SISTEMAS DE CRIPTOGRAFIA QUÂNTICA: RECEPTORES E ESTRATÉGIAS DE ESPIONAGEM

Rubens Viana Ramos[1] , *Rui Fragassi Souza*[2]

[1]Department of Electronics, Royal Institute of Technology (KTH), Electrum 229, 164 40 Kista, Sweden
[2]Departmento de Microonda e Óptica, Faculdade de Engenharia Elétrica e de Computação, UNICAMP, 13083-970 Campinas-SP, Brasil

RESUMO

Iniciamos com uma revisão do protocolo quanto-criptográfico BB84. Em seguida, trabalhamos o desenvolvimento de receptores de luz de fótons isolados, um dos principais limitantes em sistemas de QKD (*quantum key distribution*), versando sobre o APD e circuitos que o comportem. Finalizamos com a análise de duas estratégias de espionagem (*eavesdropping strategies*) no canal óptico entre Alice e Bob: Intercepta/Re-envia e Ataque por Divisor de Feixe.

1. INTRODUÇÃO

Para a segurança das transmissões de dados, técnicas de criptografia devem ser empregadas. O transmissor, responsável pela encripção, deve gerar uma palavra (conjunto de bits) secreta, conhecida como chave. Esta, através de um algoritmo de encripção, é usada para embaralhar o texto a ser enviado. Para a recuperação da mensagem original, no receptor, faz-se necessária a utilização da mesma chave, sendo a mensagem praticamente inviolável para quem não possuí-la. Portanto, uma vez que a chave tenha sido escolhida no transmissor, ela deve ser transmitida ao receptor. Nesta etapa, se um terceiro usuário, não autorizado, tiver acesso ao canal de transmissão, ele poderá obter a chave e decodificar os dados que obtiver posteriormente. Visando impossibilitar usuários não autorizados de obterem a chave durante a transmissão da mesma, foram desenvolvidos protocolos de distribuição de chave usando dados quânticos (*quantum key distribution*, QKD) [1-2]. Quando estes dados são violados pode-se medir uma alta taxa de erros de bits na recepção, indicando a presença de um intruso no canal de comunicação. O primeiro protocolo de criptografia quântica fez uso dos estados de polarização de fótons (polarimétrico), sendo conhecido como BB84. Posteriormente, o mesmo protocolo, usando a fase dos fótons (interferométrico), foi proposto. Em 1992, surgiu o protocolo B92, também em versão interferométrica. Por fim, em 1991, foi proposto uma outra forma de implementar a criptografia quântica, através da correlação não-local de estados quânticos. Neste tipo de protocolo, faz-se uso da correlação entre dois fótons preparados através de conversão paramétrica descendente. Todos estes protocolos, versão polarimétrica ou interferométrica, foram implementados sobre sistemas ópticos a fibra ou na comunicação entre satélites [1,2]. A seguir, faremos uma rápida revisão do protocolo BB84 polarimétrico. Ele faz uso de 2 pares de estados ortogonais, por exemplo: (|0°⟩,|90°⟩) e (|45°⟩,|135°⟩). Os dois primeiros estados formam a base B_1, para um espaço de Hilbert de dimensão 2 e os dois últimos formam a base B_2, para o mesmo espaço. Os estados de B_1 e B_2 são relacionados por:

$$\left|0^\circ\right\rangle = \left(1/\sqrt{2}\right)\left(\left|45^\circ\right\rangle - \left|135^\circ\right\rangle\right) \quad (1)$$

$$\left|90^\circ\right\rangle = \left(1/\sqrt{2}\right)\left(\left|45^\circ\right\rangle + \left|135^\circ\right\rangle\right) \quad (2)$$

e suas inversas. Definimos, na Tabela 1, a representação dos bits pelos estados de polarização em cada base.

BASE	ESTADO	SÍMBOLO
$\mathbf{B_1}$	$\|0°\rangle$	0
	$\|90°\rangle$	1
$\mathbf{B_2}$	$\|45°\rangle$	0
	$\|135°\rangle$	1

Tabela 1 - Representação dos bits pelos estados de polarização.

Se Alice (transmissor) prepara e envia um fóton na base B_i e Bob (receptor) mede a polarização deste fóton usando a base B_j então, usando (1) e (2), a probabilidade do resultado da medição de Bob ser o mesmo bit representado pelo estado que Alice enviou é 0,5 se $i \neq j$ e 1, se $i = j$. Por exemplo, suponhamos que Alice envie um bit 0 na base B_2 (|45°⟩) e que Bob escolha a base B_1 para medir a polarização; então, a probabilidade de Bob obter, como resultado da medida, o bit 1, é dada pelo quadrado do módulo do coeficiente que multiplica |90°⟩ na expansão de |45°⟩ na base B_1. Da mesma forma, a probabilidade de Bob obter, como resultado, o bit 0, é dada pelo quadrado do módulo do coeficiente que multiplica |0°⟩ na expansão de |45°⟩ na base B_1. Nesses dois casos, a probabilidade é de 0,5. Em outras palavras, Bob tem 50% de chance de acertar o bit que Alice enviou. Quando Bob escolhe a mesma base que Alice, a probabilidade de Bob acertar o bit que Alice enviou é de 1 pois, obviamente, o coeficiente na expansão vale 1. A seguir, descrevemos a seqüência de passos que compõem o protocolo BB84 [1-2]:

1. Alice escolhe uma seqüência aleatória de bits.
2. Alice escolhe aleatoriamente a base, B_1 ou B_2 , para cada bit da seqüência, e envia um fóton por bit a Bob.
3. Bob escolhe aleatoriamente a base, B_1 ou B_2, para medir a polarização do fóton e vai armazenando os valores dos bits que ele obteve como resultado das medições.
4. Durante uma discussão pública, sem preocupações com segurança, Alice e Bob informam, um ao outro, quais bases eles usaram. Os bits para os quais Alice e Bob escolheram a mesma base, e, portanto, Bob os leu com 100% de acerto, são guardados e formarão a chave; os demais bits são descartados (*sifting*).

A discussão aberta de quais bases foram escolhidas não revela nenhuma informação útil a um usuário não autorizado. Este, daqui por diante, será chamado de Eva. Devemos, agora, determinar a influência da presença de Eva no canal de comunicação. Suponhamos que Eva leia os bits enviados por Alice e envie os resultados de sua mensuração a Bob. Podemos, então, considerar duas situações possíveis [3]: 1) a base escolhida por Eva é igual a de Alice e/ou Bob. Nesta situação Eva não provoca nenhum erro.

2) Alice e Bob ecolhem a mesma base e Eva uma base diferente de ambos, como mostra a Fig. 1.

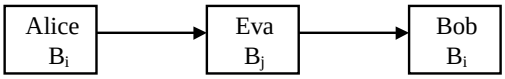

Figura 1 - Alice =Bob ≠ Eva

Nesta situação, Eva lê o bit enviado por Alice com 50% de certeza e o repassa a Bob. Este, por sua vez, lê o bit enviado por Eva com 50% de certeza. Com isto, apesar de Alice e Bob usarem mesma base, o bit lido por Bob poderá ser diferente do enviado por Alice. Como este bit fará parte da chave, Alice e Bob conterão chaves diferentes. Caso usem um algoritmo de detecção de erro, como teste de paridade, o erro poderá será detectado e, portanto, a presença de Eva também o será. Do exposto acima, verificamos que Eva tem uma probabilidade de 25% por bit de ser descoberta. Portanto, para uma chave de N bits, a probabilidade de não haver erros, na presença de Eva, é $0{,}75^N$. Alice e Bob podem escolher M, dos N bits da chave, compará-los publicamente, para ver se há erros, e depois descartá-los. Em todas as situações acima foram supostos detectores perfeitos e a ausência de ruídos. Na situação real não há como distinguir a presença de Eva e um erro causado por ruído. Se Alice e Bob acreditam que o erro na chave é devido ao ruído ou imperfeição de detectores, então pode-se usar um algoritmo de reconciliação para igualar as chaves de Bob e Alice, sendo os bits errados descartados.

2. RECEPTORES DE 1 FÓTON

O desempenho dos atuais sistemas de QKD, com a tecnologia atual, ainda esta aquém de seu valor ótimo. Por isso, o desenvolvimento de novas tecnologias para dar suporte às comunicações quânticas é um desafio a ser enfrentado. Em particular, fontes e detectores de luz de fótons isolados são os principais responsáveis pelo limitado desempenho. Basicamente, o receptor óptico deverá receber um fóton em sua entrada e gerar um pulso elétrico em sua saída. Como o nível de potência óptica devido a um fóton, nas janelas de comunicações ópticas, é muito baixo, o receptor não deve introduzir ruído, sob pena de não conseguir distinguí-lo do sinal de informação. Entretanto, um receptor óptico capaz de receber um fóton e gerar uma corrente elétrica possível de ser processada deve, necessariamente, usar um fotodiodo de avalanche, APD. Esses dispositivos são intrinsecamente ruidosos e, por isso, algumas precauções devem ser tomadas para viabilizar o uso de APDs. Para a região de 1300 nm os APDs de Ge são utilizados, enquanto que, na janela de 1550 nm, melhor para comunicações quânticas devido à baixa perda da fibra, APDs de InP/InGaAs são utilizados.

Para que uma avalanche possa ocorrer, incialmente o APD deve ser inversamente polarizado acima da tensão de ruptura, V_B (*breakdown voltage*). A eficiência de absorção, μ_1, é a probabilidade de que um fóton incidente no APD crie um par elétron-lacuna. O elétron criado é transportado por difusão para a região de ganho, onde um forte campo elétrico irá acelerá-lo. Existe um valor mínimo do campo que faz com que o elétron alcance a velocidade de saturação. Qualquer campo elétrico acima deste valor não aumenta a velocidade do elétron. Ao se deslocar pela região de ganho, o elétron se "chocará" contra os átomos da rede provocando a ionização dos mesmo. Cada novo elétron "arrancado" será também acelerado pelo campo elétrico e poderá provocar novas ionizações nos átomos da rede, criando, portanto, uma avalanche. A probabilidade de que um elétron na região de ganho crie uma avalanche é μ_2. No projeto de um receptor usando o APD, três parâmetros devem ser levados em conta: eficiência quântica, η, contagem de escuro (*dark count*), P_{esc}, e *afterpulsing*. A eficiência quântica é a probabilidade de um fóton incidente criar uma avalanche. Portanto, η depende de μ_1 e μ_2. Além disso η também depende da eficiência de acoplamento da luz no dispositivo. A eficiência quântica depende da temperatura, havendo um ponto ótimo, e do nível de tensão acima da tensão de ruptura, ao qual chamaremos tensão de excesso (*excess voltage*), V_e, através de μ_2. η aumenta com o aumento de V_e. Contagem de escuro é o aparecimento de avalanches criadas por pares elétron-lacuna de origem térmica, tunelamento ou armadilhas (*trapping process*). A contagem de escuro é um ruído e, portanto, deve ser minimizada. Para isso, o resfriamento do APD, através de nitrogênio líquido ou peltiers, é necessário. O processo de tunelamento não depende da temperatura. A contagem de escuro também depende de μ_2 e, portanto, P_{esc} aumenta com o aumento de V_e. O *afterpulsing* é o aprisionamento de portadores minoritários na região de ganho do APD. Esse portadores geram contagens de escuro. Entre a chegada de fótons consecutivos, o APD deve ter tempo suficiente para "descarregar as armadilhas" ou seja, para que esses portadores aprisionados sejam emitidos sem causar uma contagem. Portanto, o *afterpulsing* limita a taxa de transferência de fótons (e portanto de bits) entre o transmissor e o receptor. O *afterpulsing* melhora com o aumento de V_e.

Após uma avalanche ter sido iniciada, tão logo o sinal seja detectado, ela deve ser extinta (*quenched*) para não danificar o APD. Para a avalanche ser extinta devemos levar a tensão entre os terminais do APD para um valor abaixo da tensão de ruptura. Há três formas básicas de extinção da avalanche: passiva, engatilhada e ativa, podendo haver combinações dessas. Na Fig. 2 temos o circuito de extinção passiva [4-5].

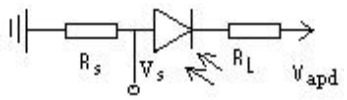

Figura 2 –Circuito de extinção passiva.

No circuito passivo temos $V_{apd} > V_B$ e R_L (kΩ) >> R_s (50Ω). Quando uma avalanche é inicada, a corrente aumenta, levando a um acréscimo na tensão entre os terminais de R_L e um correspondente descréscimo da tensão entre os terminais do APD. O tempo de extinção, T_q (ns), é dado por [4-5]:

$$T_q = \left(C_d + C_f\right)\left(R_d R_L / R_d + R_L\right) \tag{3}$$

onde R_d é a resistência interna (Ω-kΩ), C_d (1pF) é a capacitância da junção e C_f (~ pF) a capacitância de fuga (*stray*) do APD. Por outro lado, após o fim da avalanche, a tensão sobre o APD retorna a crescer, através da recarga das capacitâncias do APD, habilitando-o a iniciar uma nova avalanche. O tempo de recuperação, T_r (μs), é dado por [4-5]:

$$T_r = R_L\left(C_d + C_f\right) \tag{4}$$

Outro circuito usado é o de extinção passivo engatilhado, Fig.3.

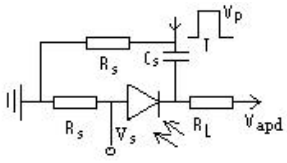

Figura 3 –Circuito de extinção passivo engatilhado.

Neste circuito $V_{apd} < V_B$. Um pulso de gatilho, de amplitude V_P e duração T se superpõe à tensão de polarização do APD, elevando-a, durante o tempo T, para um valor acima de V_B. Desta forma, a tensão de excesso, a qual afeta a eficiência, contagem de escuro e *afterpulsing*, descrita anteriormente, é dada por $V_e=V_{apd}+V_P-V_B$. Na Fig. 3, o primeiro resistor R_s (50Ω) é para casar a impedância de entrada com o gerador de pulsos, enquanto que o capacitor C_s desacopla R_s do circuito de polarização. O circuito da Fig. 3 funciona como um integrador, a tensão sobre o APD não é constante durante o intervalo T, sofrendo um decaímento. Além disso, o tempo de extinção e recuperação são modificados para [5]:

$$T_{qg} = R_L R_d \left(C_s + C_d + C_f\right) / R_L + R_d \quad (5)$$

$$T_{rg} = R_L \left(C_s + C_d + C_f\right) \quad (6)$$

Neste circuito, uma avalanche só pode ocorrer durante a presença de um pulso de gatilho, mas a exinção da mesma é devida ao circuito de extinção da Fig. 2. Entretanto, se $T < T_{qg}$ o pulso de gatilho também passa a ser responsável pela extinção. Este é o esquema que tem sido usado nos receptores em sistemas QKD. A principal vantagem dele é que uma contagem de escuro só pode acontecer dentro do intervalo T. Desta forma, a probabilidade de uma contagem de escuro é $P_{esc}=R_{esc}$T, onde R_{esc} é a taxa de contagem de escuro, suposta ser constante. Entretanto, o instante de chegada do fóton no receptor deve ser precisamente conhecido, exigindo uma perfeita sincronia entre Alice e Bob. Na Fig. 4 temos os pulsos de gatilho e de saída (V_s) devido a uma contagem de escuro (ruído), na temperatura ambiente. Os parâmetros são: V_{apd}=49V, V_P=3,30V, T=8ns, R_L=330kΩ, C_s=100nF e o APD é o C30644EJT-02 com V_B = 50V, em temperatura ambiente.

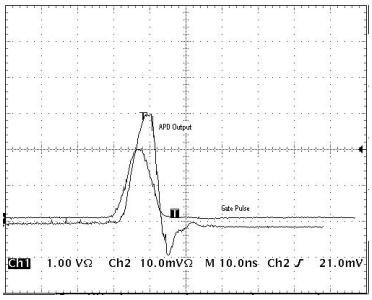

Figura 4 – Pulsos de gatilhamento e saída do Circuito da Fig. 3.

No pulso devido à avalanche, vemos a ação do integrador (*overshooting* negativo) quando da descida do pulso de gatilho. Por fim, na Fig. 5 propomos um possível circuito completo, usando gatilho, para um receptor de 1 fóton, oferencendo em sua saída um pulso com nível lógico TTL.

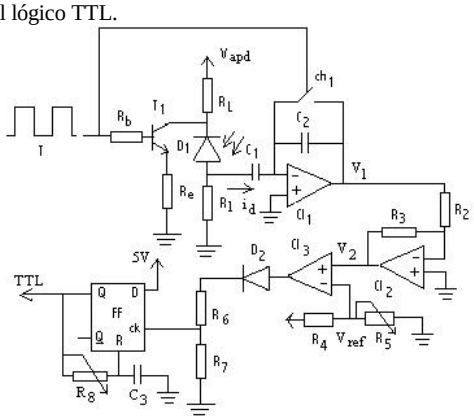

Figura 5 – Circuito para o receptor de 1 fóton.

Neste circuito, $V_{apd} > V_B$. Na presença de um pulsos de gatilho o transistor T_1 fica saturado e, sendo $R_e << R_L$, a tensão sobre o APD é menor que V_B. O nível alto do pulso de gatilho também mantém a chave ch_1 fechada. Quando o pulso vai para o nível lógico baixo, o transistor T_1 vai para o corte, elevando a tensão sobre o APD e habilitando-o a iniciar uma avalanche, e a chave ch_1 se abre. Caso uma avalanche ocorra, seja devido à chegada de um fóton ou à contagem de escuro, a corrente i_d vai, via C_1, para o integrador formado por CI_1 e C_2. A tensão na saída do integrador é dada por:

$$V_1 = \left(-1/C_2\right)\int i_d(t)dt \quad (7)$$

Quanto maior o tempo de integração, maior será V_1; entretanto, maior será, também, o tempo em que o APD deverá suportar a avalanche. Para i_d em μA, C_2 = 10pF e tempo de integração de 10ns, teremos, em média, na saída, alguns milivolts. Esta tensão é ,então, entregue ao amplificador inversor, formado por CI_2, R_2 e R_3, sendo a tensão na saída do mesmo dada por:

$$V_2 = -V_1 R_3 / R_2 \quad (8)$$

Esta tensão é, então, entregue ao comparador, formado por CI_3, R_4 e R_5, sendo estes dois últimos responsáveis pela tensão de referência, V_{ref}. Caso $V_2 < V_{ref}$ a tensão na saída de CI_3 será negativa e nada acontecerá, pois a mesma será bloqueada pelo diodo D_2. Por outro lado, se $V_2 > V_{ref}$, a tensão na saída de CI_3 será positiva, sofrerá um redução em R_6 e R_7, e servirá como entrada de *clock* do *flip-flop* tipo D, FF. Neste, quando uma transição positiva no *clock* ocorrer, o nível lógico na entrada D (sempre alto, 5V) será transferido para a saída Q, que também é a saída do receptor. Esta saída também é conectada, via circuito formado por R_8 e C_3, à entrada de *reset* do FF. Desta forma, depois de um intervalo de tempo determinado pelos valores de R_8 e C_3, o FF será zerado (a saída Q voltará ao nível lógico baixo). Assim, R_8 e C_3 controlam a duração do pulso de saída, o que pode ser útil na conexão entre o receptor e um PC. Devido à curta duração dos pulsos de gatilho (ns) os componentes devem ser velozes e com grande largura de banda. Em particular, o FF pode ser do tipo que usa lógica ECL, mais rápido que o similar que usa lógica TTL; entretanto, para tornar o receptor apto a ser conectado com um PC, conversores ECL-TTL devem ser usados. Os circuitos integrados CI_1-$_3$ podem ser trocados por um amplificador de grande largura de banda, como os usados em telefonia celular ou redes ópticas de alta velocidade. Por fim, a chave ch_1 tem a função de descarregar o capacitor C_2. Esta chave, que já vem inclusa no CI integrador, precisa permanecer fechada por 10μs para garantir a total descarga do capacitor. Portanto, entre dois níveis lógicos baixos do pulso de gatilho devemos ter, no mínimo, 10μs, o que limita a taxa de transferência de dados a 100 kbit/s.

3. TAXA DE ERRO EM SISTEMAS QKD

Durante a transmissão dos bits da chave alguns erros podem acontecer, devido às imperfeições dos componentes ou à ação de Eva. A taxa de erros em sistemas QKD, QBER, é definida como sendo a razão entre o número de bits errados e o número total de bits e pode ser estimada pela razão entre a probabilidade de Bob obter uma contagem falsa e a probabilidade total de obter uma contagem, por pulso. A probabilidade de Bob obter uma falsa contagem é devido a dois fatores: 1) erros introduzidos devido às imperfeições no link óptico - probabilidade de um fóton ir para o detector errado, P_{opt}, devido à interferência imperfeita (visibilidade do interferômetro menor que 1), luz não completamente polarizada

ou bases não perfeitamente paralelas; 2) Contagem de escuro do fotodetector (*dark count*), P_{esc}. Com isto, obtém-se para o protocolo BB84 [2]:

$$QBER = \left(P_{opt}\eta\mu_f + 0{,}5P_{esc}n\right)/\left(\eta\mu_f + nP_{esc}\right) \qquad (9)$$

onde P_{opt} é a probabilidade do fóton ir para o detector errado, n (=1,2) é o número de fotodetectores, 0,5 é a probabilidade da contagem de escuro provocar um erro, uma vez que ela pode acontecer no detector para onde o fóton deve ser realmente dirigido, η é a eficiência quântica do fotodetector e μ_f é o número médio de fótons incidindo no mesmo. Para pequenos valores de μ_f, $\eta\mu_f$ é a uma boa aproximação da probabilidade do detector realizar uma contagem devido à presença de um fóton. Usando (9), podemos avaliar o desempenho do sistema como função dos parâmetros do receptor, P_{esc} e η, e da distância entre Alice e Bob, via μ_f.

4. ESTRATÉGIAS DE ESPIONAGEM

Para realizar a espionagem, Eva pode usar chaves e acopladores ópticos. Estes dispositivos devem possuir baixa perda, ter alta velocidade de comutação e estarem bem casados ao enlace óptico entre Alice e Bob, de forma que não hajam reflexões que possam denunciar alterações no canal óptico. Além disso, Eva deve saber antecipadamente quais bases Alice e Bob usarão na comunicação. Analizaremos duas possíveis estratégias usadas por Eva: Intercepta/Re-envia (I/R) e o ataque em pulsos multifótons através de divisores de feixes (*beam splitter atack*).

4.1 Ataque Intercepta/Re-envia

Neste ataque, Eva intercepta os pulsos enviados por Alice, faz uma medição para identificar o estado quântico enviado, prepara um fóton segundo o resultado de sua medição e o envia para Bob. Para a medição, Eva usa um aparato como o mostrado na Fig. 6:

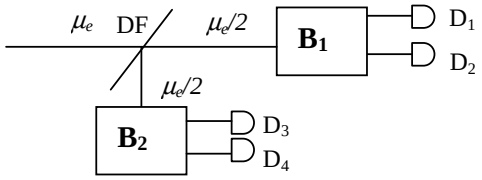

Figura 6 – Aparato de Eva para a estratégia I/R.

Nesta, DF é um divisor de feixe balanceado (50/50), μ_e é o número médio de fótons chegando em Eva, B1 e B2 são medidores nas referidas bases e D1-D4 são fotodetectores. É comum dar-se maior (ou mesmo ilimitado) poder tecnológico a Eva. Se o sistema é seguro contra uma Eva superpoderosa, será também seguro para uma Eva com os mesmo recursos tecnológicos disponíveis para Alice e Bob. Entretanto, assumiremos apenas que os fotodetectores de Eva são ideais, P_{esc}=0 e η=1, e que a probabilidade do fóton ir para o detector errado é nula. Consideremos que uma detecção nos detectores D1 e D3 representam o bit 0, enquanto que uma detecção nos detectores D2 e D4 representam o bit 1. Além disso, usaremos 1 para identificar uma contagem e 0 para identificar a ausência de uma contagem. Assim, P(D_4=0,D_3=0,D_2=0,D_1=1), ou simplesmente P(0001), por exemplo, representa a probabilidade de uma contagem no detector D_1 e nenhuma contagem nos demais detectores. Observando a Fig. 6, podemos ver que Eva pode ter 16 resultados possiveis, ou seja, todas as combinações entre nenhum detector ser disparado (0000) e todos os 4 serem disparados (1111). Entretanto, para que 3(4) detectores sejam disparados precisamos, necessariamente, ter um pulso com no mínimo 3(4) fótons. Como o pulso enviado por Alice é de baixíssima intensidade, essa probabilidade é muito pequena e não a consideraremos em nossa análise. Entretanto, para análise dos demais casos consideraremos a possibilidade de um pulso ter qualquer número de fótons. Isto simplifica a análise. O resultado 0000 não é interessante para Eva pois ela não ganha nenhuma informação. Neste caso, ela não envia nenhum pulso para Bob. Assim, separaremos os resultados de interesse em 3 casos: 1) Fóton(s) chega(m) em um único detector: 0001, 0010, 0100, 1000. 2) Fótons chegam em dois detectores mas em bases diferentes: 0101, 0110, 1001, 1010. 3) Fótons chegam nos dois detectores da mesma base: 0011, 1100. Nesta última situação Eva também não ganha nenhuma informação pois a mesma apenas indica que a base na qual as detecções ocorreram não é a mesma base que Alice usou (na base correta a probabilidade de coincidência é nula) e não dá nenhuma informação sobre o valor do bit. Desta forma, quando o caso 3 ocorrer, Eva deve descartar o resultado e não enviar nada para Bob. Antes de iniciar a análise dos casos de interesse recordemos que a probabilidade do detector, sem ruído, obter uma contagem é:

$$P_c\left(\mu_f\right) = 1 - e^{-\eta\mu_f} \qquad (10)$$

onde μ_f é o número médio de fótons chegando no fotodetector. Além disso, o medidor da base errada se comporta como um divisor de feixe balanceado. Analisemos, agora, o caso 1. As probabilidades de apenas um detector ser disparado são :

$$P(0001) = P(0010) = P(0100) = P(1000) = \qquad (11)$$
$$\frac{1}{2}\left\{\frac{1}{2}P_c(\mu_e/2)[1-P_c(\mu_e/4)]^2 + [1-P_c(\mu_e/2)][1-P_c(\mu_e/4)]P_c(\mu_e/4)\right\}$$

Ou seja, é a probabilidade de termos uma contagem (no detector) na base correta e não termos contagem na base errada ou, não termos uma contagem na base certa e termos uma contagem na base errada. O termo 0,5 ocorre porque a base correta tanto pode ser B1 quanto B2. A informação (Shannon) ganha por Eva, por pulso, é:

$$I_E = H(E) - H(E \mid A) = -\sum_{x,y=0}^{1} P_E(x,y)\log P_E(x,y) - \qquad (12)$$
$$\sum_{w,z=0}^{1} P_A(w,z)\sum_{x,y=0}^{1} P_{E|A}(x,y \mid w,z)\log P_{E|A}(x,y \mid w,z)$$

sendo $P_A(w,z)$ [$P_E(x,y)$] a probabilidade de Alice (Eva) enviar (receber) o bit $z(y)$ (0 ou 1) na base $w(x)$ (0→B1,1→B2). Supondo as probabilidades de transmissão equiprováveis, temos P_A=0,25. $P_{E|A}(x,y|w,z)$ é a probabilidade de Eva ter recebido o bit y, na base x, dado que Alice enviou o bit z na base w. As probabilidades $P_{E|A}(x,y|w,z)$ são dadas por:

$$P_{E|A} = \begin{cases} f_1 = P_c(\mu_e/2)[1-P_c(\mu_e/4)]^2 \text{ se } w = x \text{ e } z = y \\ 0 \text{ se } w = x \text{ e } z \neq y \\ f_2 = [1-P_c(\mu_e/2)][1-P_c(\mu_e/4)]P_c(\mu_e/4) \text{ se } w \neq x \end{cases} \qquad (13)$$

Por último, as probabilidades incondicionais de Eva, $P_E(x,y)$, são $P_E(0,0) = P(0001)$, $P_E(0,1) = P(0010)$, $P_E(1,0) = P(0100)$ e $P_E(1,1) = P(1000)$. Usando (10)-(13), obtemos a informação que Eva obtém quando o caso 1 ocorrer:

$$I_e^{(1)} = -4P_E(0,0)\log[P_E(0,0)] + [f_1\log(f_1) + 2f_2\log(f_2)] \quad (14)$$

De posse do resultado de sua medição, Eva deve enviar um pulso para Bob. Neste momento, Eva pode provocar um erro na comunicação entre Alice e Bob caso ela não obtenha em sua medição a base correta. A probabilidade de Eva obter a base correta e o bit errado é nula, uma vez que assumimos que a probabilidade do fóton ir para o detector errado é nula. Assim, a probabilidade de Eva obter a base errada, para cada pulso enviado por Alice é $P_{be} = 2[1-P(\mu_e/2)][1-P(\mu_e/4)]P(\mu_e/4)$ e a probabilidade de que Eva provoque um erro na comunicação entre Alice e Bob, no caso 1, é:

$$P_{erro}^{(1)} = 0{,}5P_{be}P_B \quad (15)$$

sendo 0,5 a probabilidade de Alice e Bob escolherem a mesma base e P_B a probabilidade de Bob obter uma contagem apenas no detector referente ao bit errado:

$$P_B = P_c(\mu_b/2)[1-P_c(\mu_b/2)] \quad (16)$$

onde μ_b é o número de fótons chegando em Bob. Dividindo a probabilidade de erro (15) pela probabilidade de Bob obter uma contagem, temos a $QBER_1$:

$$QBER_1 = P_{erro}^{(1)}/[0{,}5P_c(\mu_b) + P_c(\mu_b/2)(1-P_c(\mu_b/2))] \quad (17)$$

Analisemos, agora, o caso 2, uma contagem em cada base. Temos que $P(0101) = P(0110) = P(1001) = P(1010)$, e:

$$P(0101) = 0{,}5P_c(\mu_e/2)P_c(\mu_e/4)[1-P_c(\mu_e/4)] \quad (18)$$

Esta situação é a mais favorável a Eva. Após Alice e Bob divulgarem as bases que usaram, Eva terá certeza do valor do bit uma vez que ela obteve contagem em ambas as bases. Portanto, $I_e^{(2)}$=1 bit. Como Eva terá que enviar um fóton para Bob, ela poderá ecolher aleatoriamente um dos dois resultados que obteve e enviá-lo. Nesta caso, a probabilidade de Eva introduzir um erro é igual à do caso 1. Outra possibilidade, mais proveitosa para Eva, seria enviar para Bob o estado $(|x\rangle + \exp(i0{,}25\pi)|y\rangle)/\sqrt{3}$ [6], onde x e y são os estados obtidos nas medições. Por exemplo, se Eva obteve 0101, o que representa uma medição do bit 0 em cada base, e os estados de (1) e (2) são usados, Eva envia para Bob o estado $(|0^\circ\rangle + \exp(i0{,}25\pi)|45^\circ\rangle)/\sqrt{3}$. Nesta situação, a probabilidade de erro e a $QBER_2$ são dadas por:

$$P_{erro}^{(2)} = 0{,}5P_c(\mu_B/6)[1-P_c(5\mu_B/6)] \quad (19)$$

$$QBER_2 = P_{erro}^{(2)} \Big/ \left\{ \begin{matrix} P_c(5\mu_b/6)[1-P_c(\mu_b/6)] + \\ P_c(\mu_b/6)[1-P_c(5\mu_b/6)] \end{matrix} \right\} \quad (20)$$

A informação total que Eva obtém e a QBER total que ela provoca são dadas por:

$$I_e = P_1 I_e^{(1)} + P_2 I_e^{(2)} \quad (21)$$

$$QBER = P_1 QBER_1 + P_2 QBER_2 \quad (22)$$

onde P_1 e P_2 são as probabilidades dos casos 1 e 2 ocorrerem, respectivamente. Consideremos, agora, que Alice e Bob estejam separados por um distância de 50 km e Eva se posicione em algum lugar entre ambos. Alice e Eva enviam pulsos para Eva e Bob, respectivamente, com número médio de fótons μ=0,1. As fibras ópticas conectando Alice-Eva e Eva-Bob possuem perda de 0,25 dB/km. Por fim, também assumimos que os detectores de Bob são ideais. A Fig. 7, a seguir, mostra a informação ganha por Eva e o distúrbio que ela provoca, para os pulsos realmente existentes (no mínimo um fóton), como função de sua posição.

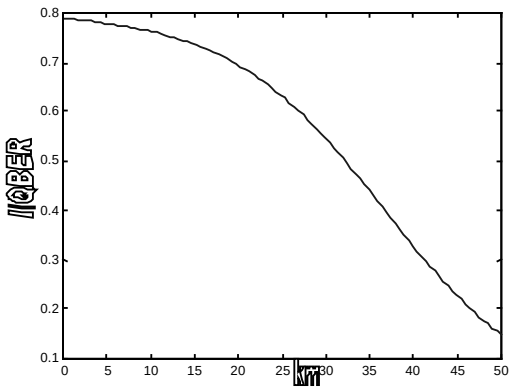

Figura 7 – Informação/QBER para o ataque I/R versus a posição de Eva.

À medida que Eva se afasta de Alice a relação (informação ganha) /(ruído introduzido) diminui. Assim, a melhor posição para Eva é tão próxima de Alice quanto possível.

4.2 Ataque por Divisor de Feixe

Este ataque é mais efetivo quando a distância entre Alice e Bob é grande, pois a probabilidade de Alice produzir um pulso multifóton é maior que a probabilidade de Bob obter uma contagem:

$$P(n \geq 2 \mid n > 0) \approx 0.5\mu_a + 0.25\mu_a^2 > P_c \approx \eta\mu_a \exp(-\alpha L) \quad (23)$$

onde L (grande o suficiente para (23) ser válida) é o comprimento da fibra e α a taxa de perda da mesma. No ataque por divisor de feixe (*beam spliter atack*), Eva tenta tirar um fóton de um pulso multifóton enviado por Alice e deixa o resto passar para Bob. Desta forma, Eva não introduz erro (uma vez que ela não envia nada para Bob), embora ela modifique as probabilidades de Bob obter uma contagem simples e de coincidência, uma vez que ela diminui a intensidade do pulso que chegará a Bob. Uma alternativa para Eva evitar essa mudança seria prover um outro enlace óptico entre ela e Bob, com menor perda, seja por fibra de melhor qualidade, ou pelo uso de um caminho alternativo de menor comprimento entre ambos, de forma a compensar a parcela de energia do pulso que ela consumiu. A configuração para o ataque por divisor de feixe é mostrada na Fig. 8.

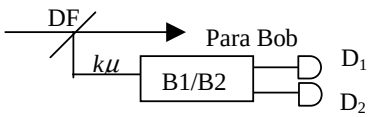

Figura 8 – Configuração de Eva para o ataque por divisor de feixe.

Na Fig. 8, *k* é a fração do pulso desviada por Eva. Assumimos que uma contagem em $D_{1(2)}$ representa o bit 0(1). Eva escolhe aleatoriamente qual base usará, B1 ou B2, para fazer uma medição do valor do bit enviado por Alice. A informação obtida por Eva é dada por:

$$I = -[P_E(0)\log(P_E(0)) + P_E(1)\log(P_E(1))] + f_1\log(f_1) + f_2\log(f2) \quad (24)$$

$$f_1 = 0{,}5P_c(k\mu_e) + 0{,}5P_c(k\mu_e/2)[1 - P_c(k\mu_e/2)] \quad (25)$$

$$f_2 = 0{,}5P_c(k\mu_e/2)[1 - P_c(k\mu_e/2)] \quad (26)$$

sendo $P_E(0)$ e $P_E(1)$ as probabilidades de Eva obter, como resultado de sua medição, os bits 0 e 1, respectivamente. f_1 e f_2 são as probabilidades condicionais dos resultados de Eva, dado o bit e a base escolhidos por Alice, $P_{E|A}$. Quando Eva não obtém nenhuma contagem ou obtém uma em cada detector, ela não ganha nenhuma informação. A Fig. 9 mostra a informação ganha por Eva para o ataque por divisor de feixe.

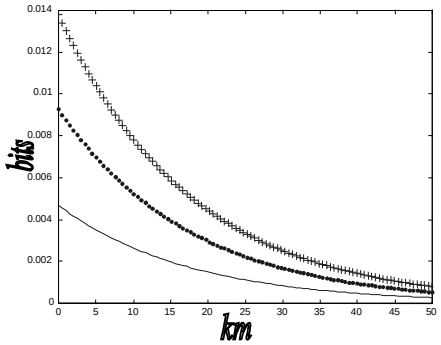

Figura 9 – Informação x posição de Eva no ataque por divisor de feixe. *k*=0,25 (-), *k*=0,5(.), *k*=0,75 (+).

Na Fig. 9 observamos que, na medida que Eva se afasta de Alice, a informação que ela obtém diminui e, portanto, a melhor posição para Eva é a mais próxima de Alice possível. Além disso, quando *k* cresce a informação também aumenta. Entretanto, um maior valor de *k* implica em menos fótons indo para Bob, o que altera fortemente as probabilidades de detecção dos mesmos, levando Bob a desconfiar da presença de Eva, caso esta não providencie uma linha com menor perda entre ela e Bob para compensar o(s) fóton(s) "roubado(s)". Nenhuma das duas estratégias apresentadas é a mais inteligente que Eva pode realizar. De fato, há outras possibilidades como o uso de UQCM (*universal quantum copy machines*), bem como o uso alternado de técnicas visando tirar o máximo proveito de cada situação. Entretanto, as duas estratégias aqui abordadas são as mais próximas da realidade tecnológica atual.

5. CONCLUSÕES

Inicialmente, fizemos uma revisão do protocolo BB84 polarimétrico, explicando os papéis de Alice, Bob e Eva no protocolo. Em seguida, trabalhamos o receptor de 1 fóton, dissertando sobre o funcionamento e propriedades de APDs, circuitos de extinção (*quenching*), com uma medição do pulso de saída no circuito engatilhado e propondo um circuito completo para o receptor, com nível de saída TTL, detalhando alguns pontos práticos importantes. Por fim, fizemos a análise de duas estratégias de espionagem possíveis de serem realizadas por Eva, Intercepta/Re-envia e Ataque por Divisor de Feixe, com Eva possuindo tecnologia de ponta atual ou possível em futuro próximo.

6. AGRADECIMENTOS

Este trabalho foi parcialmente financiando pelas agência brasileiras CAPES and CNPq.

7. REFERÊNCIAS

[1] Simon J. D. Phoenix and Paul D. Townsend, "Quantum cryptography: how to beat the code breakers using quantum mechanics", *Contemporary Physics*, **36**: 165-195, 1995.

[2] Nicolas Gisin, Grégoire Ribordy, Wolfang Tittel and Hugo Zbinden, "Quantum cryptography", quant-ph/0101098, http://xxx.lanl.gov.

[3] K. J. Blow and Simon J. D. Phoenix, " On a fundamental theorem of quantum cryptography", *Journal of Modern Optics*, **40**:33-36, 1993.

[4] Grégorie Ribordy, Jean-Daniel Gautier, Hugo Zbinden, and Nicolas Gisin, "Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters", *Applied Optics*, **37**, n° 12, 2272-2277, 1998.

[5] Frederik Gibson, **Experimental evaluation of Quantum Cryptography system for 1550nm**, Master of Science thesis, Department of eletronics-QEO, Kungl Tekniska Högskolan, 1998.

[6] Stéphane Félix, Nicolas Gisin, André Stefanov and Hugo Zbinden, "Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses" quant-ph/0102062, http://xxx.lanl.gov.