômica e secreta. O receptor da mensagem também deve possuir a chave criptográfica de modo a recuperar a mensagem original procedendo também uma operação modular. A mensagem encriptada pode ser enviada em um canal público não seguro desde que a chave seja partilhada apenas entre o rementente e o destinatário. Logo, o problema da comunicação segura é a distribuição de chaves criptográficas. Atualmente, a técnica mais utilizada é o protocolo RSA [2] que usa a distribuição pública de chaves, cuja segurança é baseada na dificuldade de fatoração de números muito grandes. No futuro, computadores quânticos, contudo, prometem uma velocidade de processamento muito superior a alcançada com computadores clássicos, colocando em risco a segurança do processo de criptografia atual.

De fato, a área de computação e informação quântica tem recebido muita atenção de pesquisadores no que diz respeito a avanços tecnológicos. Os resultados prometidos geram curiosidade e muita busca por informações sobre o tema entre estudantes e interessados no assunto. Por este motivo, vários trabalhos que buscam apresentar as ideias básicas da área para este público têm sido publicados [3–5]. Para além da difusão do conhecimento científico e tecnológico, o tema permite discutir fundamentos da física quântica a nível de graduação [6], enriquecendo o ensino desta importante área da Física.

Uma das aplicações mais conhecidas da teoria quântica é a criptografia quântica. Um protocolo alternativo, explorando propriedades quânticas em estados de polarização da luz, foi proposto em 1984 por Bennett e Brassard [7]. Trata-se do conhecido protocolo $BB84$ de distribuição de chaves criptográficas, descrito detalhadamente na seção II deste trabalho. A realização experimental desta proposta foi pela primeira vez realizada pelo La-

*Corresponding author. Email: huguenin@if.uff.br

boratório da IBM [8]. O protocolo também foi implementado com o envio de fótons em fibras sob o Lago de Genebra [9], além de ter sido implementado na região metropolitana de Boston[10]. Devido ao grande apelo tecnológico do protocolo $BB84$, surgiram trabalhos voltados à discussão didática do protocolo de modo a promover um claro entendimento dos procedimentos e princípios físicos envolvidos [11]. Experimentos simples foram também propostos de forma a mostrar a essência experimental do processo de distribuição de chaves pelo protocolo $BB84$. Usando posição transversa e variáveis de momento de um feixe laser por focalização, um experimento usando um circuito de ótica linear demonstrou os princípios básicos do protocolo[12]. Uma performance teatral muito divertida foi desenvolvida para ilustrar o funcionamento do protocolo $BB84$ usando bolas de chocolate embrulhadas em papel colorido e óculos de brinquedo com filtros de cor[13]. Nestes experimentos, diferentes sistemas foram utilizados para representar os estados de polarização de fótons e, através destas representações, a dinâmica do protocolo pôde ser discutida e compreendida.

No presente trabalho, estendemos a proposta de discutir informação quântica de forma básica para o campo experimental. Apresentamos um experimento muito simples que pode ser implementado em laboratórios didáticos dos cursos de graduação em Física e Engenharias, utilizando a polarização de um feixe laser intenso. Além disto, pode ser realizado em espaços de divulgação científica para estudantes do ensino médio e público em geral. O experimento oferece uma visão direta do funcionamento do protocolo pois as codificações dos bits que utilizamos são duas bases de polarização de um feixe laser, os ingredientes originais do protocolo de Bennet e Brassard. A grande diferença reside na fonte luminosa empregada (no protocolo original é utilizada uma fonte de fótons únicos) e no sistema de detecção (uso de fotodetectores de avalanche no protocolo original). Vale destacar que propriedades do campo eletromagnético clássico tem sido utilizadas para simular protocolos quânticos como jogos [14, 15], portas lógicas [16], além de violarem desigualdades análogas à do regime quântico como a desigualdade de Bell[17, 18]. As medidas em nosso experimento são feitas a partir da medida de intensidades de feixes intensos, que simulam os "clicks"relativos às medidas do protocolo original(fotocontagens). O experimento também permite uma discussão muito direta e intuitiva da diferença entre os regimes clássico e quântico da luz, uma vez que a troca do feixe laser intenso por uma fonte de fótons únicos e a troca dos detectores levam ao regime original de realização do protocolo. Acreditamos que o experimento é um cenário rico para a discussão sobre a descrição clássica e quântica da luz. Os resultados clássicos do experimento podem ser contrapostos aos resultados esperados pela Mecânica Quântica. Esta abordagem permitiu, ainda, simular experimentalmente um ataque de um espião e como o protocolo detecta sua presença.

O trabalho está esquematizado da seguinte forma: na seção II apresentamos uma descrição detalhada do protocolo $BB84$. A proposta experimental para simulação do protocolo e respectivo ataque de um espião é apresentada na seção III. Os resultados são apresentados e discutidos na seção IV. Por fim, as conclusões do trabalho são sumarizadas na seção V.

II. O PROTOCOLO BB84

O protocolo BB84 foi desenvolvido para distribuição segura de chaves cirpitográficas utilizando estados quânticos de polarização de fótons únicos. A seguir, faremos a apresentação da proposta original do protocolo e o efeito da ação de espionagem.

A. Proposta original

Uma visão esquemática do protocolo é apresentada na Fig.1. A informação começa a ser transmitida por Alice, que envia fótons polarizados para Bob, que irá medir a polarização dos fótons enviados. Eles devem escolher entre duas bases, cada uma composta de dois estados ortogonais de polarização — a base HV (polarização horizontal e vertical) e a base $+-$ (polarização a $\pm 45°$).

A base HV é definida em relação ao eixo de polarização horizontal. Dessa maneira, um fóton com polarização de $0°$ em relação à horizontal tem polarização H, e, analogamente, a polarização que faz um ângulo de $90°$ com relação à horizontal representa a polarização V. A base $+-$ é definida da seguinte forma: as polarizações $\pm 45°$, em relação à horizontal, representam, respectivamente, os estados $+$ e $-$.

A codificação dos bits é feita de maneira arbitrária. Neste trabalho usaremos a seguinte convenção: o bit 0 será a polarização H ou $+45°$ e o bit 1, a polarização V ou $-45°$. Como podemos observar, para definir a polarização de um bit precisamos primeiramente saber em qual base ele é preparado.

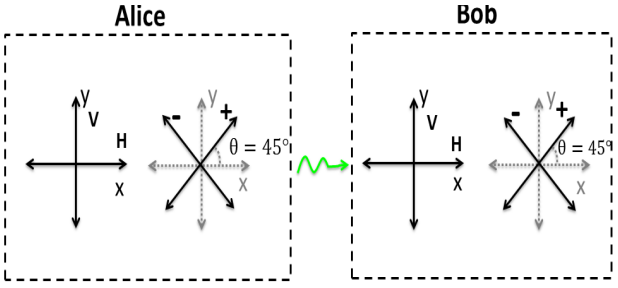

Figura 1: Visão esquemática do protocolo BB84. Alice pode escolher tanto a base HV quanto a $+-$. Para o primeiro caso, o bit 0 é representado pela polarização H e o bit 1 é representado pela polarização V; enquanto que para o segundo caso, 0 e representado por $+45°$ e 1 por $-45°$. Bob faz apenas uma escolha: em qual das duas bases irá medir o fóton.

Agora, iniciaremos a descrição do envio de bits. Primeiramente, Alice deve escolher uma base e um bit para enviar a Bob, enquanto Bob precisa escolher a base na qual irá medir o bit recebido. Estas "escolhas" são totalmente aleatórias. Após o envio de um grande número de bits, Alice divulga publicamente a sequência de bases sorteadas que ela usou para preparar os bits enviados. Com isso, Bob compara a sequência de bases usadas por ele e mantém apenas as bases coincidentes, descartando todos os bits provenientes de medidas em bases que não coincidiram com as bases que Alice usou no preparo. É importante notar que Alice publica apenas as bases da sequência enviada por ela, os bits equivalentes não são publicados. Para ver se a distribuição foi segura, após a filtragem das bases, eles comparam uma parte dos bits enviados e medidos e computam a porcentagem de acerto. É de se esperar, neste caso em que Bob mediu na mesma base que Alice enviou, que ele obtenha o mesmo bit. Porém, normalmente, parte dos bits podem ser rotacionados durante sua transmissão ou até mesmo medidos de forma incorreta por Bob devido a desalinhamentos entre as bases. Por conta dessas circunstâncias, há uma esperada taxa de erro na porcentagem de acerto dos bits, que depende da qualidade do canal. Se, após computar a porcentagem, o erro for maior do que o esperado, podemos concluir que provavelmente houve uma fonte externa de erro na transmissão — provavelmente devido a uma espionagem. Caso contrário, a comunicação está segura o suficiente e o resto dos bits poderão ser usados como chave criptográfica.

Alice		Bob	
Base A	bit A	Base B	bit B
$+-$	0	HV	0
+-	**0**	**+-**	**0**
HV	**1**	**HV**	**1**
HV	1	$+-$	0
+-	**1**	**+-**	**1**

Tabela I: Exemplo da chave criptográfica obtida. Após a aplicação do protocolo, apenas os bits provenientes de bases coincidentes são usados (em azul), os demais são descartados.Base A (B) representa a base escolhida por Alice (Bob) para preparação (medida) dos bits. O bit A (B)representa o bit enviado (medido) por Alice (Bob)

.

A Tabela I mostra um pequeno exemplo da distribuição de chaves. São mostrados as bases e os bits escolhidos por Alice, as bases escolhidas por Bob e os bits lidos por Bob. Os dados em azul são relativos aos bits aproveitados, os demais são descartados. Neste caso, após aplicarem o protocolo, Alice e Bob obtiveram a seguinte chave de bits: 011.

B. Interferência de um espião

No caso de comunicações seguras, os protocolos podem sofrer ataques de espiões. Para o protocolo $BB84$, foram propostos alguns possíveis ataques [19]. O ataque mais simples que pode ser feito é a interceptação e o re-envio de fótons para Bob pelo espião. Vamos discutir o caso mais simples onde podemos ver como a mecânica quântica fornece segurança. Para o caso de Eva (a espiã, do Inglês *eavesdrop*) espionar a comunição entre Alice e Bob, primeiramente ela precisa absorver o bit enviado por Alice e medi–lo da mesma maneira que Bob faria. A fim de não causar suspeitas em Bob, Eva precisa de um novo bit para ser enviado a ele como se fosse vindo de Alice. Como o teorema da não – clonagem da Mecânica Quântica [20] não permite que seja feita uma cópia perfeita de estados quânticos, Eva pode enviar somente estados preparados aleatoriamente, do mesmo jeito que Alice faz , ou, na melhor das hipóteses para Eva, fazer uma cópia imperfeita do bit de Alice [21]. De qualquer forma, o bit re-enviado por Eva não terá correlação perfeita com o bit enviado por Alice. Quando Bob for computar a porcentagem de acertos após a aplicação do protocolo, haverá erros nos bits obtidos com as bases coincidentes. O erro ocorre em dois casos: quando Alice e Eva escolhem a mesma base, porém diferentes bits — com certeza este caso gera erro, uma vez que Bob simplesmente irá ler o bit oposto, ou ainda, quando elas escolhem bases diferentes. Neste caso, Bob vai medir o bit certo com 50% de probabilidade, para o caso em que Eva enviou bits preparados aleatoriamente. Para o caso de clonagem imperfeita o erro será menor. Em ambos os casos, contudo, ocorre o surgimento de uma da taxa de erro pois já estamos assumindo aqui que as bases de Alice e Bob são as mesmas, uma vez que já aplicamos o protocolo. Para o caso ideal (fonte de fótons únicos e deteção perfeita dos fótons) essa taxa de erro aponta que houve uma espionagem. Na Tabela II, podemos ver a mesma situação representada na Tabela I, entretanto, agora com os erros provocados pela presença de Eva, para o caso em que ela prepara o re-envio aleatoriamente. Diferentemente de antes, após aplicarmos o protocolo, as bases coincidentes de Alice e Bob nem sempre terão os bits coincidentes. Em azul temos os bits coincidentes e em vermelho os bits de bases coincidentes que não estão de acordo com o esperado. Dessa maneira, esta chave não pode ser usada e uma nova deverá ser providenciada.

Existem outros tipos de ataque que oferecem mais risco ao protocolo, sobretudo quando o regime ideal de realização não pode ser alcançado, por exemplo, pela dificuldade de produzir-se fótons únicos. Em geral, se produz pulsos com um número N grande de fótons e Eva poderia pegar uma pequena porção destes fótons se ela tiver acesso a um sistema de detecção de alta eficiência. Este ataque é conhecido como divisor de número de fótons, explicado com detalhes na Ref.[22]. Podemos citar outras estratégias de ataques como a que explora a imperfeição do sistema de detecção de Bob [23] e a estratégia conhe-

cida como "Cavalo de Tróia"ou ataque por injeção de luz [24]. Não entraremos em detalhes destas estratégias de ataque por estarem além do escopo do presente trabalho.

Base A	bit A	Base E	bit E	Base B	bit B
$+-$	0	HV	0	HV	0
$+-$	0	$+-$	1	$+-$	1
HV	1	HV	1	HV	1
HV	1	HV	1	$+-$	0
$+-$	1	$+-$	0	$+-$	0

Tabela II: Exemplo da influência de um espião na distribuição de chaves criptográficas. Após a aplicação do protocolo, nem todos os bits coincidiram. Em vermelho, os bits provenientes de bases coincidentes que apresentam erro. A, E e B representam Alice, Eva e Bob, respectivamente. No caso de Eva, mostramos as bases e bits enviados a Bob.

III. EXPERIMENTO

Nossa proposta é realizar uma simulação do Protocolo BB84 usando um feixe laser polarizado clássico, ou seja, em regime de feixe intenso. As bases escolhidas e a codificação dos bits são exatamente as mesmas da proposta original:polarização. Utilizamos a base HV (polarização H correspondendo ao bit 0 e polarização V correspondendo ao bit 1) e a base $+-$ ($+45° \rightarrow bit\ 0$ e $-45° \rightarrow bit\ 1$). As bases são definidas a partir do ângulo de rotação de placas de meia onda (PMO), como veremos a seguir. Vale notar que a única diferença entre o experimento deste trabalho e o protocolo originalé o regime de intensidade da luz. No protocolo original é exigido regime de produção e contagem de fótons únicos, enquanto nossa proposta didática utiliza feixes intensos e mede fotocorrentes.

A. Montagem experimental livre de espião

A primeira parte do experimento simula a troca de uma chave criptográfica entre Alice e Bob sem a interferência da espiã, ou seja, Eva não participa desta etapa do experimento (Seção II A). O esquema experimental está esboçado na Fig. 2. Um feixe laser horizontalmente polarizado passa através da primeira placa de meia onda, denominada PMO_{θ_A}, que é usada por Alice com o objetivo de escolher suas bases de preparação e os bits que serão enviados a Bob. É importante notar que Alice ajusta sua base e seu bit apenas fazendo uma rotação θ_A do eixo rápido da PMO em relação à horizontal (direção da polarização incidente). Para a base HV, ela usa $\theta_A = 0°$ para enviar o feixe na polarização H (bit 0) e $\theta_A = 45°$ para enviar o feixe na polarização V (bit 1). Para a base $+-$, ela usa $\theta_A = 22.5°$ para enviar o feixe na polarização $+45°$ (bit 0) e $\theta_A = -22.5°$ para polarização $-45°$ (bit 1).

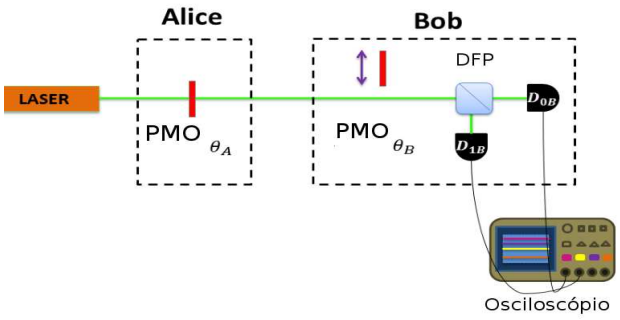

Figura 2: Esquema experimental da primeira parte do experimento. Alice pode escolher suas bases e bits a serem enviados usando uma única placa de meia onda PMO_{θ_A}. As medidas de Bob são feitas usando a meia onda PMO_{θ_B} e um DFP (Divisor de Feixe Polarizado). As saídas "0" e "1" são captadas pelos detectores D_{0B} e D_{1B} e registrados pelo osciloscópio digital.

Como Bob apenas realiza as medidas dos bits, ele precisa escolher apenas em qual base serão feitas essas medidas. Para isso, ele utiliza um Divisor de Feixes Polarizado (DFP) que transmite a polarização H e reflete a polarização V. Dois detectores são utilizados (um em cada saída do DFP) monitorando simultaneamente através de um osciloscópio digital a intensidade obtida em cada uma delas. NA ausência de osciloscópios podemos utilizar multímetros para leitura das fotocorrentes.

Portanto, Bob mede na base HV utilizando o DFP e detectores em cada saída. Se Alice manda o bit 0 na base HV (polarização H), apenas a componente transmitida pelo DFP terá uma parcela significativa de intensidade no detector D_{0B}. Para o bit 1 (polarização V), apenas a componente refletida será medida pelo detector D_{1B}. No caso onde Alice manda seus bits na base $+-$ (polarização $\pm 45°$) o DFP irá projetar estas polarizações na base HV, de forma que os dois detectores irão registrar intensidades próximas (balanceadas). Com isso, para este experimento, podemos concluir que quando as intensidades estão registrando valores próximos em ambos detectores, significa que Bob escolheu uma base diferente de Alice. Pode-se usar alguma estratégia para leitura desta medida, como por exemplo, ler o bit correspondente a maior intensidade, mesmo que seja apenas um pouco maior. Não nos preocuparemos com estes resultados, uma vez que estes casos serão descartados.

Para que Bob meça na base $+-$, ele precisa mapear os estados da base $+-$ em estados da base HV e medir com o DFP. Isto é feito inserindo-se uma placa de meia onda, PMO_{θ_B}, com o ângulo $\theta_B = 22.5°$ em relação à horizontal imediatamente antes do DFP. Se Alice mandar o bit 0 na base $+-$ (polarização $+45°$), o feixe laser passa pela $PMO_{\theta_B=22,5°}$ e sua polarização é rodada

para a polarização H. Com isso, o único detector a captar o laser será o D_{0B}. Para o bit 1 (polarização $-45°$), a $PMO_{\theta_B=22,5°}$ rotaciona esta polarização levando-a à polarização V. Com isso, apenas o feixe refletido pelo DFP será medido, pelo detector D_{1B}. Ou seja, para medir na base $+-$, é suficiente introduzir uma meia onda $HWP_{\theta_B=22,5°}$ imediatamente antes do DFP. Note que quando Alice manda um bit na base HV, a HWP_{θ_B} transforma a polarização em $\pm 45°$ e os dois detectores apresentarão intensidades balanceadas, mostrando uma escolha errada de base. Novamente a leitura de um bit poder ser feita tomando-se o que apresentar uma intensidade ligeiramente maior.

Com esta configuração é possível simular o protocolo BB84. Primeiramente, é escolhido um número N de bits que serão enviados. Usando um gerador de números aleatórios gerados numericamente em um computador, são produzidas três sequências de $N = 100$ números inteiros, que são classificados como pares ou ímpares. A primeira sequência é usada para simular a escolha de base de Alice, onde os números pares correspondem a base HV e os números ímpares correspondem a base $+-$. A segunda sequência é usada para a escolha do bit enviado por Alice, e números pares correspondem ao bit 0 e números ímpares ao bit 1. Finalmente, a terceira sequência representa a escolha de base a qual o Bob usará para medir o bit — que segue a mesma correspondência feita para Alice. Após o término do envio, Alice e Bob comparam suas bases e mantém apenas os bits cujas bases coincidiram. A chave será composta pelos bits enviados (lidos) por Alice (Bob) nas bases coincidentes.

B. Montagem experimental em presença de um espião

A segunda parte do experimento, mostrado na Fig.3, representa a distribuição de uma chave criptográfica entre Alice e Bob com a presença da espiã, ou seja, Eva irá interferir na comunicação (Seção II B). Alice usa o seu feixe laser para enviar os bits usando o procedimento apresentado na Seção III A. Porém, em vez do feixe polarizado ir diretamente a Bob, Eva desvia o feixe para que possa medí-lo. Eva faz esta medida da mesma maneira que Bob mede um bit: usando um DFP e, alternadamente, uma $PMO_{\theta_{E_I}}$, de acordo com a base escolhida para medir. Como Eva absorve o bit enviado por Alice, ela precisa de uma fonte extra de bits para mandar para Bob. Vamos utilizar a estratégia mais simples, em que Eva prepara aleatoriamente os bits a serem enviados, a partir de um novo feixe laser e uma segunda placa de meia onda $PMO_{\theta_{E_{II}}}$. Eva mede o bit enviado por Alice com os detectores D_{0E} e D_{1E}. Finalmente, Bob mede o feixe que ele recebe, i.e., o feixe enviado por Eva. Desta vez, como há duas medidas sendo feitas, o osciloscópio de quatro canais (podem ser utilizados multímetros) apresenta dois pares de resultados: o bit medido por Eva (enviado por Alice) e o bit medido por Bob (enviado por Eva).

Para esta etapa são produzidas três novas sequências de números inteiros aleatórios que representam: a escolha da base de medida de Eva, sua base de preparo de bit e sua escolha de bit. Após o término do envio de bits, Alice e Bob comparam suas bases e mantém os bits oriundos das medidas com a base coincidente. Para verificarem a confiabilidade do canal, usam parte da chave para investigar se houve alguma perturbação.

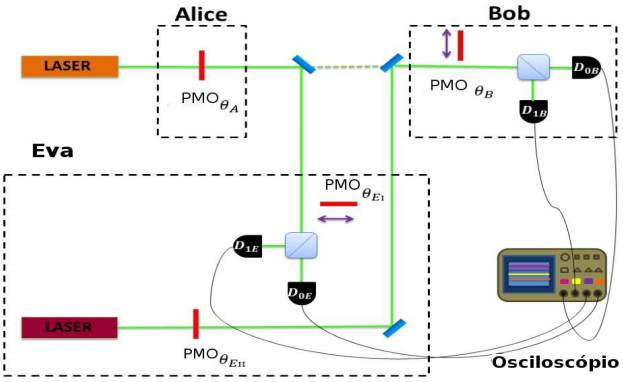

Figura 3: Esboço experimental da segunda parte do experimento. Alice e Eva escolhem suas bases e bits usando apenas uma única placa de meia onda cada uma: (PMO_{θ_A} e $PMO_{\theta_E II}$). As medidas são feitas por Eva e Bob, usando respectivamente $PMO_{\theta_E I}$ junto com um DFP e PMO_{θ_B} junto com outro DFP. Os bits 0's são detectados pelos detectores D_{0B} e D_{0E} e os 1's são detectados por D_{1B} e D_{1E}, todos registrados pelo osciloscópio digital.

IV. RESULTADOS E DISCUSSÕES

Nesta seção apresentaremos os resultados da realização de cada experimento. Mostraremos casos particulares que ilustram o funcionamento do protocolo e a consolidação dos resultados experimentais.

A. Resultados para o protocolo sem a presença de espião

Vamos discutir os resultados da primeira parte do experimento, na ausência da espiã (Fig.2). Para começar, quatro casos serão apresentados. O primeiro caso é quando Alice sorteia números pares para a base e para o bit, ou seja, base HV — bit 0 (polarização H). Na sequência, Bob também sorteia um número par, ou seja, ele mede na base HV (apenas o DFP será usado na medição). O resultado obtido pelo osciloscópio para esta situação está sendo mostrado na Fig.4(a).

Neste caso, a polarização H é transmitida pelo DFP e o detector D_{0B} capta a intensidade mostrada no Canal 1 do osciloscópio ($CH1$ - traço amarelo). O detector D_{1B}, mostrado no Canal 2 ($CH2$ - traço azul), apresenta intensidade muito perto de zero, uma vez que a polarização

do feixe detectado é horizontal. Esse é o caso onde Alice e Bob coincidem suas bases. Um segundo caso possível é quando Bob, diferentemente do primeiro caso, sorteia um número ímpar para medir seu bit, ou seja, ele mede na base $+-$. Agora, ele usa a $PMO_{\theta_B=22.5^\circ}$ antes do DFP para realizar a medida. O resultado dessa medida, mostrado na Fig.4(b), apresenta uma intensidade distrubuída entre os dois detectores D_{0B} e D_{1B}, uma vez que a meia onda rotacionou a polarização do laser para $+45^\circ$. Para operar a leitura de um bit nesta medida, podemos considerar como sendo bit 1, uma vez que o Canal 2 (traço azul) é ligeiramente superior.

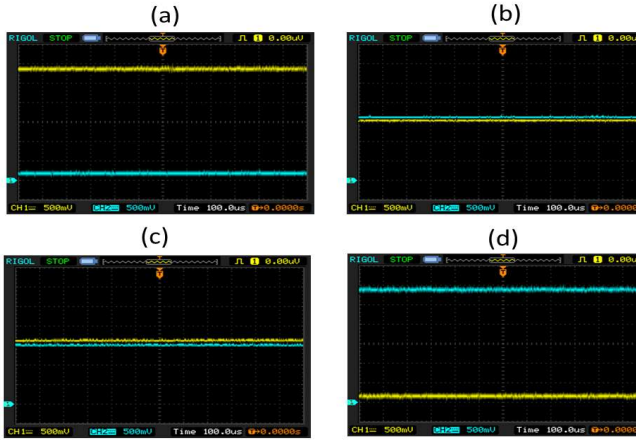

Figura 4: Resultados obtidos pelo osciloscópio de acordo com a configuração da Fig.2 para os seguintes casos: imagem (a) quando Alice envia bit 0 na base HV e Bob mede na base HV; imagem (b) Alice manda o bit 0 na base HV mas Bob mede na base $+-$; imagem (c) Alice manda o bit 1 na base $+-$ e Bob mede na base HV; imagem (d) Alice manda o bit 1 na base $+-$ e Bob mede na base $+-$.

O terceiro caso é quando Alice sorteia dois números ímpares, ou seja, ela manda o bit 1 na base $+-$ (ajustando a meia onda em $\theta_A = +22.5^\circ$) e Bob sorteia um número par, medindo na base HV. A Fig.4(c) mostra o resultado obtido nessa circunstância que, assim como o anterior, resulta em intensidades balanceadas nos detectores. Neste caso, como o Canal 1 apresenta intensidade um pouco maior, podemos realizar a leitura do bit 0. Finalmente, o quarto caso acontece quando tanto Alice quanto Bob sorteiam números ímpares. Ou seja, Alice manda o bit 1 na base $+-$ e Bob mede na base $+-$. O feixe laser com polarização -45° passa através da $HWP_{\theta_B=+22.5^\circ}$ e sua polarização é convertida para a polarização V. Com isso, o feixe é refletido pelo DFP e o detector D_{1B} capta a intensidade ($CH2$ - traço azul) enquanto Canal 1 permanece praticamente sem intensidade, como mostra a Fig.4(d).

Como pode ser observado, quando Alice e Bob coincidem suas bases, apenas um detector (o associado ao bit enviado por Alice) apresenta uma intensidade significativa. Em contrapartida, quando eles diferem em suas escolhas de base, ambos detectores apresentam intensidades, aproximadamente equivalentes.

Alice		Bob	
B_{ENV}	b_{ENV}	B_{MED}	b_{MED}
HV	0	$+-$	1
HV	1	$+-$	0
$+-$	0	$+-$	0
$+-$	1	$+-$	1
HV	0	$+-$	1
$+-$	1	$+-$	1
HV	0	HV	1
HV	1	$+-$	0
$+-$	1	$+-$	1
$+-$	0	$+-$	0

Tabela III: Amostra de 10 dos 100 bits enviados, de acordo com a configuração da Fig.2, sem a participação de Eva. B e b representam Base e bit medidos (MED) e enviados (ENV), respectivamente

A Tabela III apresenta uma amostragem de 10 repetições das 100 realizadas no experimento. É importante notar que na ausência de Eva todas as vezes em que Alice e Bob usam a mesma base, Bob necessariamente acerta o bit.

B. Resultados do experimento com a presença de espião

Passamos agora a discutir os resultados relativos à segunda parte do experimento, quando Eva começa a espionagem, de acordo com a configuração da Fig.3. O mesmo procedimento apresentado na Seção IV-A é repetido. Porém, agora são gerados seis números aleatórios para cada bit trocado correspondendo a: base de Alice, bit de Alice, base de medida de Eva, base de envio de Eva, bit de envio de Eva e base de medida de Bob. Também foi usada a mesma quantidade de bits $N = 100$. Apenas os números referentes às escolhas de Eva foram gerados nesta etapa de forma que os números relativos às escolhas de Alice e Bob foram mantidos iguais ao caso da seção IV A, para que, dessa maneira, a única diferença nesta segunda parte do experimento fosse realmente a intromissão de Eva. Assim, temos Alice mandando os mesmos bits e Bob usando as mesmas bases para fazer as medidas. Entretanto, como Eva interfere no sistema, será possível ver que o resultado não é preservado. Quando aplicado o protocolo, como visto anteriormente, são mantidos apenas os bits cujas bases coincidiram. Em vista disso, será discutido neste momento apenas estes dois casos. Na Fig 5, cada coluna representa um dos casos em questão. No primeiro caso, Alice sorteia dois números pares (bit 0 - polarização H), Eva também sorteia dois números pares para enviar seu bit (bit 0 - polarização H), e Bob sorteia um número par para realizar a medida (medida na

base HV). A imagem E-a) da Fig.5 apresenta o resultado obtido por Eva neste processo (bit 0 - polarização H). É interessante notar que esta situação é análoga a situação da Fig.4(a), porém agora em vez de Bob, Eva é quem esta detectando o bit. Dessa maneira, os resultados nos detectores são: D_{0E} mede uma alta intensidade mostrada no Canal 1 ($CH1$ - traço amarelo) e D_{1E} quase não detecta intensidade muito baixa mostrada no Canal 2 ($CH2$ - traço azul).

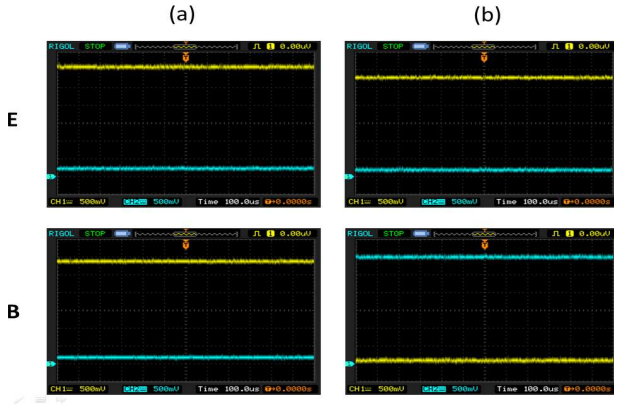

Figura 5: Resultados obtidos pelo osciloscópio de acordo com a configuração da Fig.3 para os seguintes casos: imagem E(a) Alice envia o bit 0 na base HV e Eva mede na base HV; imagem B(a) Eva manda o bit 0 na base HV e Bob mede na base HV; imagem E(b) Alice manda o bit 0 na base HV e Eva mede na base HV; imagem B(b) Eva manda o bit 1 na base HV e Bob mede na base HV.

Com isso, concluímos que Alice e Eva coincidiram suas bases. A imagem B-a) da Fig. 5 apresenta o resultado obtido por Bob (bit 0 - polarização H). Pode-se observar que este resultado é análogo ao anterior, ou seja, Eva e Bob coincidiram suas bases assim como Alice e Eva. Para concluir este primeiro caso, observa-se que apesar da presença de Eva, Bob acertou o bit enviado por Eva; porém, vale ressaltar que foi devido a coincidência do bit enviado por Eva ser idêntico ao enviado por Alice com a mesma base. Nem sempre acontecerá desta maneira como será visto a seguir.

No segundo caso Alice sorteia de novo dois números pares (bit 0 - polarização H), Eva sorteia, respectivamente, um número par e um ímpar para enviar seu bit (bit 1 - polarização V), e Bob escolhe um número par (medida na base HV). A imagem E-b) da Fig.5 apresenta o resultado obtido por Eva (bit 0 - polarização H), que é precisamente o mesmo resultado obtido por Eva anteriormente. Com isso conclui-se que Alice e Eva coincidiram suas bases novamente e consequentemente obtiveram o mesmo bit. A imagem B-b) mostra o resultado obtido por Bob (bit 1 - polarização V). A polarização V vinda de Eva é refletida pelo DFP e o detector D_{1B} capta quase toda a intensidade, mostrada no canal 2 do osciloscópio ($CH2$ - traço azul). O outro detector, D_{0B} ($CH1$ - traço amarelo), capta intensidade muito baixa, uma vez que a polarização do laser está totalmente vertical. Nesta circusntância, Alice e Bob coincidiram suas bases; entretanto, Bob não acertou o bit enviado por Alice. Isto aconteceu devido a influência de Eva, uma vez que ela espionou a comunicação e mandou para Bob um novo bit totalmente aleatório que desta vez não coincidiu como bit enviado por Alice. Por esta razão, o protocolo estabelece que Alice e Bob comparem uma pequena parte da chave criptográfica. Se houve espionagem, eles irão observar um erro de bits muito alto para as bases coincidentes. A tabela IV apresenta uma amostra de 10 das 100 sequências feitas no laboratório, que tem como única diferença para o caso anterior o acréscimo das ações de Eva. Diferentemente da situação anterior, quando Alice e Bob coincidirem suas bases, não necessariamente Bob obterá o mesmo bit enviado por Alice.

Alice		Eva			Bob
B_{ENV}	b_{ENV}	B_{MED}	B_{ENV}	b_{ENV}	B_{MED}
HV	0	+−	0	+−	0
HV	1	HV	1	+−	1
+−	0	HV	0	+−	0
+−	1	+−	0	+−	0
HV	0	+−	1	+−	1
+−	1	+−	0	+−	0
HV	0	+−	1	HV	1
HV	1	+−	0	+−	0
+−	1	HV	1	+−	1
+−	0	+−	1	+−	1

Tabela IV: Amostra de 10 dos 100 bits enviados de acordo com a configuração da Fig. 3, onde há a participação de Eva. B e b representam Base e bit medidos (MED) e enviados (ENV), respectivamente

Após as realizações experimentais em ambas configurações, com e sem Eva, uma sumarização dos resultados é apresentada na Tabela V. Para a realidade deste trabalho, que é apenas uma simulação da distribuição de chaves, a taxa de erro é devido apenas a presença da espiã. Para concluir, nota-se que quando Eva não interfere na comunição, após aplicar o protocolo, Alice e Bob vão necessariamente acertar seus bits. Entretanto, quando Eva de fato interfere, eles vão coincidir seus bits aproximadamente metade das vezes, que é precisamente a mesma chance de Eva mandar, por acaso, o mesmo bit enviado por Alice.

	BC	bC	% Acertos
Sem Eva	49	49	100.00′%
Com Eva	49	22	44.90′%

Tabela V: Resultados obtidos após a repetição de $N = 100$ bits enviados em ambas configurações: com e sem Eva. BC corresponde a bases coincidentes e bC, bits coincidences.

V. CLÁSSICO × QUÂNTICO

Como podemos ver, o experimento realizado simula o resultado da distribuição de chaves criptográficas pelo protocolo $BB84$ de criptografia quântica. Qual a diferença deste experimento para a implementação do protocolo? Basicamente, a fonte de luz envolvida e o sistema de detecção. Note que o protocolo descrito na Seção II trabalha com a codificação dos bits na polarização de fótons individuais, e a segurança repousa no Teorema de Não Clonagem[20]. Eva não consegue clonar o bit enviado por Alice para que ela possa mandar uma cópia perfeita para Bob. Se isto fosse possível o protocolo não seria seguro.

A presente proposta usa exatamente as mesmas bases e interpretações do protocolo original mas não pode ser usado para distribuição de chaves por questão de seguraça. Sendo os bits enviados em um feixe intenso, Eva poderia desviar uma pequena fração do feixe, alguns poucos fótons se ela tem os recursos. Ao retirar esta pequena fração Bob não seria capaz de distinguir a pequena diferença na intensidade, e não seria capaz de perceber a espionagem.

Vale destacar que a versão quântica de nosso experimento pode ser discutida de forma muito direta e traz a vantagem de gerar oportunidade para observarmos a diferença de comportamento nos regimes clássicos e quânticos, sendo uma ferramenta interessante para introdução de conceitos chave da teoria quântica. Para chegarmos à versão quântica deste proposta, temos que primeiramente, trocar a fonte luminosa intensa (laser) por uma fonte de fótons únicos. Os detectores (D_{0B} e D_{1B}) utilizados no experimento devem ser trocados por dois contadores de fótons (CF_{0B} e CF_{1B}). Toda preparação de bases e estados, bem como a ótica utilizada para as medidas e leituras dos bits são idênticas às utilizados no caso de feixe intenso.

Para o caso quântico sempre teremos um "*click*" em um dos contadores de fótons. Para o caso em que as bases de Alice e Bob coincidem, apenas o CF relativo ao bit enviado irá ser acionado. No caso em que Alice e Bob não tiverem suas bases coincidindo, ao invés das intensidades balanceadas observadas no caso clássico, continuaremos observando um único CF ser acionado, já que não podemos dividir um fóton. Por exemplo, se Alice enviar o fóton com polarização + (base $+-$, bit 0) e Bob medir na base HV, teremos uma probabilidade de 50% do fóton ser transmitido no DFP e detectado por CF_{0B}, e 50% de probabilidade de ser refletido pelo DFP e ser detectado pelo CF_{1B}. Eis a fonte de erro intrínsica do protocolo e o motivo pelo qual os bits medidos em bases não coincidentes são descartados da chave. Se repetirmos a medida do exemplo acima enviando muitos fótons, metade deles será transmitida e metade refletida. Nosso experimento está inteiramente de acordo com esta previsão já que apresenta intensidades balanceadas no caso de bases não coincidentes. Se tomarmos a intensidades I_{jB} de cada detector D_{jB} ($j = 0, 1$) e a intensidade total I_T (soma das intensidades), a razão I_{jB}/I_T correspodenrá a probabilidade de um fóton ser detectado no detetor D_{jB}. De fato, para experimentos de óptica linear, o resultado da média para N repetições do experimento quântico coincide com o resultado de uma realização do experimento clássico onde temos um número extremamente grande de fótons em um feixe de poucos miliwatts.

Para o experimento na presença de um espião, o regime quântico é alcançado fazendo com que Eva também tenha acesso à fontes de fótons únicos e contadores de fótons para sua detecção.

VI. CONCLUSÕES

Neste trabalho propomos e realizamos experimentalmente um experimento simples para demonstrar os princípios de funcionamento do protocolo $BB84$ de criptografia quântica em que foi explorado o mesmo instrumental para implementação do protocolo original, ou seja, duas bases de polarização da luz. Porém, utilizamos uma fonte de laser intensa, no regime clássico. Nossos resultados mostram claramente todas as nuances do protocolo, inclusive a ação de um espião, o que não foi até hoje explorado nas implementações ilustrativas do protocolo. Uma discussão sobre as propriedades quânticas do protocolo podem ser feita a partir de nossos resultados, que são uma ferramenta interessante para discutir as diferenças entre os regimes clássico e quântico. Uma versão quântica do nosso experimento pode ser obtida diretamente pela substituição da fonte luminosa e dos detectores, levando o aparato à versão original do protocolo $BB84$.

Acknowledgement

CNPq, FAPERJ, INCT- Informação Quântica

[1] F. Rubina,"One-Time Pad cryptography," Cryptologia, **20**, 359–364, (1996).

[2] R.L. Rivest, A. Shamir, and L. Adleman,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. of Tech ACM, **21**, 120:126, (1978).

[3] José Roberto Castilho Piqueira, "Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e teletransporte, Rev. Bras. Ensino de Fís., v. 33, n. 4, 4303 (2011).

[4] José, Marcelo Archanjo, Piqueira, Jos'e Roberto Castilho and Lopes, Roseli de Deus, " Introdução à programação quântica, Rev. Bras. Ensino Fís., vol.35, no.1, p.1-9 (2003).

[5] Cabral, Gustavo Eulalio M., Lima, Aércio Ferreira de

and Lula Jr., Bernardo, "Interpretando o algoritmo de Deutsch no interferômetro de Mach-Zehnder", Rev. Bras. Ensino Fís., v.26, no.2, p.109-116, (2004).

[6] Davidovich, Luiz,"Os quanta de luz e a ótica quântica, Rev. Bras. Ensino Fís., vol.37, no.4, p.4205-1-4205-12, (2015)

[7] C. H. Bennett and G. Brassard,"Quantum cryptography: Public key distribution and coin tossing," Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore,India IEEE Computer Society Press, 175–179, (1984).

[8] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin,"Experimental quantum cryptography," J. Cryptology 5, 3–28 (1992).

[9] Grégoire Ribordy, Jean-Daniel Gautier, Nicolas Gisin, Olivier Guinnard, Hugo Zbinden, Electronics Letters, **34**, (22), 2116 - 2117 (1998).

[10] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh,"Current status of the DARPA quantum network," quant-ph/0503058, (2005).

[11] Gustavo Rigolin e Andrés Anibal Rieznik, Revista Brasileira de Ensino de Física, v. 27, n. 4, p. 517 - 526, (2005).

[12] D. S. Lemelle, M. P. Almeida, P. H. Souto Ribeiro, and S. P. Walborn,"A simple optical demonstration of quantum cryptography using transverse position and momentum variables," Am. J. Phys. **74** ,542-547 (2006).

[13] Karl Svozil,"Staging quantum cryptography with chocolate balls," Am. J. Phys. **74**, 800-803, (2006).

[14] A. R. C. Pinheiro, C. E. R. Souza, D. P. Caetano, J. A. O. Huguenin, A. G. M. Schmidt, and A. Z. Khoury, "Vector vortex implementation of a quantum game,"J. Opt. Soc. Am. B **30**, 3210 (2013).

[15] W. F. Balthazar, M. H. M. Passos, A. G. M. Schmidt, D. P. Caetano,and J. A. O. Huguenin, "Experimental realization of the quantum duel game using linear optical circuits,"J. Phys. B 48, 165505 (2015).

[16] W. F. Balthazar, D. P. Caetano, C. E. R. Souza, and J. A. O. Huguenin, "Using Polarization to Control the Phase of Spatial Modes for Application in Quantum Information",Brazilian Journal of Physics 44, 658 (2014).

[17] C. V. S. Borges, M. Hor-Meyll, J. A. O. Huguenin, and A. Z. Khoury,"Bell-like inequality for the spin-orbit separability of a laser beam," Phys. Rev. A **82**, 033833 (2010).

[18] K. H. Kagalwala, G. D. Giuseppe, A. F. Abouraddy, and B. E. A. Saleh,"Bell's measure in optivcal classical coherence," Nat. Photonics **7**, 72 (2012).

[19] R. Aggarwal, H. Sharma, and D. Gupta, "Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol," International Journal of Computer Applications **20**, 28-31 (2011).

[20] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* Cambridge University Press, (2000).

[21] V. Scarani, S. Iblisdir, N. Gisin, and Antonio Acìn, "Quantum cloning," REVIEWS OF MODERN PHYSICS, **77**, 1225-1256 (2005).

[22] N. Lu tkenhaus, "Security against eavesdropping attacks in quantum cryptography," Phys. Rev. A 54(1), 97- 111 (1996).

[23] V. Makarov and D.R. Hjelme, "Faked states attack on quantum cryptosystems," Journal of Modern Optics, **52**, 691-705 (2005).

[24] A. Vakahitov, V. Makarov and D.R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," Journal of Modern Optics, **48**, 2023-2038 (2001).