Universidade Federal de Goiás
Instituto de Física

Guilherme Silva Barros

Distribuição Quântica de Chaves Utilizando o Perfil Transversal de Fótons Únicos

Goiânia
2024

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE FÍSICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): Guilherme Silva Barros

Título do trabalho: Distribuição Quântica de Chaves Utilizando o Perfil Transversal de Fótons Únicos

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Rafael De Morais Gomes**, **Professor do Magistério Superior**, em 06/02/2024, às 16:07, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Guilherme Silva Barros**, **Discente**, em 09/02/2024, às 14:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Guilherme Silva Barros

Distribuição Quântica de Chaves Utilizando o Perfil Transversal de Fótons Únicos

Trabalho de Conclusão de Curso apresentado à banca examinadora do Instituto de Física da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Bacharel em Física.

Área de concentração: Física

Linha de pesquisa: Óptica Quântica

Orientador: Prof. Dr. Rafael de Morais Gomes

Goiânia
2024

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Barros, Guilherme Silva
Distribuição Quântica de Chaves Utilizando o Perfil Transversal de Fótons Únicos [manuscrito] / Guilherme Silva Barros. - 2024.
35, f.

Orientador: Prof. Dr. Rafael de Morais Gomes.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, , Física, Goiânia, 2024.
Bibliografia.
Inclui abreviaturas, lista de figuras.

1. QKD. 2. Criptografia Quântica. 3. Informação Quântica. 4. Óptica Quântica. I. Gomes, Rafael de Morais, orient. II. Título.

CDU 53

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE FÍSICA

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos 2 dias do mês de fevereiro de 2024, a partir das 10h00min, **no Instituto de Física - UFG, sala 1-229**, realizou-se a sessão pública de Defesa de Trabalho de Conclusão de Curso do estudante do curso de Física, Bacharelado, **Guilherme Silva Barros,** matrícula 201803270, para apresentar sua monografia intitulada: "**Distribuição Quântica de Chaves Utilizando o Perfil Transversal de Fótons Únicos**". A banca examinadora foi composta pelos professores **Rafael de Morais Gomes** (IF/UFG), **Ardiley Torres Avelar** (IF/UFG) e **Guilherme Luiz Zanin** (IF/UFG). A sessão pública de Defesa de TCC foi aberta pelo Presidente da Banca Examinadora, Professor Rafael de Morais Gomes (Orientador), que na sequência passou a palavra para o estudante apresentar sua monografia. Após a exposição, a Banca Examinadora realizou a arguição do estudante. Ao finalizar a arguição, a Banca reuniu-se em sessão secreta a fim de concluir o julgamento da monografia. A Banca atribuiu ao estudante a nota **10,0**, este foi **APROVADO** na disciplina de TCC. Proclamados os resultados pelo Professor Rafael de Morais Gomes (Presidente), foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos membros da Banca Examinadora.

Documento assinado eletronicamente por **Rafael De Morais Gomes**, **Professor do Magistério Superior**, em 02/02/2024, às 09:10, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Guilherme Luiz Zanin**, **Professor do Magistério Superior**, em 02/02/2024, às 10:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Ardiley Torres Avelar**, **Professor do Magistério Superior**, em 02/02/2024, às 10:59, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4343729** e o código CRC **2C34DFD9**.

Referência: Processo nº 23070.059790/2023-14 SEI nº 4343729

Agradecimentos

Agradeço a minha família e amigos por me apoiarem nessa longa jornada. Agradeço também ao Prof. Dr. Rafael de Morais Gomes por aceitar me orientar e confiar no desenvolvimento deste projeto.

"Haveis de ver que percebeis a fundo
O que não cabe no cérebro humano!"

– Johann Wolfgang von Goethe

Resumo

A Distribuição Quântica de Chaves é um protocolo de Criptografia Quântica que promete atingir um alto nível de segurança na transmissão de informações confidenciais. Tal procedimento garante a segurança da troca de informações sigilosa em decorrência do uso de propriedades quânticas em um sistema, como o teorema da não clonagem, a desigualdade de Bell e a superposição de estados. No seguinte trabalho, é feito um estudo sobre o perfil de transversal de fótons únicos dentro do campo da criptografia quântica. Analisando teoricamente e experimentalmente protocolos de distribuição quântica de chaves que utilizam de variáveis contínuas transversais e variáveis de polarização de fótons únicos. Além disso, investigamos uma nova forma de ataque potencialmente perigosa para os sistemas de distribuição quântica de chaves.

Palavras - chave: QKD, Criptografia Quântica, Informação Quântica, Óptica Quântica.

Abstract

The Quantum Key Distribution is a Quantum Cryptography protocol that promises to achieve a high level of security in the transmission of confidential information. This procedure guarantees the security of the exchange of sensitive information due to the use of quantum properties in a system, such as the non-cloning theorem, Bell's inequality and the superposition of states. In the following work, a study is made of the transversal profile of single photons within the field of quantum cryptography. We analyze theoretically and experimentally Quantum Key Distribution protocols that use transverse continuous variables and single photon polarization variables. In addition, we investigate a new form of attack that is potentially dangerous for quantum key distribution systems.

Key - words: QKD, Quantum Cryptography, Quantum Information, Quantum Optics.

Lista de Figuras

Lista de Abreviações

UFG Universidade Federal de Goiás

QKD Quantum Key Distribution

BS Beam Splitter

HWP Half-Wave Plate

PBS Polorized Beam Splitter

EPR Einstein Podolsky Rosen

CHSH Clauser Horne Shimony Holt

QBER Quantum Bit Error Rate

Sumário

CAPÍTULO 1

Introdução

Por séculos, a necessidade de transmitir informações de modo seguro e em total sigilo tem sido um desafio para pesquisadores. A área do conhecimento que estuda e aplica formas de comunicação confidenciais recebe o nome de criptografia. A necessidade de um canal seguro de comunicação e transmissão de informações tem sido de grande importância durante diferentes períodos da historia, mas principalmente em tempos de conflitos em que o o envio de mensagem confidenciais eram de extrema importância. Mas, nos tempos atuais, com o advento da internet, a forma como é possível se comunicar tornou-se ampla e fácil, mas que carrega grandes riscos de segurança. Dessa forma, a criptografia atual vem exigindo cada vez mais o desenvolvimento de métodos seguros no envio de informações.

A criptografia moderna utiliza de protocolos que anunciam publicamente o algoritmo utilizado para codificar a informação a ser transmitida. No entanto, ao disponibilizar publicamente o procedimento quebra com toda a intenção de sigilo e seguração da mensagem transmitida. Os protocolos são a transmissão de uma sequência de números aleatórios entre um emissor (na literatura chamado de Alice) e um receptor (Bob). Para a transmissão de informação, o emissor utiliza de um canal público autenticado.

Por mais seguro que o canal de transmissão seja, sempre existe a possibilidade de um espião (chamado Eve) efetuar um ataque e roubar as informações sem que Alice e Bob possam saber. Os protocolos de criptografia clássica partem do princípio de garantir que o espião seja detectado antes que possa obter alguma informação relevante, produzindo algoritmos que levam tempo demais para descriptografar a mensagem.

A criptografia quântica surge para sanar a preocupação da seguração na transmissão de informações sigilosa, uma vez que, é possível detectar espiões que tentaram obter dados do protocolo. Uma vez que a Quantum Key Distribution (QKD) tem se tornado uma realidade comercial [1] que vem crescendo a cada ano, existe um grande interesse em desenvolver protocolos e implementações ainda mais seguros para a transmissão de informações. Neste trabalho, analisamos um protocolo de distribuição quântica de chaves utilizando de variáveis contínuas e discretas para a proteção dos dados [2]. Além disso, in-

vestigamos ainda uma nova forma de ataque ao protocolo descrito o qual não performado diretamente ao canal quântico.

1.1 QKD

As primeiras ideias de distribuição quântica de chaves foram propostas por Wisner no final dos anos 1960 [3]. No entanto, as ideias de Wisner não foram aceitas para publicação de antemão, e somente após quase uma década Wisner teve seu trabalho publicado [4]. Wisner havia proposto que estados quânticos emaranhados, caso pudessem ser armazenados por longos períodos de tempo, poderiam ser usados para sistema de segurança bancário. O primeiro protocolo de QKD foi proposto por Bennett e Brassard em um artigo publicado em 1984 [5] e ainda é uma referência para os estudos atuais da criptografia quântica. Comumente chamado de BB84, neste esquema a chave é criada enviando fótons que podem ser preparados em quatro estados de polarização.

No entanto, estes fótons não estão emaranhados, sendo assim, em 1991, Artur K. Ekert, propôs um novo protocolo (E91) [6] fazendo uso do estado de Bell para a transmissão de informação, onde a segurança do esquema se baseia na restrição da violação da desigualdade de Clauser-Horne-Shimony-Holt (CHSH) [7].

A seguir, traremos uma breve explicação de como ambos os protocolos, BB84 e E91, funcionam.

1.2 BB84

No protocolo BB84, Alice deseja enviar uma informação a Bob e gera uma sequência aleatória de zeros e um, codificando cada bit em um respectivo qubit, $|0\rangle$ ou $|+\rangle$ se o bit corresponder ao 0 e $|1\rangle$ ou $|-\rangle$ se for correspondente a 1. Para cada bit Alice escolhe um base de polarização (Horizontal 0° / Vertical 90°) e (Diagonal +45° / Antidiagonal −45°) e a direção de polarização dos fótons serão os observáveis a definirem o qudit da chave. Como representado na figura 1.1, cada digito, para formar uma chave, será um autoestado do fóton.

A mistura de estados da base, a qual é escrita a partir da construção de cada estado quântico de um conjunto $\{|\psi_1\rangle, |\psi_2\rangle, \ldots |\psi_n\rangle\}$ [8]:

$$\rho = \sum p_n |\psi_n\rangle\langle\psi_n| \tag{1.1}$$

onde a probabilidade associada aos autoestados é denotado por p_n. Veja que, para as bases, os estados correlacionados tem a seguinte forma:

$$|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}$$

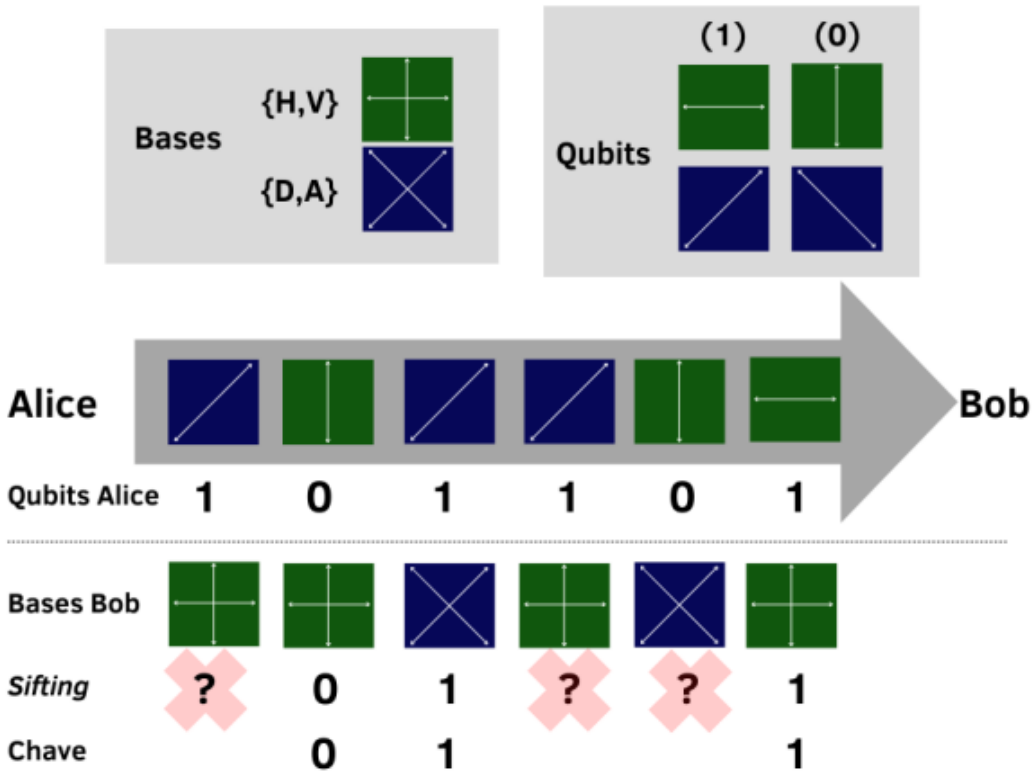

Figura 1.1: Representação do esquema experimental do protocolo BB84(FERRO, 2023).

$$|A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}$$

A probabilidade para cada autoestado que foi preparado com as bases ortogonais {H,V} e medido nas bases ortodiagonais {D,A} é $p_o = 1/2$ e $p_1 = 1/2$. Para cada qubit, Bob realiza suas medições escolhendo aleatoriamente as bases de medição, sem receber informações sobre a base escolhida por Alice, sendo assim, metade das vezes Bob escolhe a base certa e tem o mesmo bit que Alice, isso é claro se considerarmos que não há um espião ou ruído no protocolo. Através de um canal de um canal clássico, Bob transmite a Alice as respectivas bases de escolhida das medições. Ainda por um canal clássico e público, Alice informa as bases que ela escolheu para transmitir cada qubit, com isso, eles excluem todas as medições as quais as bases escolhidas não coincidem. Após isto, eles compartilham uma *raw key* e a partir disso começam a gerar uma chave segura.

Por um canal público, Alice e Bob comparam suas chaves de uso único e a partir dessa comparação é possível saber a taxa de erro devido aos efeitos de ruído ou a ação de um espião. Se essa taxa for muito alta, o protocolo é descartado e todo o procedimento recomeça. Caso contrário, é realizada uma reconciliação de informação e amplificação de privacidade sobre os bits restante de suas chaves de uso único.

1.3 E91

O protocolo proposto por Ekert em 1991 [6] é um criptosistema que utiliza do emaranhamento dos pares EPR [9]. Uma fonte S emite um par de qubits no estado EPR

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1.2}$$

O qubits são enviados em direções opostas, o primeiro é entregue a Alice e o segundo a Bob (ver figura 1.2). Alice e Bob podem descobrir a presença de um espião à transmissão dos pares EPR explorando a correlação destes pares. As medições são realizadas em três diferentes direções $\hat{a_1}$, $\hat{a_2}$, $\hat{a_3}$ para Alice e $\hat{b_1}$, $\hat{b_2}$, $\hat{b_3}$ para Bob (ver figura 1.3). Para cada par, Alice e Bob escolhem aleatoriamente entre seus eixos (bases) de medições.

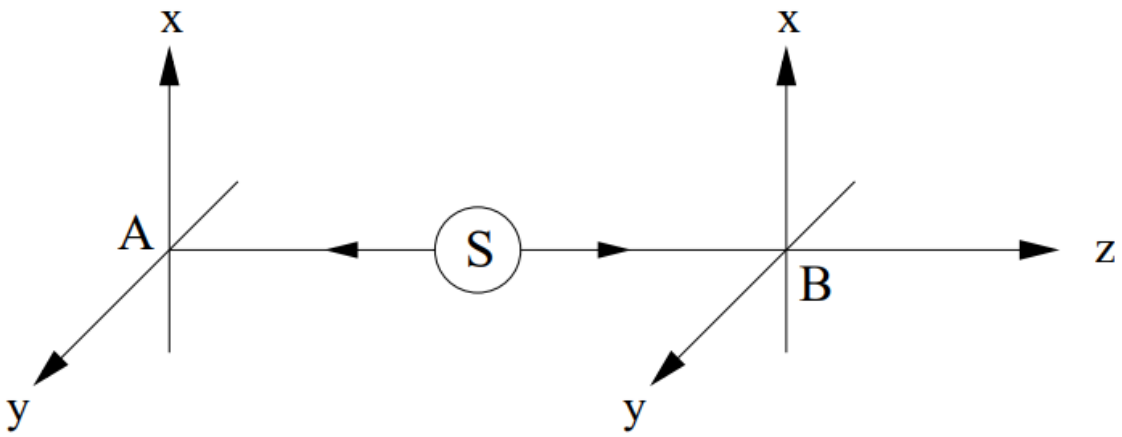

Figura 1.2: Esquema do protocolo E91(BENENTI, 2004).

A probabilidade de Alice efetuar suas medições na base de polarização ao longa da direção $\hat{a}_i$ é denotado por $p_{\pm\pm}(\hat{a}_i, \hat{b}_j)$ o que implica no resultado ± 1 e a medição de Bob ao longo de $\hat{b}_j$ da ± 1. Podemos definir os coeficientes de correlação como [10]:

$$E(\hat{a_i}, \hat{b_j}) = p_{++}(\hat{a_i}, \hat{b_j}) + p_{--}(\hat{a_i}, \hat{b_j}) + p_{+-}(\hat{a_i}, \hat{b_j}) - p_{-+}(\hat{a_i}, \hat{b_j}). \tag{1.3}$$

Sabendo que

$$C \equiv E(\hat{a_1}, \hat{b_1}) - E(\hat{a_1}, \hat{b_3}) + E(\hat{a_3}, \hat{b_1}) + E(\hat{a_3}, \hat{b_3}) = -2\sqrt{2} \tag{1.4}$$

ou seja, a mecânica quântica viola a desigualdade de CHSH, a qual no diz $\|C\| \leq 2$.

Através de um canal público, Alice e Bob transmitem seus eixos de escolha das medições realizadas. Então eles tornam público os resultados em que seus eixos de medição não foram iguais. Assim, é possível que Alice e Bob verifiquem a igualdade acima. Caso

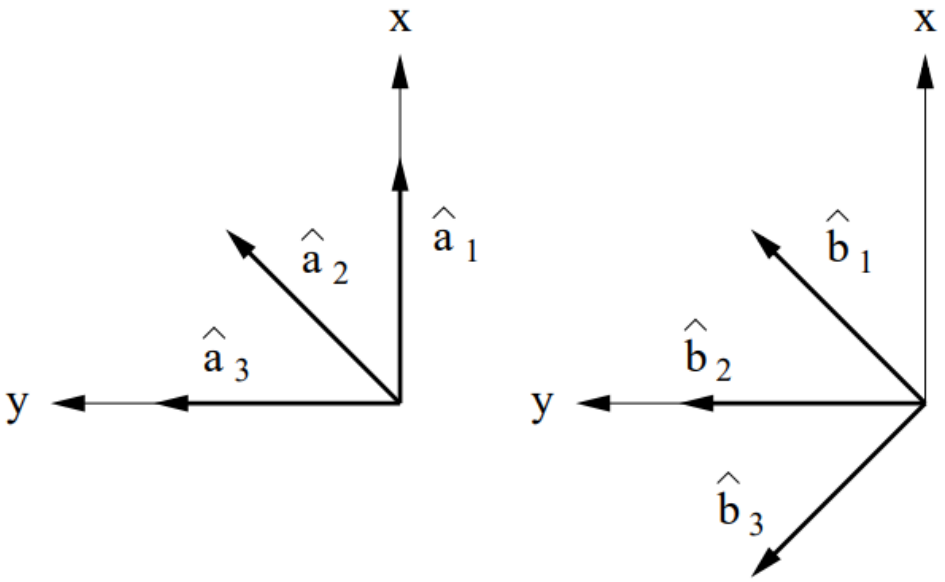

Figura 1.3: Direções dos eixos de medições de Alice (esquerda) e Bob (direita)(BENENTI, 2004).

$C > -2\sqrt{2}$, então o espião atacou o par EPR ou houve efeitos de ruído. Caso tais efeitos não estejam presentes, as medições de Alice e Bob estão perfeitamente anticorrelacionadas,

$$E(\hat{a}_2, \hat{b}_1) = E(\hat{a}_3, \hat{b}_2) = -1 \tag{1.5}$$

Com os resultados dessas medições são as *raw key* compartilhadas entre Alice e Bob. Note que, as chave concordam quando Bob nega suas saídas $0 \to 1$ e $1 \to 0$.

Por simplicidade, Alice e Bob podem realizar medições nos eixos x ou z, de forma que a decisão do eixo escolhido seja aleatória em que cada escolha tenha probabilidade $\frac{1}{2}$. Após as medições, Alice e Bob transmitem, através de um canal público, qual observável foi medido para cada par EPR. Caso os eixos de medição sejam os mesmo, os resultados são perfeitamente anticorrelacionados. Após isso, Alice e Bob descartam os outros resultados que não coincidem e geram a chave de uso único. O restante do procedimento segue o mesmo do protocolo BB84.

Vale notar que a chave só é gerada após as medições de Alice e Bob, logo, a chave secreta surge por um processo fundamentalmente aleatório. Sendo assim, o protocolo E91 é interessante para armazenamento de chaves, no entanto, o problema de sua segurança se estabelece justamente no armazenamento. Uma vez que Alice e Bob geram a chave secreta, ela é guardada em um cofre até que possa ser utilizada. Mas, a chave é uma *string* de bits clássicos, ou seja, pode ser clonada. Mesmo que seja muito difícil violar o cofre, não é impossível.

1.4 Teorema da Não-Clonagem

O teorema da Não-Clonagem [11] estabelece que é impossível para qualquer dispositivo receber um estado quântico desconhecido e arbitrário como entrada e reproduzir exatamente o mesmo estado e uma cópia dele como saída. Para a prova, segue que, supondo que exista uma máquina quântica capaz de copiar um estado qualquer [12]

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.6}$$

O resultado possível é

$$M|0\rangle|\phi\rangle = |\phi\rangle|\phi\rangle \tag{1.7}$$

Então:

$$M|0\rangle|\phi\rangle = M|0\rangle(\alpha|0\rangle + \beta|1\rangle) = M(\alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle) \tag{1.8}$$

Na mecânica quântica, M deve ser um operador linear, de tal forma que

$$M(\alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle) = \alpha M|0\rangle|0\rangle + \beta M|0\rangle|1\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \neq |\phi\rangle|\phi\rangle \tag{1.9}$$

Logo, a cópia não é idêntica ao estado original.

CAPÍTULO 2

Perfil Transversal de Fótons Únicos

Por conta da da natureza binária, protocolos de sistemas quânticos de dois níveis são a melhor escolha para a implementação da QKD. Mas a taxa geral de distribuição de chaves é limitada devido a transmissão de informação por fóton $I \leq 0.5 qubits/fóton$.

Uma das maneiras de aumentar a taxa de transmissão de chaves é utilizando sistemas de dimensões maiores para o envio das informações. Trazendo qubits d-dimensionais (qudits) acaba melhorando a taxa de transmissão de informação sendo $I = \log_2 \frac{d}{2} bits/qudit$ [13]. O uso de sistemas de maiores dimensões é vantajoso, pois a segurança do protocolo também aumenta devido a possibilidade de interferência de um qudit é menor dentro do espaço amostral maior.

O aumento da segurança pode ser alcançado utilizando de variáveis continuas e discretas no sistema. As informações podem ser codificadas tanto na polarização quanto no perfil transversal do feixe. Podemos escrever a amplitude complexa do componente elétrico de um campo eletromagnético como sendo:

$$\vec{E}(x, y, z) = A(x, y, z)\vec{\varepsilon}e^{-ikz} \tag{2.1}$$

onde $k = \frac{2\pi}{\lambda}$ é o número de onda, o envelope complexo é $A(x, y, z)$ e $\vec{\epsilon}$ é o vetor de polarização. Lasers monocromáticos tem como característica serem bem colimados, por isso divergem pouco a medida que se propagam [14]. Portanto, podemos fazer uma aproximação (Aproximação Paraxial de Helmholtz) para um feixe se propagando na direção $\hat{z}$:

$$\left|\frac{\partial\psi(\vec{r})}{\partial z^2}\right| \ll \left|\frac{\partial^2\psi(\vec{r})}{\partial x^2}\right|, \left|\frac{\partial^2\psi(\vec{r})}{\partial y^2}\right|, \left|\frac{\partial\psi(\vec{r})}{\partial z}\right| \tag{2.2}$$

onde $\psi(\vec{r})$ é a função que determina a estrutura transversal do feixe. Utilizando está aproximação na Equação de Helmholtz, temos que:

$$\frac{i}{k}\frac{\partial}{\partial z}A = -\frac{1}{2k^2}\left(\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}\right)A - \frac{1}{n_0}\Delta n(x,y)A \tag{2.3}$$

A equação deve ser satisfeita assumindo que meu envelope complexo do feixe varia lentamente em respeito a z, sendo que as posições x e y são transversais à propagação. A equação acima possui certas similaridades com a equação de Schrödinger bidimensional $\left(-\frac{\hbar^2}{2m}\nabla^2\psi(\vec{r},t)+V(\vec{r},t)\psi(\vec{r},t) = -i\hbar\frac{\partial\psi(\vec{r},t)}{\partial t}\right)$ considerada para um campo complexo monocromático o qual se propaga em um meio que possui índice de refração n_0 e flutuações Δn. Para o caso de propagação livre, não há flutuação, então o termo direto da equação some.

A relação entre os observáveis do sistema é dado por:

$$[\hat{s},\hat{p}] = i\hbar \tag{2.4}$$

onde a variável s representa o vetor posição no plano x-y.

Dessa forma, Alice pode enviar um caractere escolhendo entre as bases {H, V} ou {D, A} e também das bases de posição e momento transversal { s, p}. O caractere será determinado pela abertura no plano transversal. A base de posição ou momento é definida ao transmitir a imagem da abertura para o plano de detecção (posição) ou o momento linear $\hat{p}$ do fóton.

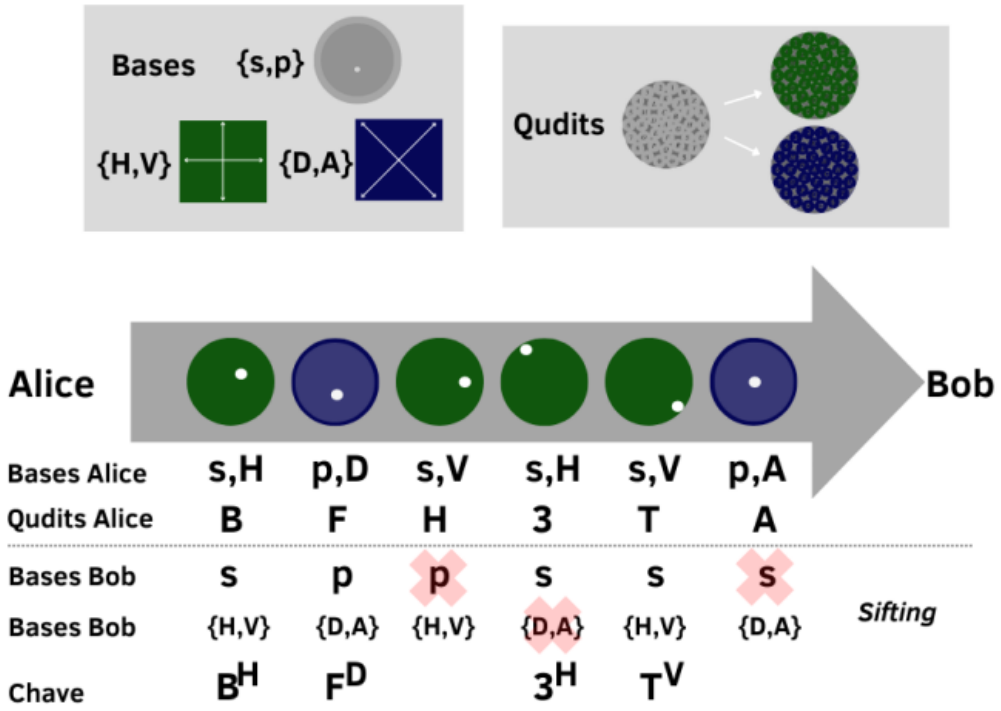

Figura 2.1: Esquema experimental proposto em (FERRO, 2023)

Considerando um sistema onde as bases contínuas de posição e momento {s, p}

e as bases discretas de polarização {H, V},{D, A}. Alice deve escolher aleatoriamente uma base contínua e uma discreta para codificar sua informação através de um qudit d-dimensional e um bit de polarização. Dessa forma, Alice tem 4 informações, a base contínua, a base discreta, a polarização e o caractere. Alice envia o fóton para Bob pelo canal escolhido e Bob deve escolher aleatoriamente uma base contínua e discreta para efetuar as medições.

A partir dessa configuração, temos 5 casos possíveis. No primeiro caso, há a troca básica de informações, as bases de Alice e Bob combinam, assim como seus qudits e qubits. Não há perturbação e sem detecção de espião.

No segundo caso, há um erro onde as bases contínuas de Alice e Bob não coincidem, logo o qudit é descartado. Existe ainda a possibilidade de testar a segurança do sistema mantendo um qudit de polarização a fim de detectar pertubações no sistema, um esforço útil, uma vez que parte da string descartada é utilizada como reforço.

No terceiro caso, as bases de Alice e Bob coincidem, mas os qudit não, portanto, houve distúrbio no sistema indicando um possível ataque do espião.

No quarto caso, semelhante ao anterior, as bases de polarização coincidem, mas os qudits de polarização não. Visto que é um possível ataque ao sistema, o qudit é descartado.

No quinto caso, há uma forte pertubação no sistemas, pois as bases de Alice e Bob coincidem, mas os qudits e suas bases de polarização não. O qudit é descartado.

Tendo um feixe de fótons paraxial e monocromático como sistema físico onde o estado quântico é expandido nas bases de polarização e variáveis continuas, o plano inicial do estado pode ser escrito da seguinte maneira:

$$|\Psi\rangle = \int v(s)|s\rangle|H\rangle ds \tag{2.5}$$

sendo s a componente transversal do vetor de onda k e H é a polarização horizontal do feixe. O espectro angular $v(s)$ é dado por:

$$v(s) = \frac{1}{2\pi}\int u(p,0)e^{-is}pdp \tag{2.6}$$

para $z = 0$ e $s = (x, y)$ (plano inicial) o envelope complexo do campo elétrico no é denotado por $u(p, 0)$.

A amplitude do campo no plano de saída, de acordo com [15] é

$$\mathcal{A}_{FF}(p) = \frac{\varepsilon k^2}{2f_c f}u(p,0) \tag{2.7}$$

$$\mathcal{A}_{II}(p) = \frac{\varepsilon k^3}{f_c f^2}u(-p,0) \tag{2.8}$$

$$\mathcal{A}_{IF}(p) = \frac{\varepsilon k^3}{2f_c f^2} v(\frac{k}{2f}p) \tag{2.9}$$

$$\mathcal{A}_{FI}(p) = \frac{\varepsilon k^3}{2f_c f^2} v(\frac{k}{2f}p) \tag{2.10}$$

onde ε é uma constante, k a magnitude do vetor de onda e f_j é o tamanho focal das N lentes.

Através das equações acima, Alice codifica as informações a serem enviadas para Bob posicionando a abertura em uma determinada posição de forma que a abertura corresponda ao caractere no alfabeto d-dimensional [15]. Neste caso o espião pode ser identificado mesmo ao medir na base contínua correta. Caso Eve escolha a base contínua errada com uma chance $1 - 1/d$, há uma chance de $1/2$ de escolher a base de polarização errada, o que nos da $1 - 1/2d$ chance de erro na medição do espião.

Para o ataque do tipo intercept-resend em um esquema onde todos os caracteres $(2d)$ possuem a mesma probabilidade de detecção, a taxa de erro para os fótons interceptados é

$$E = \frac{1}{4}\left(1 - \frac{1}{2d}\right) + \frac{1}{4}\left(1 - \frac{1}{2}\right) + \frac{1}{4}\left(1 - \frac{1}{d}\right) \tag{2.11}$$

onde, o primeiro termo corresponde a Eve quando mede nas duas bases errada, o segundo se refere a medição errada somente da base de polarização, e o terceiro termo é devido a medição somente da base espacial.

2.1 Informações Propagadas

Supondo que Alice manda cada caractere m com probabilidade P_m, que podemos definir como

$$P_m = \frac{1}{2}\int u(p - p_A)\mathcal{A}_{FI}(p)dp \tag{2.12}$$

onde a função $\mathcal{A}_{FI}(p)$ é a transformada de Fourier da função $u(p - p_A)$, sendo a variável p_A a posição do círculo no perfil transversal no plano de Alice.

A quantidade total de informação I_A que Alice pode codificar em cada fóton [16] é dada por:

$$I_A = -\sum_{m=0}^{2d-2} P_m \log_2 P_m \tag{2.13}$$

sendo d o número de círculos no plano transversal, logo, $2d$ representa o número de caracteres do alfabeto. P_m é a probabilidade de Alice enviar um determinado caractere m.

A quantidade de informação que Alice pode enviar para Bob na presença de ruído e erros [16] é

$$I_{AB} = H_i - H_f \tag{2.14}$$

A probabilidade $P(m \mid m)$ depende unicamente da taxa de erro, $P = (m \mid m) = 1 - \varepsilon_k$ por outro lado, a probabilidade $P(n \mid m) = \frac{P_m \varepsilon_n}{1-P_n}$, onde a probabilidade de detectar um caractere m incorreto dado que um erro tenha ocorrido é $\frac{P_m}{1-P_n}$. Assim, a quantidade de informação que Alice transmite a Bob na presença de ruído ou de um espião é [17]

$$I_{AB} = I_A + \sum_{0}^{2d-2} P_m(1-\epsilon_m)\log_2(1-\epsilon_m) + \sum_{n=0}^{2d-2}\sum_{m=0,n\neq m}^{2d-2} \frac{P_n\epsilon_n P_m}{1-P_n}\log_2\frac{\epsilon_n P_m}{1-P_n} \tag{2.15}$$

2.2 Ataque Intercept-Resend

Existem diferentes estrategias básicas de ataque do espião. A informação mutua entre Alice e Bob depende de uma taxa de erro ϵ_m, logo, o objetivo de Eve é obter uma grande quantidade de informação (I_E) sem induzir uma alta taxa de erro ϵ_m a qual pode ser detectado por Alice e Bob.

No ataque tipo intercept-resend, Eve faz sua medição usando a mesma configuração que Alice e Bob. Portanto, metade das vezes Eve mede corretamente a posição de abertura, e metade da vezes terá apenas pequenas informações. A taxa de erro é

$$\epsilon_m = \frac{\alpha}{4}(1-P_m) + \frac{\alpha}{4}(1-1/2) + \frac{\alpha}{4}(1-2P_m) \tag{2.16}$$

sendo α a fração de fótons que Eve mede e P_m a probabilidade de medir o caractere m. O campo de entrada ´para uma abertura na posição p_j dada por uma função gaussiana é equivalente à função de abertura

$$u(p-p_j,0) = \frac{1}{w\sqrt{\pi}} exp\left[-\frac{|p^2+p_j^2|}{2w^2}\right] \tag{2.17}$$

Como descrito anteriormente, Eve obtém poucas informações quando mede na base errado, mas 1/4 dos fótons interceptados lhe dão a informação correta e assim Eve permanece indetectável. A quantidade de informação obtida por Eve é

$$I_E = -\frac{\alpha}{4}\sum_{m=0}^{2d-2} P_m \log_2 P_m \tag{2.18}$$

A física quântica contribui para a segurança destes protocolos, no entanto, o espião pode ir além do canal quântico. Existem outras formas de ataques que focam na fragilidade do sistema de envio e detecção da mensagem [18–20].

2.3 Ataque Cavalo de Troia

O canal quântico oferece uma transmissão de sistema quânticos isolados do mundo exterior ao ponto de que o receptor recebe a mensagem praticamente sem pertubação. Como descrito anteriormente, a segurança dos protocolos é garantida, em particular, pelo teorema da não clonagem [11], no entanto, a física quântica não garante a segurança dos aparatos de Alice e Bob. Os equipamentos eletrônicos utilizados nos experimentos são protegidos por meios clássicos. Neste ponto é que um ataque fora do canal de comunicação quântico toma relevância.

O canal quântico em si pode ser uma potencial porta de entrada para o espião interferir nos aparatos de Alice e Bob [18]. Eve pode aproveitar o curto período de tempo em que o canal quântico é aberto (tempo em que potencialmente há informações relevantes) para mandar um pulso de luz para os aparatos de Alice e/ou Bob. Dessa forma, caso Alice se descuide, Eve pode descobrir exatamente em qual estado quântico ela preparou e acessou a chave. Mas Alice pode ter cuidado suficiente para limitar a informação e elimina-la através da ampliação de privacidade. Este tipo de ataque é conhecido como Cavalo de Troia.

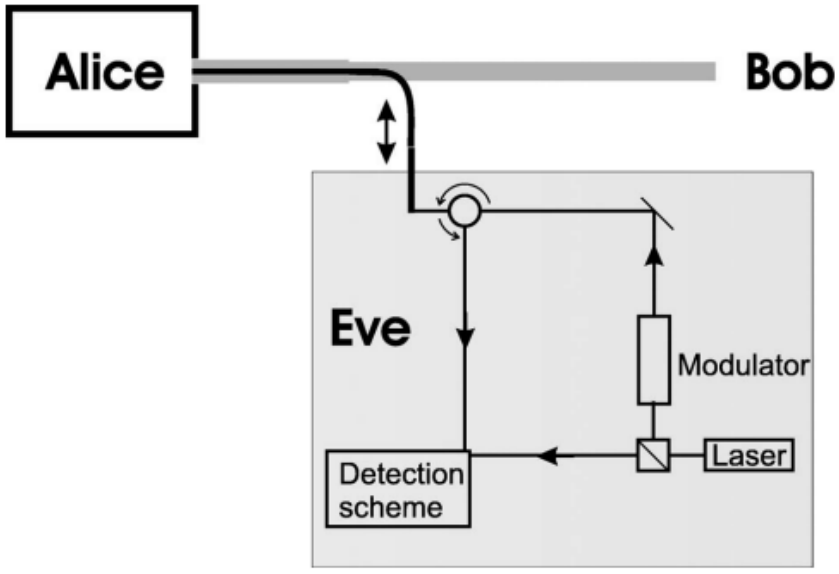

Figura 2.2: Esquema do principio do ataque do cavalo de troia. Eve ocupa parte do canal quântico, espacialmente, temporalmente e pelos modos de frequência para interceptar o aparato de Alice. Eve usa de um fonte para modular e analisa o retroespalhamento do sinal com um detector(GISIN, 2006).

Grande parte das implementações de QKD, são realizadas por fibra óptica, ou seja, diferentes sistemas de componentes são conectados. Idealmente toda a luz de *input* é perfeitamente transmitida para o *output*. Contudo, em um cenário real, enquanto a luz viaja pela interface ou dentro de um componente, uma porção da luz é refletida ou

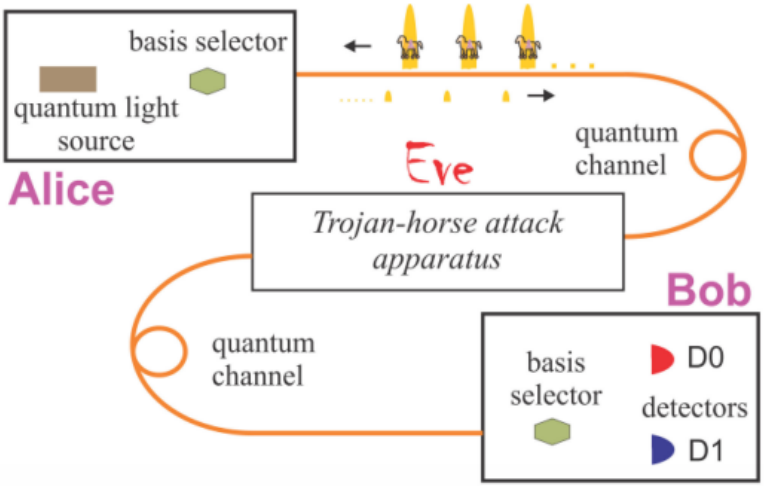

Figura 2.3: Esquema experimental do ataque cavalo de troia. Eve ataca Alice enviando pulsos luminosos para ter ciência das bases escolhidas por Alice durante o protocolo QKD.(JAIN, NITIN et al. 2014)

espalhada. A quantidade de luz refletida ou espalhada depende do comprimento de onda e intensidade da luz de entrada.

Um pulso de luz emitido por Eve pelo canal quântico no subsistema QKD, Alice, encontrará diversas reflexões e espalhamentos. Um fluxo de reflexões podem ser propagados do dispositivo de Alice do canal quântico. Eve precisa analisar cuidadosamente a luz retro-refletida para então conseguir adquirir informações sobre as propriedades de funcionamento do aparato de Alice [21].

No entanto, para realizar a amplificação de privacidade, Alice e Bob precisam saber um limite para a informação do espião, no entanto, a amplificação reduz a taxa da chave secreta. O objetivo então é encontrar o limite de informação de Eve para que seja o menor possível.

A fim de evitar estes ataques o sistema pode ser construído de forma que:

- Somente a luz em um determinado comprimento de onda passe;
- A fenda deve se abrir por curtos períodos de tempo, ou seja, os componentes de codificação devem ser ativados por pouco tempo ativando um modulador de fase somente quando o qubit está lá;
- A quantidade de luz refletida deve ser limitada para um valor conhecido.

Para ter ciência das informações de Eve, e quantificar o quanto de informação Eve pode extrair de um estado fracamente coerente quando ela sabe a base, façamos uma analise.

2.3.1 Ganho de Informação do Espião

Por conta do componente de vácuo do estado fracamente coerente, os estados correspondentes da base não são ortogonais. Grande parte dos protocolos de QKD são apresentados com qubits abstratos sendo preparados em diferentes bases, mas a maioria das implementações usam pulsos de laser fracos. Os estados de qubits $|0_L\rangle$ e $|1_L\rangle$ podem ter dois modos: $|0_L\rangle = |\alpha\rangle \otimes |0\rangle$ e $|1_L\rangle = |0\rangle \otimes |\alpha\rangle$. Logo, Eve deve diferenciar entre os dois estados $|\alpha\rangle \otimes |0\rangle$ e $|0\rangle \otimes |\alpha\rangle$. A mensuração que maximiza o ganho de informação do espião [22] é:

$$I_{Eve}^{Troia}\left(|\alpha|^2\right) = 1 - H(p) \tag{2.19}$$

onde

$$p = \frac{1}{2}\left(1 + \sqrt{1 - |\langle \alpha, 0|0, \alpha\rangle|^2}\right) \tag{2.20}$$

$$= \frac{1}{2}\left(1 + \sqrt{1 - exp(-2)|\alpha|^2}\right) \tag{2.21}$$

$$\approx \frac{1 + \sqrt{2}|\alpha|^2}{2} \tag{2.22}$$

H denota a entropia binaria. Como:

$$I_{Eve}^{Troia}(|\alpha|^2) = \frac{1}{\ln(2)}|\alpha|^2 + O(|\alpha|^4) \tag{2.23}$$

2.3.2 Redução de Informação do Espião

A figura 2.2 nos mostra como o espião pode sondar o aparato de Alice e/ou Bob, para ganha o máximo de informação possível sobre as configurações do protocolo. Devido ao poder de ganho de informação de Eve, Alice e Bob precisam abrir mão de uma fração significante da *raw key* antes de obter a chave secreta. Para encontrar o limite de Eve, Alice ou Bob podem escolher aleatoriamente a fase de $|\alpha\rangle$ relativa ao referencial de Eve. Dessa forma Eve não possui mais $|\alpha, 0\rangle$ ou $|0, \alpha\rangle$, dependendo do aparato utilizado no experimento, mas agora possui estados misto ρ_0 ou ρ_1, respectivamente, sendo:

$$\rho_0 = \int_0^{2\pi} \frac{d\theta}{2\pi} |e^{i\theta}\alpha, 0\rangle\langle e^{i\theta}\alpha, 0|, \tag{2.24}$$

$$= \sum_{n\geq} P\left(n|\alpha|^2\right) |n, 0\rangle\langle, 0|, \tag{2.25}$$

$$\rho_1 = \int_0^{2\pi} \frac{d\theta}{2\pi} |0, e^{i\theta}\alpha\rangle\langle 0, e^{i\theta}\alpha|, \tag{2.26}$$

$$= \sum_{n\geq} P\left(n|\alpha|^2\right)|0,n\rangle\langle 0,n| \tag{2.27}$$

onde $P\left(n|\alpha|^2\right) = \left(\frac{|\alpha|^{2n}}{n!}\right)e^{-|\alpha|^2}$ é a probabilidade da distribuição de Poisson. Inicialmente, Eve faz a medição do número do fóton, caso nenhum fóton seja encontrado, não há ganho algum de informação. Caso contrário, quando um ou mais fóton são encontrados, Eve tem toda a informação. A informação ganha é igual a probabilidade de um estado fracamente coerente α não estar vazio:

$$I_{Eve}^{reduzido}(|\alpha|^2) = 1 - P(0|\alpha|^2) = 1 - exp\left(-|\alpha|^2\right) \approx |\alpha|^2 \tag{2.28}$$

Veja que $I_{Eve}^{reduzido}(|\alpha|^2) < I_{Eve}^{Troia}(|\alpha|^2)$. É importante também que Alice e Bob incrementem em seu protocolo a adição de fase aleatórias para qualquer luz que possa ser retroespalhada [23]. Vale reforçar que as fases aleatórias são como fases globais irrelevantes no qubit, não afetando propriamente o protocolo de QKD, mas são relativas a qualquer possibilidade de referencias que Eve possua.

CAPÍTULO 3

Implementações Experimentais

A seguir, vamos descrever a implementação experimental desenvolvida tanto em [15] quanto em [2] usada para o estudo da distribuição de fótons enviados por Alice para Bob usando protocolo QKD descrito anteriormente.

3.1 WALBORN et al. 2006

No esquema experimental proposto por Walborn, Alice codifica suas informações posicionando a abertura da fenda no plano P_{Ain}, sendo assim, cada posição da abertura $\mathbf{p}_d$ corresponde a um caractere no alfabeto d-dimensional, como é ilustrado na figura 3.1. Se Alice e Bob escolhem a mesma configuração de lentes, as amplitudes de detecções de Bob vão ter a mesma função de abertura e Bob terá medido o caractere correto.

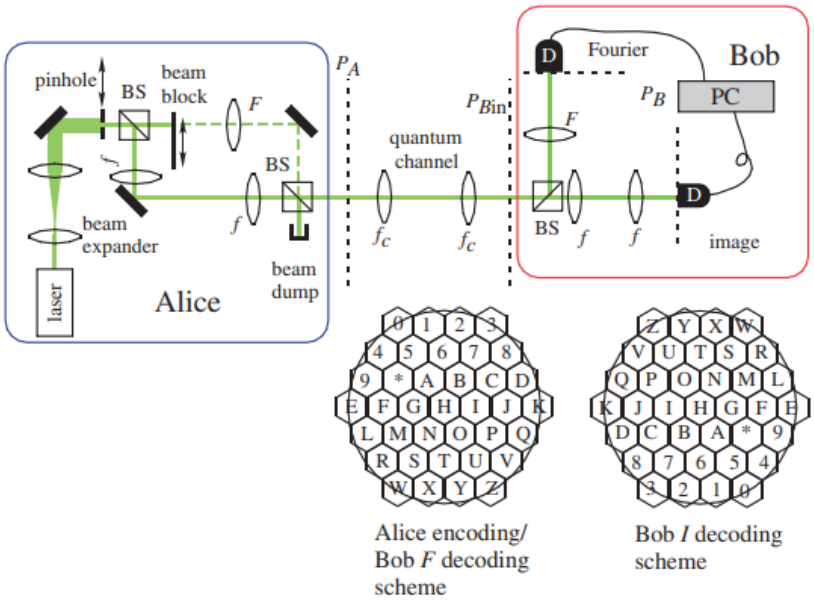

Figura 3.1: Esquema da demonstração experimental(WALBORN et al. 2006).

O experimento foi realizado com o uso de um feixe laser atenuado, o qual não possui termos multifótons presentes, podendo ser aproximado para um estado de fóton único [17].

Usando um Beam Splitter (BS), Bob escolhe aleatoriamente entre imagem e o sistema de Fourier, sendo que seus sistemas óticos são iguais aos usado por Alice. A dimensão d do alfabeto utilizado é determinado pelo tamanho da abertura $A(p)$ e da transformada de Fourier. Alice e Bob devem decidir a melhor forma de configurar as posições no plano transversal P_{Ain} e P_B (abertura de Alice e o detector de Bob, respectivamente) que implicam em seus caracteres do alfabeto.

3.2 FERRO et al. 2023

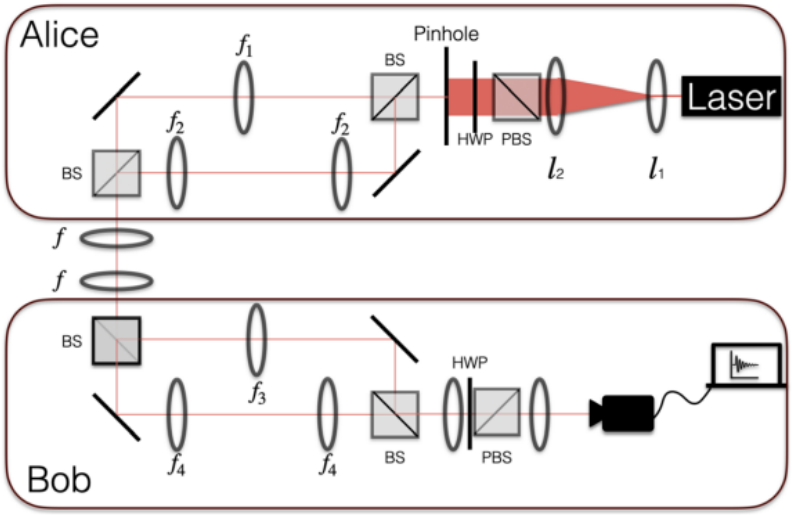

Figura 3.2: Esquema experimental proposto em (FERRO et al. 2023).

O esquema proposto em [2] é semelhante ao descrito anteriormente no protocolo de Walbron, mas aqui é considerado um número maior de caracteres e o uso de variáveis discretas e contínuas. As primeiras lentes mostradas no esquema são para ampliar o feixe de laser de forma que a intensidade com que ele chega em cada caractere de codificação (ver figura 3.3) seja a mesma. O primeiro divisor de feixe BS certifica que a polarização esteja bem definida, assim a polarização do feixe de laser possa ser modificada posteriormente pelo prato de meia onda Half-Wave Plate (HWP).

A fenda é posicionada no plano x-y a uma certa distância do centro do feixe inicial de luz de forma que a posição transversal implica dois diferentes caracteres. Então Alice escolhe aleatoriamente usar a base de posição ou momento para codificar a informação. Da mesma foram, ela ainda escolhe aleatoriamente a base de polarização, onde posiciona o prato de onda em 0° ou 45° para {H, V} e +22.5° ou −22.5° para {D, A}. Para a base de posição, Alice usa um sistemas de lentes que vão gravar a imagem da fenda no plano

de entrada de Bob. Para a codificação pelo momento, Alice usa um sistema de lentes para implementar a transformada de Fourier do orifício do plano de entrada de Bob. Note que, ao Alice escolher aleatoriamente a sua base de posição ou momento através das lentes f_4 e f_3, respectivamente, ela bloqueia um dos braços do interferômetro, assim como Bob ao fazer a medição usando um sistema de lentes semelhante (f_2 e f_1), como é possível observar através da figura 3.2.

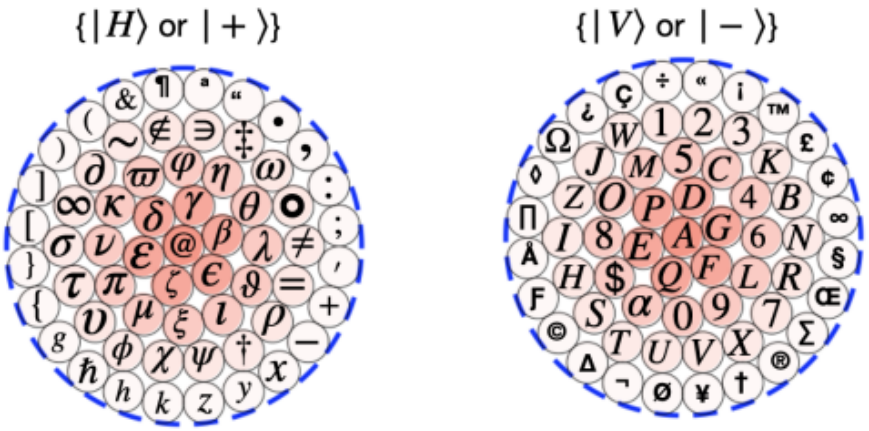

Figura 3.3: Os círculos pequenos em branco representam as posições no plano de Alice. O círculo grande em cinza representa a transformada de Fourier dos círculos pequenos(FERRO, 2023).

O procedimento para Bob vai ocorrer de forma similar para a escolha de cada base contínua. Caso Bob faça suas medições na mesma base continua que Alice, ele encontrará a posição do orifício. No entanto, ele ainda precisa que suas medições no estado de polarização tenham todas as informações enviadas por Alice. Para que isso seja possível, um sistema realiza uma tomografia na polarização do estado utilizando o sistema de HWP e o divisor de feixes polarizados Polorized Beam Splitter (PBS).

Aqui, a taxa entre a largura da função Gaussiana que representa a transformada de Fourier do orifício e a largura da função Gaussiana que representa o orifício em si é 26. Assim, de acordo com [24] é possível descrever até 547 caracteres sem interferência.

Para cada configuração escolhida por Alice, o receptor, seja ele Bob ou Eve, tem somente uma única combinação de bases que leva ao caractere correto. O ganho energético deste protocolo se mostra 33% mais eficiente em relação ao protocolo desenvolvido em [15], mostrando assim a melhora significativa no envio e segurança ao utilizar um números de caracteres maior assim como o uso das variáveis contínuas e discretas.

CAPÍTULO 4

Conclusões

A distribuição quântica de chaves é um método seguro de implementação de um protocolo envolvendo a mecânica quântica. É possível ter uma chave secreta compartilhada entre remetente e receptor, onde esta chave somente é conhecida entre os envolvidos que utilizaram da mecânica quântica para codificar e decodificar a mensagem. Na discussão trazida neste trabalho, evidencia-se a impressionante capacidade de codificação e decodificação que os estudos e implementações experimentais dessa área possuem. Através dos protocolos aqui citados, como a grande referência da área impressionante trabalho o BB84 [5] e E91 [6] até os estudos avançados envolvendo um esquema de alfabeto d-dimensional usando graus de liberdade espaciais de fótons [15] e um protocolo alternativo utilizando de variáveis híbridas contínuas e discretas de fótons únicos [2].

Apesar dos grandes avanços da área, uma das dificuldades que persistem é a transmissão de informação pelo espaço livre [17, 25, 26]. Apesar das dificuldade, o envio de fótons pela atmosfera pode implicar em algumas vantagens, visto que o meio não é essencialmente birrefringente [17] o que torna possível o uso de um plano de codificação de polarização. Uma das maneiras de contornar a limitação da distância em protocolos QKD é o uso de nós confiáveis [26]. Mas para atingir grandes distâncias é necessários muitos nós. Logo, outra possível solução é a implementação de satélites, os quais podem servir como nós confiáveis e não confiáveis, vendo assim, o satélite como um "correio"confiável que possa realizar a QKD assim como viajar rapidamente em uma determinada orbita.

Há ainda a possibilidade de continuidade de estudo do protocolo descrito neste trabalho, uma vez que o ataque Cavalo de Troia é um ótimo meio de testar e aumentar a segurança do sistema. Este tipo de ataque é especialmente perigoso para sistemas de fóton único, assim como para sistemas *plug-and-play* [27] onde a quantidade de luz refletida é mais do que a maioria dos sistemas alternativos.

Vemos então como a criptografia quântica é um campo com grande potencial que vem crescendo a cada ano, e ilustra bem a relação entre conceitos básicos e aplicados da física, combinando conceitos da física quântica e teoria da informação e trazendo grandes possibilidades de progresso para a óptica quântica.

CAPÍTULO 5

Perspectivas

Em razão do curto período de tempo em que este trabalho foi desenvolvido, não foi possível a implementação de diferentes métodos de ataque, principalmente um ataque que leve em conta a fragilidade da transmissão e detecção da mensagem [18–20, 28], ou seja, um ataque fora do canal quântico, o que mostrar interessante visto que, poderá testar o quão bom é a segurança do protocolo desenvolvido em [2].

Sugere-se um estudo mais detalhado sobre protocolos focados em novos ataques de espionagem e até a mesmo a implementação experimental destes ataque, como por exemplo o cavalo de troia [18], uma vez que este tipo de ataque se mostra perigoso para sistemas de fótons únicos. Implementando contra medidas através de filtros e tempos de abertura cuidadosamente estabelecidos.

A necessidade de proteger a mensagem vai além do reforço no canal quântico, mas também a preocupação com os aparatos experimentais protegidos por meios clássicos. A precisão do monitoramento de detecção estabelece a quantidade de amplificação de privacidade deve ser realizada para que este tipo de ataque seja evitado.

Referências Bibliográficas

[1] STIX, G. Best-kept secrets. **Scientific American**, JSTOR, v. 292, n. 1, p. 78–83, 2005. Citado na página 14.

[2] FERRO, L. F. et al. Single photon hybrid quantum key distribution. **Physica Scripta**, 2023. Citado 5 vezes nas páginas 14, 29, 30, 32 e 33.

[3] NIELSEN, M. A.; CHUANG, I. L. **Quantum computation and quantum information**. [S.l.]: Cambridge university press, 2010. Citado na página 15.

[4] WIESNER, S. Conjugate coding. **ACM Sigact News**, ACM New York, NY, USA, v. 15, n. 1, p. 78–88, 1983. Citado na página 15.

[5] BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. **Theoretical computer science**, Elsevier, v. 560, p. 7–11, 2014. Citado 2 vezes nas páginas 15 e 32.

[6] EKERT, A. K. Quantum cryptography based on bell's theorem. **Physical review letters**, APS, v. 67, n. 6, p. 661, 1991. Citado 3 vezes nas páginas 15, 17 e 32.

[7] CLAUSER, J. F. et al. Proposed experiment to test local hidden-variable theories. **Physical review letters**, APS, v. 23, n. 15, p. 880, 1969. Citado na página 15.

[8] JIRAKITPUWAPAT, W. et al. A quantum key distribution on qudits using quantum operators. **Mathematical Methods in the Applied Sciences**, Wiley Online Library, v. 46, n. 15, p. 15924–15939, 2023. Citado na página 15.

[9] ASPECT, A.; GRANGIER, P.; ROGER, G. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. **Physical review letters**, APS, v. 49, n. 2, p. 91, 1982. Citado na página 17.

[10] BENENTI, G.; CASATI, G.; STRINI, G. **Principles of quantum computation and information-volume I: Basic concepts**. [S.l.]: World scientific, 2004. Citado na página 17.

[11] WOOTTERS, W. K.; ZUREK, W. H. A single quantum cannot be cloned. **Nature**, Nature Publishing Group UK London, v. 299, n. 5886, p. 802–803, 1982. Citado 2 vezes nas páginas 19 e 25.

[12] ALMEIDA, N. G. **Introdução à Computação e Informação Quântica Incluindo Álgebra Linear com Kets e Bras**. [S.l.]: Livraria da Física, 2020. v. 1. Citado na página 19.

[13] TENTRUP, T. B. H. et al. Large-alphabet quantum key distribution using spatially encoded light. **New journal of physics**, IOP Publishing, v. 21, n. 12, p. 123044, 2019. Citado na página 20.

[14] SALEH, B. E.; TEICH, M. C. **Fundamentals of photonics**. [S.l.]: john Wiley & sons, 2019. Citado na página 20.

[15] WALBORN, S. et al. Quantum key distribution with higher-order alphabets using spatially encoded qudits. **Physical review letters**, APS, v. 96, n. 9, p. 090501, 2006. Citado 5 vezes nas páginas 22, 23, 29, 31 e 32.

[16] WALBORN, S. et al. Schemes for quantum key distribution with higher-order alphabets using single-photon fractional fourier optics. **Physical Review A**, APS, v. 77, n. 6, p. 062323, 2008. Citado 2 vezes nas páginas 23 e 24.

[17] GISIN, N. et al. Quantum cryptography. **Reviews of modern physics**, APS, v. 74, n. 1, p. 145, 2002. Citado 4 vezes nas páginas 24, 30 e 32.

[18] GISIN, N. et al. Trojan-horse attacks on quantum-key-distribution systems. **Physical Review A**, APS, v. 73, n. 2, p. 022320, 2006. Citado 4 vezes nas páginas 24, 25 e 33.

[19] GERHARDT, I. et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. **Nature communications**, Nature Publishing Group UK London, v. 2, n. 1, p. 349, 2011. Citado na página 33.

[20] JAIN, N. et al. Trojan-horse attacks threaten the security of practical quantum cryptography. **New Journal of Physics**, IOP Publishing, v. 16, n. 12, p. 123030, 2014. Citado 2 vezes nas páginas 24 e 33.

[21] JAIN, N. et al. Risk analysis of trojan-horse attacks on practical quantum key distribution systems. **IEEE Journal of Selected Topics in Quantum Electronics**, IEEE, v. 21, n. 3, p. 168–177, 2014. Citado na página 26.

[22] PERES, A. **Quantum theory: concepts and methods**. [S.l.]: Springer, 1997. v. 72. Citado na página 27.

[23] LO, H.-K.; PRESKILL, J. Phase randomization improves the security of quantum key distribution. **arXiv preprint quant-ph/0504209**, 2005. Citado na página 28.

[24] GRAHAM, R. L. et al. Dense packings of congruent circles in a circle. **Discrete Mathematics**, Elsevier, v. 181, n. 1-3, p. 139–154, 1998. Citado na página 31.

[25] WALBORN, S. P. et al. Spatial correlations in parametric down-conversion. **Physics Reports**, Elsevier, v. 495, n. 4-5, p. 87–139, 2010. Nenhuma citação no texto.

[26] LO, H.-K.; CURTY, M.; TAMAKI, K. Secure quantum key distribution. **Nature Photonics**, Nature Publishing Group UK London, v. 8, n. 8, p. 595–604, 2014. Citado na página 32.

[27] MULLER, A. et al. "plug and play" systems for quantum cryptography. **Applied physics letters**, American Institute of Physics, v. 70, n. 7, p. 793–795, 1997. Citado na página 32.

[28] FEI, Y.-Y. et al. Quantum man-in-the-middle attack on the calibration process of quantum key distribution. **Scientific reports**, Nature Publishing Group UK London, v. 8, n. 1, p. 4283, 2018. Citado na página 33.