

Instituto Federal de Educação, Ciência e Tecnologia do Ceará

Departamento de Telemática

Programa de Pós-Graduação em Engenharia de Telecomunicações

Comunicação Quântica Segura Direta usando Distribuição Quântica de Chaves

RANARA LOUISE CAMPOS DAMASCENO

Fortaleza – Ceará
2017

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ

DEPARTAMENTO DE TELEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE
TELECOMUNICAÇÕES

Comunicação Quântica Segura Direta usando Distribuição Quântica de Chaves

Autora

RANARA LOUISE CAMPOS DAMASCENO

Orientador

RUBENS VIANA RAMOS

Dissertação submetida à Coordenação do Programa de Pós-Graduação em Engenharia de Telecomunicações como requisito parcial para a obtenção do título de Mestre em Engenharia de Telecomunicações na linha de pesquisa em Informação Quântica.

Fortaleza – Ceará

2017

Catálogo na fonte: Bibliotecário Jorge Macedo Lopes CRB-3/802

D155c Damasceno, Ranara Louise Campos

Comunicação quântica segura direta usando distribuição quântica de chaves / Ranara Louise Campos Damasceno. - Fortaleza: IFCE, 2017.

52 f.

Dissertação (Mestrado em Engenharia de Telecomunicações).

Orientador: Prof. Dr. Rubens Viana Ramos.

1. ENGENHARIA DE TELECOMUNICAÇÕES – DISSERTAÇÃO.
2. REDE DE TELECOMUNICAÇÃO. 3. FIBRA ÓPTICA. I. Título.

CDD 621.38275

Agradecimentos

À Deus, que na sua infinita bondade me guiou por caminhos que eu nunca ousei pensar trilhar.

À minha mãe (Juciara), que desde sempre me deu o exemplo do trabalho e da dignidade, além de ser a minha amiga e conselheira de todas as horas.

Ao meu marido (Glaucionor) que me apresentou ao mundo infinito de possibilidades que o estudo pode proporcionar e que me ajuda, há quase 10 anos, a superar com leveza e paciência os desafios que aparecem na vida.

À família maravilhosa que Deus me deu: meu padrasto Júnior e meus irmãos Luigi, Dara, Ana Luzia e Gabriel.

Ao Prof. Rubens Viana Ramos por ter confiado na minha capacidade, por ter me ajudado em todos os momentos, por me ajudar a concretizar a experiência de participar de um congresso internacional!

Aos amigos Geovan Guerra e Roterdan Abreu sem os quais teria sido muito mais difícil entender o universo da física quântica.

Ao Prof. Fábio Alencar por ter me ajudado nos primeiros passos no mundo quântico e Prof. Glendo de Freitas por ter me ajudado tantas vezes com os cálculos da graduação em engenharia e do mestrado em informação quântica.

Aos amigos do GIQ (UFC) pelos momentos agradáveis de descontração e trabalho.

E por fim, aos amigos e professores do PPGET (IFCE) pelos ensinamentos que completaram a minha formação, em especial aos Profs. Daniel Xavier e Glendo de Freitas.

Resumo

A evolução das redes de comunicações está pautada na garantia do sigilo dos dados que trafegam por ela. Atualmente este sigilo está baseado na complexidade matemática de fatorar números grandes em fatores primos que são utilizados nos algoritmos clássicos de encriptação de dados. O desenvolvimento do processamento quântico da informação visa, no que diz respeito às comunicações, a proposição e a realização prática de novos protocolos que sejam mais eficientes do que os implementados com base nos princípios da física clássica. A partir de uma revisão bibliográfica de quatro protocolos de distribuição quântica de chaves (BB84, B92, DPS-QKD e DQPS-QKD), bem como de dois protocolos de comunicação quântica segura direta (QSDC com “*One-Time Pad*” e QSDC com Autenticação usando Dois Estados não Ortogonais) foi possível propor o protocolo objeto deste trabalho. Neste sentido, esta dissertação propõe um sistema de fibra óptica que executa uma comunicação quântica segura direta sem o uso de estados emaranhados. O sistema proposto é baseado na distribuição quântica de chaves com deslocamento diferencial de fase em quadratura e apresenta como principal vantagem do protocolo a sua implementação com a tecnologia atual.

Abstract

The evolution of communications network is based on ensuring the confidentiality of data traveling through it. Currently, this confidentiality is based on mathematical complexity of factoring large prime numbers used in classical data encryption algorithms. The development of quantum information processing aims the proposition and the practical realization of new protocols more efficient than those implemented based on classical physics principle. From a literature review of four quantum key distribution protocols (BB84, B92, DPS-QKD and DQPS-QKD), as well as two quantum secure direct communication protocols (QSDC with One-Time Pad and QSDC with Authentication using Two Non-Orthogonal States) it was possible to propose the protocol object of this work. In this direction, this work shows an optical setup that runs a quantum secure direct communication protocol without using entangled states. The proposed system is based on differential quadrature phase-shift quantum key distribution. The main advantage of the present protocol is its implementation with today technology..

Índice de Figuras

Figura 1.1	Diagrama esquemático da criptografia	14
Figura 1.2	Esquema óptico para o protocolo BB84	16
Figura 1.3	Esquema óptico para o protocolo B92	17
Figura 1.4	Esquema óptico para DPS-QKD. (BS) Divisor de feixes, ($\emptyset_A$) Modulador de Fase de Alice	19
Figura 1.5	Esquema óptico para DQPS-QKD. (BS) Divisor de feixes, ($\emptyset_A$) Modulador de Fase de Alice, ($\emptyset_B$) Modulador de Fase de Bob	21
Figura 2.1	Ilustração de uma sequência genérica z . Os pontos pretos representam h_A^a , os cinzas representam h_A^e e os brancos representam y	32
Figura 2.2	Resumo do protocolo de comunicação quântica segura direta com autenticação	34
Figura 3.1	Esquema óptico para QSDC empregando dois DQPS-QKD	37
Figura 3.2	Esquema óptico para QSDC empregando dois DQPS-QKD e usando diversidade de polarização. Os PBS1,2,3 são divisores de feixe por polarização enquanto R é um rotacionador de polarização	46

Índice de Quadros

Quadro 1.1	Procedimento do BB84. (+) Base Linear, (×) Base Diagonal	17
Quadro 1.2	Procedimento do B92	18
Quadro 1.3	Codificação de Alice	22
Quadro 2.1	Resumo das incógnitas do PASSO 1	31
Quadro 2.2	Resumo das incógnitas do PASSO 2 ao PASSO 4	33
Quadro 3.1	Escolhas de Alice para enviar ‘00’	43
Quadro 3.2	Escolhas de Alice para enviar ‘11’	45

Lista de Abreviaturas

B92	Protocolo de distribuição quântica de chaves proposto por Charles Henry Bennet em 1992.
BB84	Protocolo de distribuição quântica de chaves proposto por Charles Henry Bennet e Gilles Brassard em 1984.
BS	Beam Splitter
DPS-QKD	Differential Phase-Shift Quantum Key Distribution
DQPS-QKD	Differential Quadrature Phase-Shift Quantum Key Distribution
EPR	Einstein-Podolsky-Rosen
PBS	Polarizing Beam Splitter
QKD	Quantum Key Distribution
QSDC	Quantum Secure Direct Communication
XOR	Exclusive OR

Sumário

Resumo	3
Abstract	4
Índice de Figuras	5
Índice de Quadros	6
Lista de Abreviaturas	7
Introdução	11
Capítulo 1 – Distribuição Quântica de Chaves	14
1.1 Introdução	14
1.2 Protocolo BB84	16
1.3 Protocolo B92	18
1.4 Estados Coerentes	20
1.5 Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase – DPS-QKD	21
1.6 Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase em Quadratura – DQPS-QKD	23
1.7 Conclusão	25
Capítulo 2 – Comunicação Quântica Segura Direta	27
2.1 Comunicação Quântica Segura Direta <i>versus</i> Distribuição Quântica de Chaves.	27
2.2 Protocolo de Comunicação Quântica Segura Direta com “ <i>One-Time Pad</i> ”	28
2.2.1 Descrição do Protocolo	28
2.2.2 Segurança do Protocolo	30
2.3 Protocolo de Comunicação Quântica Segura Direta com Autenticação Usando Dois Estados não Ortogonais	31
2.3.1 Protocolo de Comunicação Quântica Segura Direta com Autenticação	32
2.3.2 Análise de Segurança	36
a. Ataque do tipo Personificação	36
b. Ataque do tipo Intercepta-Reenvia	37
2.4 Conclusão	38
Capítulo 3 – Comunicação Quântica Segura Direta Usando Distribuição Quântica de Chaves	39

3.1 Esquema Óptico para Implementar QSDC usando DQPS-QKD	39
3.2 Análise da Probabilidade de Erros Causados por Eva	45
3.3 Conclusão	48
Capítulo 4 – Conclusões e Perspectivas de Trabalhos Futuros	50
4.1 Conclusões	50
4.2 Perspectivas de Trabalhos Futuros	51
Referências Bibliográficas	52

Introdução

Entre 2014 e 2015 o crescimento da internet no mundo foi de pouco mais de 10%, crescendo de 2,9 bilhões de pessoas com acesso à internet em 2014 para 3,2 bilhões em 2015 [1]. Junto com o crescimento da internet também cresceram as operações que são realizadas através dela como: transações financeiras (em 2015 foram realizadas 11,2 bilhões de transações bancárias no Brasil, um crescimento de 138% em relação às 4,7 bilhões de transações realizadas em 2014 [2]); *e-commerce* (o comércio eletrônico no Brasil apresentou crescimento de 15% no faturamento de 2015 – 41,3 bilhões – em relação a 2014 – 35,8 bilhões [3]); troca de informações secretas entre empresas; troca de informações militares; dentre outras.

O ponto mais relevante para o crescimento contínuo das redes de comunicações, nas quais a internet está inserida, é a garantia do sigilo dos dados que trafegam por elas, ou seja, elas devem garantir que mesmo sofrendo tentativas de espionagem de usuários não autorizados, os dados permanecerão seguros. Atualmente, para assegurar este sigilo nas comunicações são usados algoritmos de encriptação de dados cuja segurança é garantida pela complexidade matemática em fatorar números grandes em fatores primos.

Entretanto, depois que Peter Shor, matemático americano que trabalhava no Bell Labs, em 1994 descreveu um algoritmo de fatoração que, quando executado por um computador quântico, seria capaz de executar fatorações de números muito grandes num tempo muito inferior ao dos computadores clássicos, a segurança dos sistemas que utilizam autenticação por chave pública ficou seriamente comprometida [4].

Por outro lado, os esquemas de encriptação que utilizam protocolos do tipo “*one-time pad*”, aqueles em que as chaves são usadas apenas uma única vez, são considerados incondicionalmente seguros justamente porque os usuários devem manter um processo dinâmico de descarte da chave recém utilizada e de compartilhamento de uma nova chave [5]. Mas existe uma pergunta que precisa ser respondida: como garantir que um usuário não autorizado não monitore a troca desta chave?

Os avanços da física quântica no século XX possibilitaram que o homem pudesse explicar, descrever e compreender alguns fenômenos e sistemas físicos que a física

clássica era considerada incompleta para explicar. Quando, em 1983, o trabalho “*Conjugate Coding*”, escrito por Stephen Wiesner, foi publicado mostrando para a sociedade científica que as propriedades da física quântica poderiam ser usadas em criptografia, surgiu um novo e interessante horizonte para continuar avançando e tentar responder à pergunta feita anteriormente: como garantir que um usuário não autorizado não monitore a troca desta chave [6]?

É neste contexto que o processamento quântico da informação se torna interessante, pois é a área da tecnologia da informação que se utiliza de princípios da física quântica para prover novos protocolos de comunicações e algoritmos de computação que sejam, de alguma forma, mais eficientes quando comparados aos protocolos e algoritmos implementados apenas com base nos princípios da física clássica [7]. Na área de comunicações, podemos citar como exemplo os protocolos de distribuição quântica de chaves [5, 8, 9], os de compartilhamento quântico de segredos [10, 11], os de comunicação quântica segura direta [12, 13, 14], os de prova de conhecimento nulo [15, 16, 17], dentre outros, que apresentam como principal vantagem uma maior segurança da informação.

No que diz respeito às comunicações, o desenvolvimento do processamento quântico da informação segue na direção do desenvolvimento e da realização prática de novos protocolos. Neste sentido, esta dissertação apresenta um novo protocolo de comunicação quântica segura direta baseado na distribuição quântica de chaves com deslocamento diferencial de fase em quadratura.

Esta dissertação está dividida em quatro capítulos. No primeiro capítulo é apresentada uma revisão sobre distribuição quântica de chaves e mostrado o princípio de operação dos protocolos BB84, B92, DPS-QKD (*Differential Phase-Shift Quantum Key Distribution*) e DQPS-QKD (*Differential Quadrature Phase-Shift Quantum Key Distribution*).

No segundo capítulo são revistos três protocolos de comunicação quântica segura direta: Protocolo de Comunicação Quântica Segura Direta com Chave Pública Conhecida; Protocolo de Comunicação Quântica Segura Direta com “*One-Time Pad*”; e Protocolo de Comunicação Quântica Segura Direta com Autenticação Usando Dois Estados não Ortogonais.

No terceiro capítulo é proposto um esquema óptico que implementa um protocolo de comunicação quântica segura direta baseado na distribuição quântica de chaves com deslocamento diferencial de fase em quadratura, além de apresentar uma análise das suas vantagens e desvantagens.

Por fim, as conclusões e as perspectivas de trabalhos futuros são apresentadas no quarto capítulo.

Capítulo 1

Distribuição Quântica de Chaves

A chave utilizada por algoritmos de criptografia precisa ser segura a ponto de garantir que a informação trocada entre transmissor e receptor não possa ser descoberta por um espião. A técnica que permite, teoricamente, a troca perfeitamente segura de uma sequência aleatória de bits (chave) é a Distribuição Quântica de Chaves (QKD – *Quantum Key Distribution*), cuja segurança dos protocolos utilizados é garantida pelos postulados da física quântica. Os primeiros protocolos de Distribuição Quântica de Chaves, BB84 e B92, são descritos neste capítulo, além de outros dois protocolos que utilizam modulação em fase (Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase – DPS-QKD (*Differential Phase-Shift Quantum Key Distribution*) e Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase em Quadratura – DQPS-QKD (*Differential Quadrature Phase-Shift Quantum Key Distribution*)).

1.1. Introdução

A criptografia é a técnica de troca de mensagens secretas que garante que somente os usuários legítimos da comunicação sejam capazes de decifrá-la, pois apenas estes detêm a chave criptográfica, sem a qual é muito difícil, senão impossível, para um espião recuperar a mensagem original [5].

A criptografia inclui o processo de encriptação dos dados que serão enviados, a decriptação dos dados que foram recebidos e o processo de distribuição da chave criptográfica entre o transmissor e o receptor com a qual realizam-se os processos de encriptação e decriptação, conforme pode ser visto na Figura 1.1 [18].

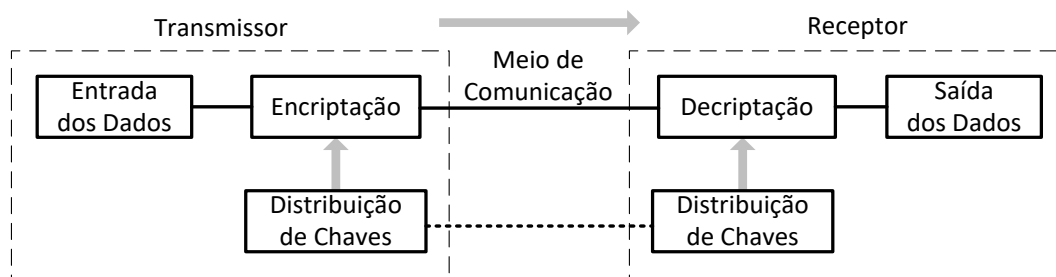


Fig. 1.1. Diagrama esquemático da criptografia

Fonte: [18]

Existem dois métodos de criptografia: o assimétrico e o simétrico. No método assimétrico, uma chave pública, criada a partir de uma chave secreta que apenas um usuário (receptor, chamado de Bob) detém, é divulgada para um outro usuário que deseja lhe transmitir mensagens (transmissor, chamado de Alice). Quando Alice enviar uma mensagem codificada fazendo uso da chave pública que Bob lhe enviou, apenas ele conseguirá decodificá-la, pois ele é o detentor da chave secreta correta. No método simétrico, Alice e Bob compartilham uma chave secreta escolhida aleatoriamente que será utilizada para codificar a mensagem através de uma operação adição módulo 2 entre a mensagem e a chave [5].

A segurança do método assimétrico fundamenta-se na complexidade matemática e computacional para decifrar o código e por isso ela é ameaçada pelo avanço tecnológico (computador quântico, algoritmos de fatoração mais rápidos). Já a segurança do método simétrico é em decorrência da operação *XOR*, mas é necessário garantir que a chave secreta que codifica a mensagem seja conhecida apenas por Alice e Bob. Assim, o principal desafio dos sistemas criptográficos é garantir que a chave seja distribuída seguramente entre os usuários legítimos da comunicação. É nesse contexto que se insere a criptografia quântica, que tem como objetivo a execução de tarefas que são impossíveis com a criptografia convencional, através do uso das propriedades da mecânica quântica como o teorema da não clonagem e o princípio da incerteza de Heisenberg.

A aplicação mais importante e mais conhecida da criptografia quântica é a distribuição quântica de chaves, que já provou ser segura sob determinadas condições experimentais [19]. Atualmente, sistemas de distribuição quântica de chaves estão disponíveis no mercado para compra e há sistemas implementados com centenas de quilômetros que utilizam fibra óptica ou o espaço livre como canal de comunicação [19].

A distribuição quântica de chaves permite que dois entes distantes, Alice e Bob, compartilhem uma chave aleatória na presença de uma espiã, Eva, e com ela possam realizar tanto comunicação quanto autenticação seguras. Para realizar a distribuição quântica de chaves, é necessário que Alice e Bob tenham sido previamente autenticados, ou seja, eles devem compartilhar de uma mesma chave secreta que os identificará quando da primeira comunicação [19].

Dois dos primeiros protocolos de distribuição quântica de chaves foram o BB84 e o B92, mas há também outras variações de protocolos de distribuição quântica de chaves que utilizam modulação de fase, que é o caso da Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase – DPS-QKD (*Differential Phase-Shift Quantum Key Distribution*) e da Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase em Quadratura – DQPS-QKD (*Differential Quadrature Phase-Shift Quantum Key Distribution*), discutidos a seguir.

1.2. Protocolo BB84

Proposto em 1984 por Charles Henry Bennet e Gilles Brassard, o BB84 consiste de um esquema de quatro estados quânticos que constituem duas bases ortogonais: usando-se a polarização da luz tem-se, por exemplo, a base linear ($\uparrow, \rightarrow$) e a base diagonal ($\nearrow, \nwarrow$). O protocolo BB84 pode ser dividido em duas fases: I) comunicação quântica e II) discussão pública [8].

- I) Na fase de comunicação quântica, Alice envia para Bob uma sequência de fótons, cada um polarizado aleatoriamente em um dos quatro estados quânticos ($\uparrow, \rightarrow, \nearrow, \nwarrow$). Para cada fóton recebido, Bob escolhe, aleatoriamente, uma das duas bases (linear ou diagonal) para realizar a medição. Bob registra a base usada para a medição bem como o resultado medido e informa publicamente que recebeu o sinal.
- II) Na segunda fase, a fase de discussão pública, Alice informa as suas bases de preparação e Bob informa as suas bases de medição. Alice e Bob descartam todos os eventos em que eles usaram bases diferentes. Para verificar a presença de um espião na comunicação, Alice escolhe aleatoriamente uma fração dos eventos remanescentes (aqueles nos quais as bases de Alice e Bob

coincidiram) e transmite publicamente as polarizações usadas para estes eventos. Em seguida, Bob transmite os resultados de suas medições naqueles eventos. Alice e Bob computam a taxa de erro dos eventos testados e se ela for maior do que um valor limite preestabelecido eles descartam toda a chave, caso contrário eles procedem para o próximo passo. Na próxima etapa, Alice e Bob convertem a polarização dos eventos restantes numa sequência binária (por exemplo, mapeando um fóton vertical ou diagonal a direita como o bit ‘0’ e um horizontal ou diagonal a esquerda como o bit ‘1’) chamada de chave bruta. Daí por diante eles podem efetuar um processo clássico de correção de erro e de amplificação de privacidade para gerar uma chave final [5].

A Figura 1.2 mostra o esquema óptico que implementa o protocolo BB84. Alice envia para Bob uma sequência de fótons polarizados aleatoriamente num estado quântico ($\uparrow, \rightarrow, \nwarrow, \nearrow$). Bob escolhe aleatoriamente se realizará a medição de cada fóton com a base linear (sem rotação de $\pi/4$) ou se com a base diagonal (com rotação de $\pi/4$).

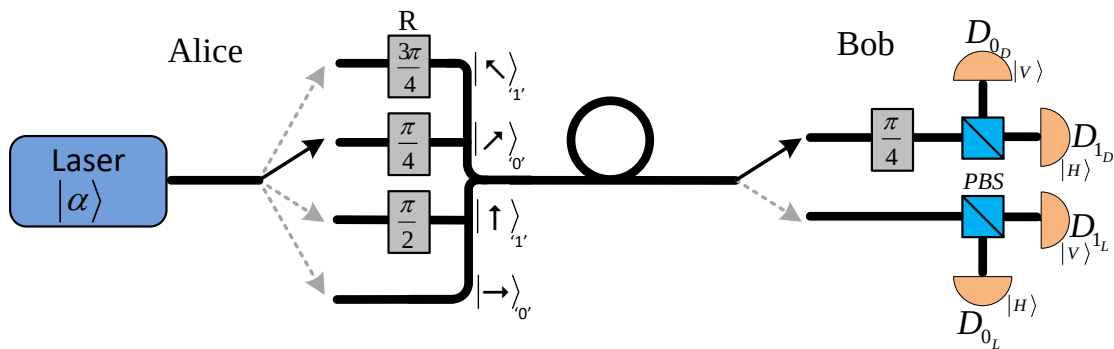


Fig. 1.2. Esquema óptico para o protocolo BB84

Fonte: o autor

No Quadro 1.1 abaixo pode-se verificar um exemplo do procedimento do protocolo BB84 descrito acima.

Quadro 1.1 – Procedimento do BB84. (+) Base Linear, (×) Base Diagonal

Bits de Alice	0	1	1	1	0	1	0	0	0	1
Bases de Alice	+	×	+	+	×	×	+	×	+	×
Polarização dos fótons de Alice	$\rightarrow$	$\nwarrow$	$\uparrow$	$\uparrow$	$\nearrow$	$\nwarrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\nwarrow$
Bases de Bob	+	+	×	+	+	×	×	+	+	×
Polarização medida por Bob	$\rightarrow$	$\uparrow$	$\nwarrow$	$\uparrow$	$\rightarrow$	$\nwarrow$	$\nearrow$	$\uparrow$	$\rightarrow$	$\nwarrow$
Polarização coincidente de Bob com Alice	$\rightarrow$	?	?	$\uparrow$	?	$\nwarrow$	?	?	$\rightarrow$	$\nwarrow$
Bits de Bob	0	-	-	1	-	1	-	-	0	1

Fonte: o autor

1.3. Protocolo B92

O protocolo B92 foi criado em 1992 por Charles Henry Bennett e difere do BB84 no que tange à quantidade de estados quânticos utilizada na implementação do protocolo. Enquanto o protocolo BB84 usa duas bases ortogonais, ou seja, quatro estados quânticos, o B92 utiliza apenas dois estados quânticos não ortogonais ($\rightarrow, \nearrow$ ou $\uparrow, \nwarrow$ ou $\rightarrow, \nwarrow$ ou $\uparrow, \nearrow$). Por exemplo, o bit ‘0’ pode ser um fóton polarizado horizontalmente e o bit ‘1’ um fóton com polarização diagonal à direita [20].

A Figura 1.3 apresenta o esquema óptico que implementa este protocolo e a sua execução acontece da seguinte forma: Alice envia para Bob uma sequência de fótons, cada um polarizado aleatoriamente em um dos dois estados quânticos (aqui serão utilizados os estados $\rightarrow$ e $\nearrow$). Para cada fóton, Bob escolhe aleatoriamente se rotaciona ou não de $\pi/4$ a polarização do fóton que chega ao seu aparato óptico.

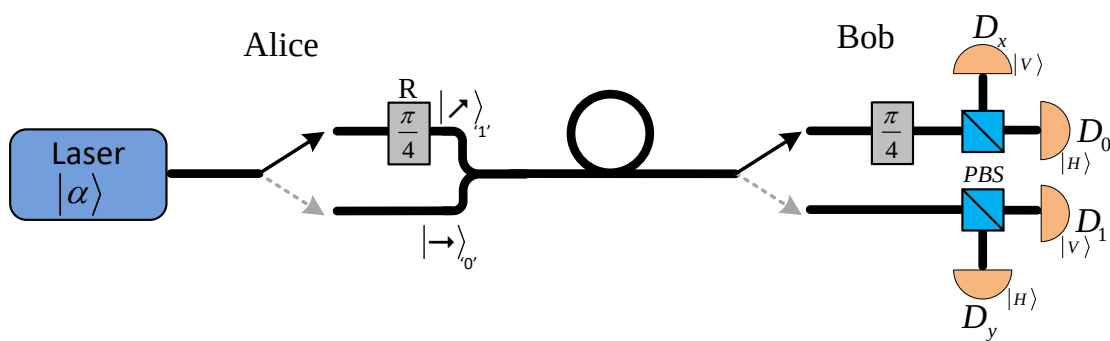


Fig. 1.3. Esquema óptico para o protocolo B92

Fonte: o autor

Caso Alice tenha enviado o estado $|\rightarrow\rangle$ (bit ‘0’) e Bob escolha rotacionar o estado, então poderá haver detecção em D_0 ou em D_x com 50% de probabilidade cada, pois após a rotação o estado será $|\nearrow\rangle = 1/\sqrt{2}|\rightarrow\rangle + 1/\sqrt{2}|\uparrow\rangle$. Entretanto, se Bob decidir não rotacionar o estado, então poderá haver detecção apenas em D_y .

Similarmente, se Alice enviar o estado $|\nearrow\rangle$ (‘1’) e Bob escolher rotacioná-lo poderá haver somente em D_x , mas se Bob não rotacioná-lo poderá haver detecção em D_1 ou em D_y com 50% de probabilidade cada, pois o estado será $|\nearrow\rangle = 1/\sqrt{2}|\rightarrow\rangle + 1/\sqrt{2}|\uparrow\rangle$ [5].

Como pode-se perceber, tanto o estado $|\rightarrow\rangle$ como o estado $|\nearrow\rangle$ enviados por Alice podem produzir uma contagem em D_x ou em D_y dependendo da escolha de Bob a respeito da rotação, mas apenas o estado $|\rightarrow\rangle$ pode produzir uma contagem em D_0 assim como apenas o estado $|\nearrow\rangle$ pode produzir uma contagem em D_1 . Dessa forma, Bob consegue concluir com certeza qual fora o bit enviado por Alice. Percebe-se que, ao contrário do BB84, não é necessário passar pela fase de discussão pública de divulgação das bases.

No Quadro 1.2 abaixo pode-se verificar o procedimento do protocolo B92.

Quadro 1.2 – Procedimento do B92

Bits de Alice	0	1	1	1	0	1	0	0	0	1
Polarização dos fótons de Alice	$\rightarrow$	$\nearrow$	$\nearrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\nearrow$
Rotação realizada por Bob	$\frac{\pi}{4}$	0	0	0	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	0	0
Possibilidades de detecção em Bob	$D_{0,x}$	$D_{1,y}$	$D_{1,y}$	$D_{1,y}$	$D_{0,x}$	D_x	$D_{0,x}$	$D_{0,x}$	D_y	$D_{1,y}$
Contagem de Bob	D_0	D_1	D_1	D_1	D_0	D_x	D_0	D_0	D_y	D_1
Polarização coincidente de Bob com Alice	$\rightarrow$	$\nearrow$	$\nearrow$	$\nearrow$	$\rightarrow$	-	$\rightarrow$	$\rightarrow$	-	$\nearrow$
Bits de Bob	0	1	1	1	0	-	0	0	-	1

Fonte: o autor

1.4. Estados Coerentes

Os estados que possuem distribuição Poissoniana do número de fótons são chamados de estados coerentes. Ao contrário dos estados número, que possuem fase totalmente aleatória, os estados coerentes possuem fase mais bem definida, devido à característica de possuir distribuição Poissoniana do número de fótons, além do produto de incerteza ser o mínimo permitido pelo princípio da incerteza de Heisenberg [21]

$$\Delta p \Delta q = \frac{\hbar}{2} \quad (1.1)$$

A expressão do estado coerente em função dos estados números é definida como sendo [5]

$$|\alpha\rangle = e^{(\alpha a^\dagger - \alpha^* a)} |0\rangle = e^{\alpha a^\dagger} e^{-\alpha^* a} e^{-|\alpha|^2/2} |0\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad (1.2)$$

em que $a^\dagger$ é o operador criação e a é o operador aniquilação.

Os estados coerentes possuem algumas propriedades bastante importantes que podem ser percebidas a partir da equação (1.2):

(a) Número médio de fótons do estado $|\alpha\rangle$:

$$\langle n \rangle = \langle \alpha | a^\dagger a | \alpha \rangle = |\alpha|^2. \quad (1.3)$$

(b) Probabilidade de encontrar n fótons no estado $|\alpha\rangle$:

$$p(n) = \langle n | \alpha \rangle \langle \alpha | n \rangle = \frac{\langle n \rangle^n e^{-\langle n \rangle}}{n!}. \quad (1.4)$$

(c) Relação de completude para o conjunto supercompleto de todos os estados coerentes $|\alpha\rangle$:

$$\frac{1}{\pi} \int |\alpha\rangle \langle \alpha| d^2\alpha = 1 \quad (1.5)$$

1.5. Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase – DPS-QKD (*Differential Phase-Shift Quantum Key Distribution*)

Nos protocolos de distribuição quântica de chaves com deslocamento diferencial de fase, Alice envia para Bob um trem de pulsos coerentes altamente atenuados sendo que cada pulso tem a sua fase aleatoriamente modulada por $\{0, \pi\}$. A potência do sinal transmitido é muito baixa, de forma que o número médio de fótons por pulso é menor do que um, por exemplo 0,1, de modo que a probabilidade de haver dois fótons no pulso seja muito pequena [5].

No aparato de Bob há um interferômetro Mach-Zehnder (formado por dois BS – divisor de feixes) que possui um braço longo e outro curto, sendo o atraso experimentado pelo pulso que segue pelo braço longo, τ , o mesmo intervalo de tempo decorrido entre dois pulsos consecutivos, como se pode observar na Figura 1.4. Em virtude dessa diferença de tamanho dos braços do interferômetro, a interferência no BS₂ ocorrerá entre pulsos adjacentes.

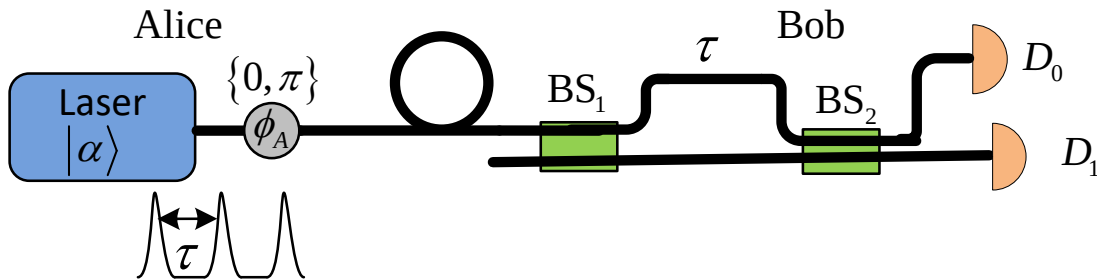


Fig. 1.4. Esquema óptico para DPS-QKD. (BS) Divisor de feixes, (ϕ_A) Modulador de Fase de Alice.

Fonte: o autor

Se dois estados coerentes, por exemplo $|\xi\rangle$ e $|\lambda\rangle$, chegam nas entradas do divisor de feixes ao mesmo tempo e com a mesma polarização, então os estados coerentes nas saídas do divisor de feixes serão [21]:

$$U_{BS} |\xi, \lambda\rangle = \left| \frac{(\xi + \lambda)}{\sqrt{2}} \right\rangle \left| \frac{(-\xi + \lambda)}{\sqrt{2}} \right\rangle. \quad (1.6)$$

Em (1.1) U_{BS} representa a operação que modela a ação do divisor de feixes. Aplicando (1.1) no sistema da Figura 1.4, obtém-se a seguinte expressão para o resultado da interferência no BS₂ entre os pulsos $n-1$ e n :

$$U_{BS_2} \left| \frac{\alpha}{\sqrt{2}} e^{i\phi_A^{n-1}} \right\rangle \left| \frac{\alpha}{\sqrt{2}} e^{i\phi_A^n} \right\rangle = \left| \sqrt{2}\alpha e^{i(\phi_A^{n-1} + \phi_A^n)} \cos\left(\frac{\phi_A^{n-1} - \phi_A^n}{2}\right) \right\rangle_0 \left| -\sqrt{2}\alpha e^{i(\phi_A^{n-1} + \phi_A^n)} \sin\left(\frac{\phi_A^{n-1} - \phi_A^n}{2}\right) \right\rangle_1. \quad (1.7)$$

Em (1.2), os subíndices ‘0’ e ‘1’ indicam as portas de saída do divisor de feixes. Dessa forma, os fótons serão detectados de acordo com a diferença de fase entre os pulsos interferentes n e $n-1$: se a diferença de fase entre os pulsos for igual a 0 haverá um *click* no detector D_0 ($\cos(0) = 1$ e $\sin(0) = 0$), significando que um bit ‘0’ foi obtido; se a diferença de fase for igual a π haverá um *click* no detector D_1 ($\cos(\pi/2) = 0$ e $\sin(\pi/2) = 1$), significando a obtenção de um bit ‘1’.

Após a recepção do sinal, Bob informa para Alice, através de um canal clássico, em quais *time slots* houve detecção de fótons. Somando-se a esta informação o conhecimento da fase usada para a modulação, Alice consegue saber em quais detectores ocorreram os *clicks* e, na ausência de ruídos, ambos obtêm uma sequência de bits idêntica.

Este protocolo DPS-QKD caracteriza-se pela maior simplicidade do esquema óptico e maior eficiência quando comparado ao BB84, pois neste último há um procedimento de seleção de base e o descarte de fótons onde as bases usadas por Alice e Bob são incompatíveis, o que não existe no DPS-QKD. O resultado é que no DPS-QKD todos os fótons detectados contribuem para a formação da chave, aumentando assim a eficiência na criação de chaves [9].

Outra vantagem do DPS-QKD é a redução da complexidade do aparato de Bob, pois utiliza-se apenas um conjunto de medição formado por dois detectores, ao contrário do BB84 e do B92 que normalmente emprega uma combinação de um divisor de feixes com dois conjuntos de medição totalizando quatro detectores. Além disso, há o fato de que um menor número de detectores causa um menor erro de contagem de escuro, resultando assim num número maior de bits de chave seguros depois das etapas de correção de erro e de amplificação de privacidade.

1.6. Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase em Quadratura – DQPS-QKD (*Differential Quadrature Phase-Shift Quantum Key Distribution*)

O esquema óptico que implementa o protocolo DQPS-QKD pode ser visto na Figura 1.5 e seu funcionamento é descrito em seguida.

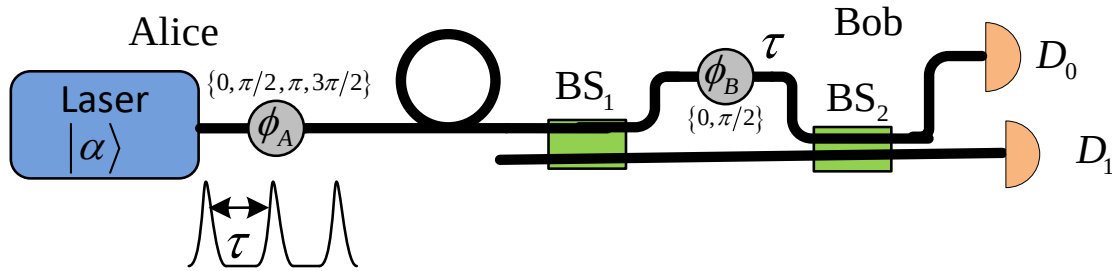


Fig. 1.5. Esquema óptico para DQPS-QKD. (BS) Divisor de feixes, (ϕ_A) Modulador de Fase de Alice,

(ϕ_B) Modulador de Fase de Bob.

Fonte: o autor

No DQPS-QKD cada pulso enviado de Alice para Bob tem a sua fase aleatoriamente deslocada de $\{0, \pi/2, \pi, 3\pi/2\}$, além de ser fortemente atenuado para ter, na média, menos do que um fóton por pulso. O pulso é enviado para Bob que o encaminha para um interferômetro Mach-Zehnder que possui um braço curto e outro longo, onde se encontra um modulador de fase. Novamente, a diferença de tempo de propagação entre os braços é igual ao tempo de separação entre dois pulsos consecutivos [22]. Para cada pulso que chega, Bob escolhe, aleatoriamente no seu modulador ϕ_B , um valor de deslocamento de fase entre os valores $\{0, \pi/2\}$. Neste caso, os estados da luz que chegam em BS₂ na Figura 1.5 são:

$$\begin{aligned} & \dots \underbrace{\left| \frac{\alpha}{\sqrt{2}} e^{i\phi_A^n} \right\rangle_S \left| \frac{\alpha}{\sqrt{2}} e^{i(\phi_A^{n-1} + \phi_B^{n-1})} \right\rangle_L}_n \dots \underbrace{\left| \frac{\alpha}{\sqrt{2}} e^{i\phi_A^3} \right\rangle_S \left| \frac{\alpha}{\sqrt{2}} e^{i(\phi_A^2 + \phi_B^2)} \right\rangle_L}_3 \\ & \quad \otimes \underbrace{\left| \frac{\alpha}{\sqrt{2}} e^{i\phi_A^2} \right\rangle_S \left| \frac{\alpha}{\sqrt{2}} e^{i(\phi_A^1 + \phi_B^1)} \right\rangle_L}_2 \underbrace{\left| \frac{\alpha}{\sqrt{2}} e^{i\phi_A^1} \right\rangle_S |0\rangle_L}_1. \end{aligned} \quad (1.8)$$

Em (1.3), ϕ_A^K (ϕ_B^K) representa o valor da fase escolhida por Alice (Bob), respectivamente, no k -ésimo *time slot*. A interferência ocorre entre os pulsos vindos dos braços curto e longo que chegam em BS₂ ao mesmo tempo. Considerando a ação de divisores de feixe balanceados como em (1.1), os campos depois de BS₂ são:

$$\begin{aligned}
 & \left| \frac{\alpha}{2} e^{i\phi_A^1} \right\rangle_0 \left| \frac{\alpha}{2} e^{i\phi_A^1} \right\rangle_1 \\
 & \left| \alpha e^{i\left(\frac{\phi_A^1 + \phi_A^2 + \phi_B^1}{2}\right)} \cos\left(\frac{\phi_A^1 + \phi_B^1 - \phi_A^2}{2}\right) \right\rangle_0 \left| -i\alpha e^{i\left(\frac{\phi_A^1 + \phi_A^2 + \phi_B^1}{2}\right)} \sin\left(\frac{\phi_A^1 + \phi_B^1 - \phi_A^2}{2}\right) \right\rangle_1 \\
 & \left| \alpha e^{i\left(\frac{\phi_A^2 + \phi_A^3 + \phi_B^2}{2}\right)} \cos\left(\frac{\phi_A^2 + \phi_B^2 - \phi_A^3}{2}\right) \right\rangle_0 \left| -i\alpha e^{i\left(\frac{\phi_A^2 + \phi_A^3 + \phi_B^2}{2}\right)} \sin\left(\frac{\phi_A^2 + \phi_B^2 - \phi_A^3}{2}\right) \right\rangle_1 \\
 & \vdots \\
 & \left| \alpha e^{i\left(\frac{\phi_A^{n-1} + \phi_A^n + \phi_B^{n-1}}{2}\right)} \cos\left(\frac{\phi_A^{n-1} + \phi_B^{n-1} - \phi_A^n}{2}\right) \right\rangle_0 \left| -i\alpha e^{i\left(\frac{\phi_A^{n-1} + \phi_A^n + \phi_B^{n-1}}{2}\right)} \sin\left(\frac{\phi_A^{n-1} + \phi_B^{n-1} - \phi_A^n}{2}\right) \right\rangle_1.
 \end{aligned} \tag{1.9}$$

Como pode ser notado em (1.4), as detecções registradas quando $\phi_A^{n-1} + \phi_B^{n-1} - \phi_A^n$ é igual a ‘0’ ou ‘ π ’ são usadas para formar a chave e as outras são descartadas. Para Bob, detecção em D_0 significa bit ‘0’ e detecção em D_1 significa bit ‘1’. Para Alice, tem-se o código mostrado no Quadro 1.3.

Quadro 1.3 – Codificação de Alice

$\phi_A^{n-1} - \phi_A^n$	ϕ_B^{n-1}	Bit de Alice
0	0	0
Π	0	1
$-\pi/2$	$\pi/2$	0
$\pi/2$	$\pi/2$	1

Fonte: o autor

Dessa forma, os fótons serão detectados de acordo com a diferença de fase entre os pulsos interferentes n e $n-1$: se a diferença de fase entre os pulsos enviados por Alice for igual a 0 e Bob escolher $\phi_B = 0$ também, haverá um *click* no detector D_0 , significando o bit ‘0’; se a diferença de fase entre os pulsos enviados por Alice for igual a π e Bob escolher $\phi_B = 0$ haverá um *click* no detector D_1 , significando o bit ‘1’.

Semelhantemente, se a diferença de fase entre os pulsos enviados por Alice for igual a $-\pi/2$ e Bob escolher $\phi_B = \pi/2$, haverá um *click* no detector D_0 , significando o bit ‘0’; Por outro lado, se a diferença de fase entre os pulsos enviados por Alice for igual a $\pi/2$ e Bob escolher $\phi_B = \pi/2$, haverá um *click* no detector D_1 , significando o bit ‘1’.

No fim do protocolo, Bob informa para Alice em quais *time slots* ele teve detecção e quais os valores de fase usados a fim de que ela saiba quais bits precisam ser descartados.

1.7. Conclusão

Este capítulo mostrou que o principal desafio para os sistemas criptográficos é garantir que a chave secreta utilizada para encriptar e decriptar os dados seja distribuída de forma segura entre os usuários legítimos da comunicação e que a criptografia quântica, que faz uso de propriedades da mecânica quântica, consegue executar as tarefas que são impossíveis de realizar com a criptografia convencional. Também foi mostrado que a aplicação mais importante da criptografia quântica é a distribuição quântica de chaves. Quatro protocolos de distribuição quântica de chaves foram apresentados: BB84, B92, DPS-QKD e DQPS-QKD.

O protocolo BB84 caracteriza-se por utilizar quatro estados quânticos, alcançados a partir de duas bases ortogonais, e pela necessidade da fase de discussão pública, onde Alice e Bob informam as bases utilizadas na preparação/medição dos fótons a fim de descartar os eventos em que foram utilizadas bases diferentes na preparação e medição.

O protocolo B92 utiliza apenas dois estados quânticos não ortogonais e não se faz necessário realizar a etapa de divulgação pública das bases.

No protocolo DPS-QKD a informação está na diferença de fase $\{0, \pi\}$ entre dois pulsos consecutivos. Outra característica deste protocolo é a maior simplicidade dos esquemas ópticos de Alice e Bob, quando comparado aos protocolos BB84 e B92, e a maior eficiência na criação de chaves, quando comparado ao BB84.

O protocolo DQPS-QKD, o último apresentado, assemelha-se ao protocolo DPS-QKD por representar a informação através da diferença de fase, mas difere deste por

possibilitar que o pulso enviado por Alice tenha sua fase modulada por um dos quatro ângulos $\{0, \pi/2, \pi, 3\pi/2\}$ e também por apresentar um modulador de fase no aparato de Bob, que também modula a fase do pulso recebido em um dos dois ângulos $\{0, \pi/2\}$. A eficiência deste protocolo é menor do que a do DPS-QKD porque, assim como no protocolo BB84, faz-se necessário realizar a etapa de discussão pública de bases utilizadas. Entretanto, ele é mais seguro contra os ataques de espões, pois a detecção de um pulso depende da fase escolhida por Bob.

Capítulo 2

Comunicação Quântica Segura Direta

Estabelecer comunicação segura entre duas ou mais partes sem o indesejável vazamento de informação é o objetivo final da criptografia [12]. O caminho convencional para atingir este objetivo é o compartilhamento de pares de chave entre os participantes da comunicação, onde pelo menos uma das chaves deve ser privada. Os protocolos de distribuição quântica de chaves têm facilitado esta atividade na prática, entretanto outro caminho para cumprir este objetivo é utilizando protocolos de Comunicação Quântica Segura Direta (QSDC – *Quantum Secure Direct Communication*) que são estudados neste capítulo.

2.1. Comunicação Quântica Segura Direta *versus* Distribuição Quântica de Chaves

Dado que as partes estão autenticadas, geralmente acredita-se que esquemas criptográficos são completamente seguros apenas se as duas partes da comunicação, Alice e Bob, compartilharem uma chave secreta antes de transmitir a mensagem [13]. Isso significa dizer que primeiro eles terão que criar uma sequência de bits aleatória que não é conhecida por mais ninguém e que tem o mesmo comprimento da mensagem, para então transmitir a mensagem criptografada. Para transmitir, Alice realiza uma operação adição módulo 2 nos bits da mensagem um a um com os bits da chave e apenas Bob será capaz de interpretar a mensagem de Alice.

Diferente da distribuição quântica de chaves, cujo objetivo é gerar chaves privadas que serão utilizadas para encriptar as mensagens trocadas entre duas partes remotas, a comunicação quântica segura direta permite que dois usuários possam transmitir mensagens secretas diretamente sem a prévia criação de uma chave para encriptá-las [14].

2.2. Protocolo de Comunicação Quântica Segura Direta com “*One-Time Pad*”

Foi apresentado em [13] um esquema de comunicação quântica segura direta que utiliza fótons únicos com estados de dois qubits para transmitir a mensagem secreta. No esquema de comunicação quântica segura direta proposto em [23], e apresentado neste tópico, também se propõe o uso de fótons únicos, mas com o próprio estado desses fótons servindo como um “*one-time pad*” (chave de uso único) e codificando a mensagem secreta através de duas operações unitárias diferentes.

2.2.1. Descrição do Protocolo

Assume-se, inicialmente, que Alice quer transmitir uma mensagem secreta para Bob. Similarmente ao protocolo de distribuição quântica de chaves BB84, Alice e Bob usam duas bases de medição, base linear $\{|H\rangle = 0, |V\rangle = 1\}$, e base diagonal $\{|u\rangle = 1/\sqrt{2}(|H\rangle + |V\rangle), |d\rangle = 1/\sqrt{2}(|H\rangle - |V\rangle)\}$, nas quais $|H\rangle$ e $|V\rangle$ são os estados de polarização horizontal e vertical respectivamente. Como no BB84, os estados $|H\rangle$ e $|u\rangle$ representam o valor binário 0, e os estados $|V\rangle$ e $|d\rangle$ representam o valor binário 1 [23].

Inicialmente, considera-se um canal ideal sem ruído. O funcionamento do protocolo de comunicação quântica segura direta usando “*one-time pad*” pode ser dividido em duas fases [23]:

- I) Bob prepara um lote de fótons únicos polarizados e os envia para Alice. Cada fóton está em um dos quatro estados de polarização: $|H\rangle$, $|V\rangle$, $|u\rangle$ e $|d\rangle$. Neste estágio, este lote de fótons é chamado de Lote-A, uma vez que vai em direção a Alice. Depois de receber o lote de fótons, Alice e Bob verificam a presença de espião através do seguinte procedimento: Alice seleciona aleatoriamente um subgrupo de fótons do Lote-A, suficientemente grande, o qual será chamado de Lote-S. Em seguida, ela mede cada um deles usando uma das duas bases de medição (linear ou diagonal) também escolhida aleatoriamente. Alice informa para Bob as posições, as bases de medição e o resultado da medição para cada

um dos fótons do Lote-S. Com esta informação, Bob pode determinar, através da taxa de erro, se há algum espião. Se a taxa de erro for alta, Bob conclui que o canal não é seguro e a comunicação é suspensa. Caso contrário, Alice e Bob passam para a próxima fase. Os fótons remanescentes no Lote-A (que sobraram após a verificação de espião) agora são chamados de Lote-B, assim o Lote-B é a diferença entre o Lote-A e o Lote-S: $B=A-S$.

II) Depois que a verificação da segurança do Lote-A é feita, Alice codifica cada fóton do Lote-B com uma das duas operações unitárias, $I = |H\rangle\langle H| + |V\rangle\langle V|$ ou $U = i\sigma_y = |H\rangle\langle V| - |V\rangle\langle H|$, de acordo com a mensagem secreta. Se o bit secreto é 0, então a operação I é realizada, caso contrário, a operação U é realizada [23]. O interessante da operação U é que ela gira de $\pi/2$ os estado nas duas bases de medição:

$$U|H\rangle = -|V\rangle, U|V\rangle = |H\rangle, U|u\rangle = |d\rangle, U|d\rangle = -|u\rangle. \quad (2.9)$$

Depois disso, Alice reenvia os fótons do Lote-B para Bob. Como o Lote-A foi preparado por Bob, ele sabe as bases de medição e o estado original de cada fóton no lote-B. A mesma base de medição que Bob utilizou para preparar o fóton ele usa para medi-lo, e lê a mensagem secreta diretamente. Para garantir a segurança de todo o processo de comunicação, é necessário que Alice use, aleatoriamente, alguns dos fótons do Lote-B como instâncias de verificação. Ela anunciará publicamente as posições e os valores dos bits codificados destes fótons de verificação depois que a transmissão de um lote estiver completa. Esta medição dá a Alice e Bob uma estimativa se há um espião (Eva) na linha para interceptar a comunicação deles. Entretanto, Eva pode interromper a comunicação deles nesta fase, mas não pode pegar qualquer informação útil sobre a mensagem secreta desde que ela não tenha pego nenhuma informação útil durante a transmissão do Lote-B [23].

2.2.2. Segurança do Protocolo

Em se tratando de comunicação quântica segura direta, além da habilidade de detectar um espião, os usuários devem assegurar-se de que as mensagens secretas codificadas não vazem para o espião antes que este seja detectado.

A codificação das mensagens secretas na segunda fase é idêntica ao processo de codificação numa encriptação “*one-time pad*”, onde o texto é encriptado com uma chave aleatória assim como o estado do fóton no Lote-B é completamente aleatório. A encriptação “*one-time pad*” é completamente segura e nenhuma mensagem secreta pode ser decryptada, mesmo que o texto encriptado tenha sido interceptado por um espião. O protocolo de comunicação quântica segura direta com “*one-time pad*” quântico é ainda mais seguro do que o protocolo com “*one-time pad*” clássico no sentido de que um espião sequer consegue interceptar todo o texto encriptado, uma vez que a base de medição dos fótons é escolhida aleatoriamente. Assim, a segurança deste protocolo depende totalmente da primeira fase, quando Bob envia o Lote-A para Alice.

O processo para garantir a segurança do Lote-A de fótons é similar ao do BB84, em que a segurança é garantida desde que Alice e Bob escolham, aleatoriamente, instâncias suficientes para verificar a presença de espião, sendo este protocolo seguro até mesmo quando o canal é ruidoso. A diferença, entretanto, entre estes dois protocolos é que os fótons do Lote-B precisam ser armazenados enquanto que no BB84 todos os fótons são medidos um por um.

O esquema de comunicação quântica segura direta, até o ponto antes de Alice encriptar a sua mensagem usando uma das operações unitárias, é idêntico ao esquema do protocolo BB84.

De acordo com a análise realizada em [23] do limite de Holevo acerca da informação mútua entre Bob e Eva e considerando que Bob prepara os quatro estados ($|H\rangle$, $|V\rangle$, $|u\rangle$ e $|d\rangle$) com a mesma frequência, pode-se dizer que Alice e Bob podem compartilhar uma sequência de estados quânticos seguramente.

Neste protocolo de comunicação quântica segura direta, a segurança é garantida pelo fato da comunicação acontecer de lote em lote. Depois que um lote de fótons é transmitido de Bob para Alice e que a segurança do canal é constatada (através da

amostragem de um subconjunto de instâncias do lote suficientemente grande), então este lote seguro é utilizado para encriptar a mensagem secreta. Dessa forma, a transmissão da mensagem encriptada é realizada somente depois da confirmação de que o canal quântico é seguro. Assim, Eva não consegue nada, mesmo que ela monitore o resto do processo de comunicação.

2.3. Protocolo de Comunicação Quântica Segura Direta com Autenticação Usando Dois Estados não Ortogonais

A autenticação de identidade, definida como um procedimento de verificação de identidade de cada parte da comunicação, é capaz de evitar que um espião finja ser um dos usuários legítimos da comunicação. Esta é uma forma efetiva de se proteger contra os ataques do tipo personificação. Neste tipo de ataque, o espião finge ser um dos dois usuários legais para se comunicar com o outro. Por exemplo, ele finge ser o receptor para receber mensagens secretas do transmissor, ou finge ser o transmissor para enviar mensagens falsas para o receptor. A maioria dos protocolos de comunicação quântica segura direta pode se proteger de ataques do tipo intercepta-reenvia, ataque de medição-emanhada, dentre outros. Entretanto, eles geralmente são fracos contra os ataques do tipo personificação, uma vez que nenhum esquema de autenticação é adotado, mesmo sendo um requisito necessário se defender deste tipo de ataque [14].

Além de realizar autenticação, este protocolo de comunicação quântica segura direta com autenticação utiliza dois estados não ortogonais como portadoras quânticas. Os estados utilizados são $|H\rangle$ e $|u\rangle$. A verificação da identidade dos dois usuários é realizada através da utilização de uma função *hash* de uso único e a codificação de um bit clássico é realizada pela execução de uma operação unitária, I ou U ($\sigma_x = |H\rangle\langle V| + |V\rangle\langle H|$), pelo transmissor.

2.3.1. Protocolo de Comunicação Quântica Segura Direta com Autenticação

Como nos outros protocolos de comunicação quântica segura direta, há dois usuários, Alice e Bob, que querem se comunicar. Alice quer enviar uma mensagem secreta x com n bits clássicos para Bob diretamente, mas certificando-se de que Bob realmente é quem ele diz ser. Esta tarefa pode ser realizada através de vários passos descritos a seguir:

PASSO 1) Inicialização.

(1.1) Alice e Bob compartilham uma chave secreta k_{AB} através de um protocolo seguro de distribuição quântica de chaves, depois eles combinam uma função *hash* de uso único $h = \{0,1\}^* \rightarrow \{0,1\}^{2n}$ e geram um número aleatório, cada um, r_A e r_B . As identidades dos dois usuários são denotadas por ID_A e ID_B . Assim, Alice e Bob vão obter duas sequências *hash* $h_A = h(k_{AB}, ID_A, r_B)$ e $h_B = h(k_{AB}, ID_B, r_A)$, respectivamente. Aqui, k_{AB} é secreto, mas r_A , r_B , ID_A , ID_B são públicos. Consequentemente, as sequências *hash* h_A e h_B são conhecidos apenas pelos dois usuários legítimos da comunicação (Alice e Bob);

(1.2) Bob gera uma sequência a com número de bits igual a $2n$, escolhidos aleatoriamente, e insere cada bit da sequência *hash* h_B na sequência a em posições aleatórias. A nova sequência de bits é denotada por b . Depois disso, de acordo com o valor de b , Bob prepara $4n$ fótons, os quais são denotados pela sequência T_B . Se $b = 0$, a partícula (o fóton) é preparada no estado $|H\rangle$ e se $b = 1$ a partícula é preparada no estado $|u\rangle$. Na sequência T_B , as partículas correspondentes à sequência a são denotadas pela sequência S_B e as partículas correspondentes à sequência h_B são denotadas pela sequência AC_B . A sequência S_B é usada para codificar, enquanto a sequência AC_B para verificar a identidade de Bob e checar a segurança do canal quântico na primeira transmissão [14]; Todas as incógnitas usadas pelo protocolo no PASSO 1 são apresentadas no Quadro 2.2;

Quadro 2.1 – Resumo das incógnitas do PASSO 1

x	Mensagem secreta a ser transmitida
n	Número de bits clássicos da mensagem secreta x
k_{AB}	Chave secreta compartilhada
r_A	Número aleatório gerado por Alice
r_B	Número aleatório gerado por Bob
ID_A	Identidade de Alice
ID_B	Identidade de Bob
$h_A=h(k_{AB}, ID_A, r_B)$	Sequência <i>hash</i> de Alice (tamanho $2n$)
$h_B=h(k_{AB}, ID_B, r_A)$	Sequência <i>hash</i> de Bob (tamanho $2n$)
a	Sequência gerada por Bob (tamanho $2n$)
b	Sequência de bits gerada por Bob formada por a e h_B (tamanho $4n$)
T_B	Sequência de bits gerada por Bob formada a partir de b (tamanho $4n$)
S_B	Sequência contida em T_B correspondente às partículas da sequência a , usada para encriptar a mensagem secreta (tamanho $2n$)
AC_B	Sequência contida em T_B correspondente às partículas da sequência <i>hash</i> de Bob h_B , usada para verificar a identidade de Bob e checar a segurança do canal na 1ª transmissão (tamanho $2n$)

Fonte: o autor

PASSO 2) Verificando a identidade de Bob e checando a segurança da primeira transmissão.

(2.1) Bob envia a sequência T_B para Alice;

(2.2) Depois de confirmar que Alice recebeu a sequência T_B , Bob diz para Alice as posições do AC_B através do canal clássico público. Então Alice realiza a medição em cada partícula de AC_B nas bases apropriadas de acordo com h_B . Se $h_B = 0$, ela faz a medição com a base Z , mas se $h_B = 1$, ela faz a medição com a base X . Obviamente, ela obterá um resultado errado caso a medição resulte em $|V\rangle$ ou $(|d\rangle = 1/\sqrt{2}(|H\rangle - |V\rangle))$. Desta forma, ela pode calcular a taxa de erro, a qual é definida como a razão entre o número de resultados errados e a soma das partículas em AC_B (isto é, $2n$). Se a taxa de erro é menor do que o limite, ela considera que

Bob é legítimo e que o canal quântico é seguro, e então continua o protocolo. Caso contrário, o protocolo é abandonado [14];

PASSO 3) Codificação e decodificação.

(3.1) Alice divide a sequência *hash* h_A em duas partes $h_A^a = (h_A(1), h_A(2), \dots, h_A(n))$, a qual representa a primeira metade de h_A , e $h_A^e = (h_A(n+1), h_A(n+2), \dots, h_A(2n))$, a qual representa a segunda metade de h_A , onde $h_A(i)$ representa o i -ésimo bit de h_A . A primeira parte (h_A^a) é usada para verificar a legitimidade de Alice, enquanto a segunda parte (h_A^e) é usada para encriptar a mensagem secreta x . De acordo com os valores da (2.10) mensagem secreta x e h_A^e , obtém-se:

$$y = h_A^e \oplus x.$$

O símbolo $\oplus$ representa a adição módulo 2. Em seguida, Alice insere cada bit de y na sequência h_A^a em posições aleatórias. A nova sequência de bits depois da inserção é denotada por z , a qual só é conhecida por Alice. O procedimento de geração da sequência de bits z é ilustrado pela Figura 2.1;

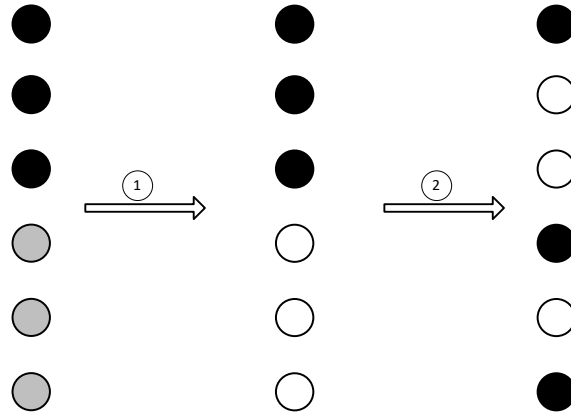


Fig. 2.1. Ilustração de uma sequência genérica z . Os pontos pretos representam h_A^a , os cinzas representam h_A^e e os brancos representam y .

Fonte: [14]

(3.2) Alice faz uma das duas operações unitárias, $I = |H\rangle\langle H| + |V\rangle\langle V|$ ou $U = |H\rangle\langle V| + |V\rangle\langle H|$, para cada partícula na sequência esquerda S_B de acordo com z . Se $z = 0$, ela faz a operação I , caso contrário, se $z = 1$, ela faz a operação U . Depois da codificação, a nova sequência é denotada por T_A . Em T_A , as partículas correspondentes a y são denotadas pela sequência S_A e as partículas correspondentes a h_A^a são denotadas pela sequência AC_A . S_A é usado para carregar

o texto cifrado y , enquanto AC_A é usado para verificar a identidade de Alice e checar a segurança do canal quântico para a segunda transmissão [14];

(3.3) Alice envia a sequência T_A para Bob;

(3.4) Para cada partícula em T_A , Bob realiza medições nas bases que ele preparou originalmente. Se o resultado é o mesmo com o estado original, ele lê a operação que Alice aplicou como I . Caso contrário, ele lê a operação de Alice como U . Depois de decodificar totalmente as partículas, ele obtém o resultado $\hat{z}$.

PASSO 4) Verificando a identidade de Alice e checando a segurança da segunda transmissão.

(4.1) Depois de confirmar que Bob finalizou a decodificação, Alice informa as posições de AC_A em T_A . Assim, Bob pode ter $\hat{h}_A^a$ e $\hat{y}$ de acordo com a informação de Alice. Então, ele compara $\hat{h}_A^a$ com h_A^a para estimar a taxa de erro. Se a taxa de erro estiver abaixo do limite, ele considera que Alice é legítima e que o canal quântico é seguro e lê a mensagem secreta através de:

$$\hat{x} = \hat{y} \oplus h_A^e. \quad (2.11)$$

Caso contrário, o protocolo é abandonado [14]. As incógnitas usadas pelo protocolo desde o PASSO 2 até o PASSO 4 são apresentadas no Quadro 2.3.

Quadro 2.2 – Resumo das incógnitas do PASSO 2 ao PASSO 4

h_A^a	Sequência de bits correspondente à primeira metade da sequência hash de Alice h_A (tamanho n)
h_A^e	Sequência de bits correspondente à segunda metade da sequência hash de Alice h_A (tamanho n)
y	Resultado da operação módulo 2 de x com h_A^e (tamanho n)
z	Sequência de bits gerada por Alice formada a partir de y e h_A^a (tamanho $2n$)
T_A	Sequência de bits gerada por Alice formada a partir de z (tamanho $2n$)
S_A	Sequência contida em T_A correspondente às partículas da sequência y , usada para encriptar a mensagem secreta (tamanho n), usada para carregar o texto encriptado.
AC_A	Sequência contida em T_A correspondente à primeira metade da sequência hash de Alice h_A , usada para verificar a identidade de

	Alice e checar a segurança do canal na 2ª transmissão (tamanho n)
$\widehat{h}_A^a$	Decodificação de Bob para h_A^a , usada para estimar a taxa de erro de bit
$\hat{y}$	Decodificação de Bob para y
$\hat{x}$	Decodificação de Bob para x

Fonte: o autor

Todo o procedimento do protocolo pode ser verificado na Figura 2.2 abaixo:

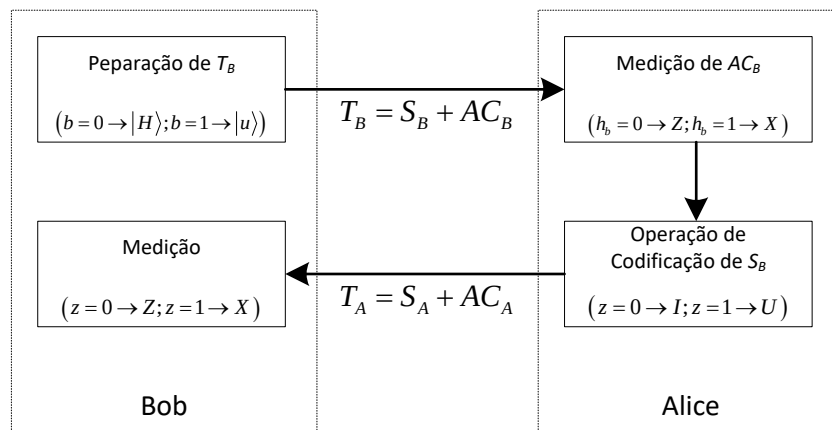


Fig. 2.2. Resumo do protocolo de comunicação quântica segura direta com autenticação.

Fonte: [14]

2.3.2. Análise de Segurança

A segurança do protocolo de comunicação quântica segura direta com autenticação contra os ataques do tipo personificação e intercepta-reenvia é analisada nas seções a seguir.

a. Ataque do Tipo Personificação

Num ataque do tipo personificação um *hacker* malicioso pode tentar se personificar em um dos dois usuários legítimos da comunicação: Bob (chamado de Bob*) ou Alice (chamada de Alice*). Quando o *hacker* se personifica em Bob, ele deseja obter

a mensagem codificada por Alice e quando o *hacker* se personifica em Alice, ele deseja enviar uma mensagem falsa para Bob [17].

No primeiro caso (*hacker* se personifica em Bob), Bob* tem que preparar a sequência de partículas AC_B nos estados corretos a fim de fingir sua autenticidade para Alice, mas isso depende de h_B . Entretanto, Bob* não pode fazer isso porque ele não conhece h_B . Na verdade, se Bob* gerar h_B com uma sequência de bits aleatória, Alice vai detectar a sua ação no PASSO 2 com probabilidade 25%.

No segundo caso (*hacker* se personifica em Alice), Alice* tem que fazer as operações corretas para gerar a sequência de partículas AC_A de acordo com h_A^a , mas ela não tem ideia de quem que é h_A^a . Caso Alice* tente gerar h_A^a com uma sequência de bits aleatória, Bob detectará a sua ação no PASSO 4 com probabilidade 50%.

A partir destas duas análises, conclui-se que o protocolo é seguro contra o ataque do tipo personificação [14].

b. Ataque do Tipo Intercepta-Reenvia

Nos ataques do tipo intercepta-reenvia o espião (Eva) intercepta as partículas transmitidas, mede-as, e então reenvia partículas falsas para o usuário alvo de acordo com os resultados da medição. O objetivo do espião é obter as operações de codificação de Alice.

Analizando inicialmente a situação onde Eva realiza este ataque apenas na segunda transmissão, ela intercepta T_A e realiza medições na base X ou Z em cada partícula de T_A . Neste caso, para cada partícula, Eva pode adivinhar a operação de codificação de Alice (I ou U) com probabilidade 75%. Por exemplo, se o resultado da medição de Eva é $|H\rangle$, ela confirma, com 75% de probabilidade, que Alice fez a operação I . Esta espionagem será detectada por Bob com probabilidade 25%, o mesmo que ocorre no protocolo BB84 [14].

Se Eva quiser pegar mais informações sobre as operações de Alice, ela atacará nas duas transmissões. Na primeira transmissão, Eva intercepta a sequência T_B e mede cada partícula dela na base X ou Z aleatoriamente. Se o resultado da medição de Eva for $|H\rangle$,

ela prepara uma partícula falsa no estado $|H\rangle$, mas caso o resultado da medição seja $|u\rangle$, ela prepara uma partícula falsa no estado $|u\rangle$ e reenvia isso para Alice. Adicionalmente, se o resultado da medição for $|V\rangle$ (ou $|d\rangle$), Eva saberá indubitavelmente que o estado enviado por Bob é $|u\rangle$ (ou $|H\rangle$). Neste caso, ela vai preparar a partícula falsa no estado $|u\rangle$ (ou $|H\rangle$) e reenviar para Alice, mas Alice detectará esta ação com probabilidade 12,5%. Por exemplo, supondo que Eva intercepte uma partícula cujo estado é $|H\rangle$, ela somente introduzirá um erro quando ela realizar medições na base X e obtiver o resultado $|u\rangle$. Isso ocorrerá com probabilidade 50%. Consequentemente, a probabilidade de detecção é $50\% \times 50\% \times 50\% = 12,5\%$ [14].

2.4. Conclusão

O protocolo de comunicação quântica segura direta com “*one-time pad*” usa fótons únicos em lotes, onde o próprio estado do fóton serve como um “*one-time pad*”. Os fótons são codificados com a mensagem secreta através de duas operações unitárias diferentes (I ou U). O protocolo pode ser visto como uma modificação do protocolo de distribuição quântica de chaves BB84. Na implementação deste protocolo são necessárias fontes de fótons únicos e técnicas para armazenamento de estados quânticos.

O protocolo de comunicação quântica segura direta com autenticação utiliza uma função *hash* de uso único para realizar a autenticação dos dois usuários e uma operação unitária de partícula única para encriptar a mensagem secreta. Diferente do protocolo de comunicação quântica segura direta com “*one-time pad*” que requer técnicas para armazenamento de estados quânticos, o protocolo com autenticação requer apenas técnicas de geração de fótons únicos. Neste protocolo, todos os fótons são preparados por Bob e cabe a Alice realizar a encriptação destes estados a fim de transmitir a mensagem secreta para Bob.

Capítulo 3

Comunicação Quântica Segura Direta usando Distribuição Quântica de Chaves

Neste capítulo, é mostrado um esquema óptico que executa comunicação quântica segura direta baseado na distribuição quântica de chaves com deslocamento diferencial de fase em quadratura. Além disso, apresenta-se também uma análise das suas vantagens e desvantagens ao fim do capítulo.

3.1. Esquema Óptico para implementar QSDC usando DQPS-QKD

O primeiro esquema óptico proposto para implementar QSDC utiliza dois DQPS-QKD e é mostrado na Figura 3.1.

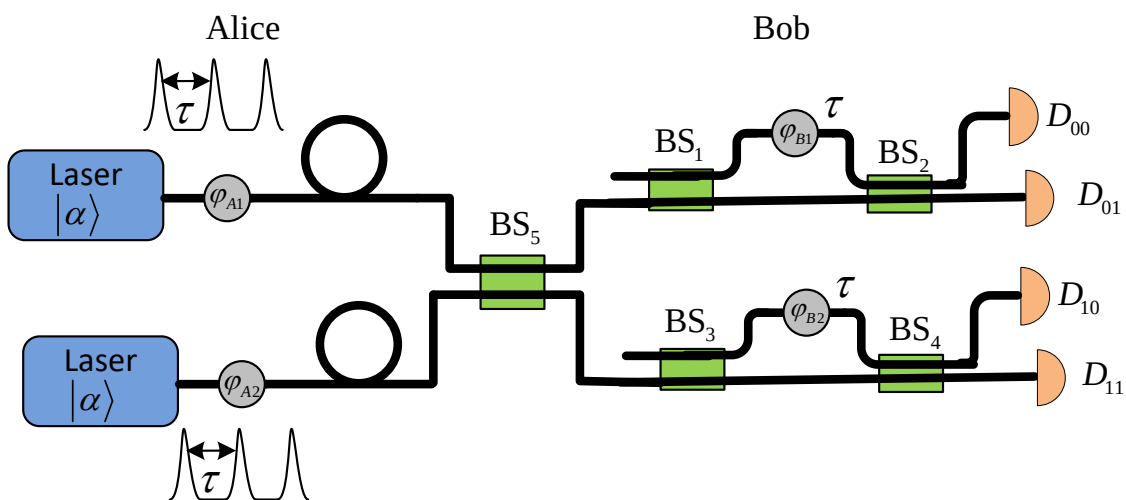


Fig. 3.1. Esquema óptico para QSDC empregando dois DQPS-QKD

Fonte: o autor

Como se pode observar na Figura 3.1, o esquema óptico para QSDC emprega dois esquemas de DQPS-QKD trabalhando juntos. O aparato de Bob inicia-se a partir do BS₅, onde ocorre interferência. Os estados da luz que chegam no BS₅ são:

$$|E_{BS5}\rangle = |\alpha e^{i\varphi_{A1}}\rangle_S |\alpha e^{i\varphi_{A2}}\rangle_I \quad (3.1)$$

onde S indica o estado que chega pelo braço superior e I o estado que chega pelo braço inferior.

O estado da luz que sai no braço superior do interferômetro é:

$$\begin{aligned} |S_{S5}\rangle &= \left| \frac{\alpha}{\sqrt{2}} (e^{i\varphi_{A1}} + e^{i\varphi_{A2}}) \right\rangle = \left| \frac{\alpha}{\sqrt{2}} \left(e^{i\left(\frac{\varphi_{A1}+\varphi_{A1}}{2}\right)} + e^{i\left(\frac{\varphi_{A2}+\varphi_{A2}}{2}\right)} \right) \right\rangle \\ &= \left| \frac{\alpha}{\sqrt{2}} \left(e^{i\left(\frac{\varphi_{A1}+\varphi_{A1}}{2}\right)} e^{i\left(\frac{\varphi_{A2}-\varphi_{A2}}{2}\right)} + e^{i\left(\frac{\varphi_{A2}+\varphi_{A2}}{2}\right)} e^{i\left(\frac{\varphi_{A1}-\varphi_{A1}}{2}\right)} \right) \right\rangle \\ &= \left| \frac{\alpha}{\sqrt{2}} \left(e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} e^{i\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right)} + e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} e^{-i\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right)} \right) \right\rangle \\ &= \left| \frac{\alpha}{\sqrt{2}} e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \left(e^{i\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right)} + e^{-i\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right)} \right) \right\rangle \\ &= \left| \frac{2\alpha}{\sqrt{2}} e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \cos\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right) \right\rangle \\ |S_{S5}\rangle &= \left| \sqrt{2}\alpha e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \cos\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right) \right\rangle. \end{aligned} \quad (3.2)$$

O estado que sai no braço inferior do interferômetro é:

$$\begin{aligned} |I_{S5}\rangle &= \left| \frac{\alpha}{\sqrt{2}} (-e^{i\varphi_{A1}} + e^{i\varphi_{A2}}) \right\rangle = \left| \frac{\alpha}{\sqrt{2}} \left(-e^{i\left(\frac{\varphi_{A1}+\varphi_{A1}}{2}\right)} + e^{i\left(\frac{\varphi_{A2}+\varphi_{A2}}{2}\right)} \right) \right\rangle \\ &= \left| \frac{\alpha}{\sqrt{2}} \left(-e^{i\left(\frac{\varphi_{A1}+\varphi_{A1}}{2}\right)} e^{i\left(\frac{\varphi_{A2}-\varphi_{A2}}{2}\right)} + e^{i\left(\frac{\varphi_{A2}+\varphi_{A2}}{2}\right)} e^{i\left(\frac{\varphi_{A1}-\varphi_{A1}}{2}\right)} \right) \right\rangle \\ &= \left| \frac{\alpha}{\sqrt{2}} \left(-e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} e^{i\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right)} + e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} e^{-i\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right)} \right) \right\rangle \\ &= \left| \frac{\alpha}{\sqrt{2}} e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \left(-e^{i\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right)} + e^{-i\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right)} \right) \right\rangle \end{aligned} \quad (3.3)$$

$$= \left| -\frac{2i\alpha}{\sqrt{2}} e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \sin\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right) \right\rangle$$

$$|I_{S5}\rangle = \left| -\sqrt{2}i\alpha e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \sin\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right) \right\rangle.$$

Os estados da luz na entrada de BS₁ são:

$$|E_{BS1}\rangle = \left| \sqrt{2}\alpha e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \cos\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right) \right\rangle_I |0\rangle_s \quad (3.4)$$

ou seja, é o estado vácuo e o estado que saiu do braço superior do BS₅.

Após a interferência ocorrida em BS₁, obter-se-á, no braço superior (e no braço inferior (I_{S1}), o estado:

$$|S_{S1}\rangle = |I_{S1}\rangle = \frac{\left| \sqrt{2}\alpha e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \cos\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right) \right\rangle}{\sqrt{2}} = \left| \alpha e^{i\left(\frac{\varphi_{A1}+\varphi_{A2}}{2}\right)} \cos\left(\frac{\varphi_{A1}-\varphi_{A2}}{2}\right) \right\rangle. \quad (3.5)$$

O estado S_{S1} passará pelo modulador de fase φ_{B1} e sofrerá um atraso de τ . Por causa deste atraso, os estados que sofrerão interferência em BS₂ são originários de pulsos ópticos diferentes, mas consecutivos. Ou seja, a parcela do 1º pulso que saiu pelo braço inferior do BS₁ interferirá com o vácuo (presente na entrada superior do BS₂); a parcela do 2º pulso que saiu pelo braço inferior do BS₁ interferirá com a parcela do 1º pulso que saiu pelo braço superior do BS₁ e sofreu modulação de fase φ_{B1} ; a parcela do 3º pulso que saiu pelo braço inferior do BS₁ interferirá com a parcela do 2º pulso que saiu pelo braço superior do BS₁ e sofreu modulação de fase φ_{B1} ; e assim sucessivamente. Matematicamente, representa-se os estados na entrada de BS₂ da seguinte forma:

$$\begin{aligned}
& \underbrace{\left| \alpha \cos\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) e^{i\left(\frac{\varphi_{A1}^n + \varphi_{A2}^n}{2}\right)} \right\rangle_I \left| \alpha \cos\left(\frac{\varphi_{A1}^{n-1} - \varphi_{A2}^{n-1}}{2}\right) e^{i\left(\frac{\varphi_{A1}^{n-1} + \varphi_{A2}^{n-1}}{2} + \varphi_{B1}^{n-1}\right)} \right\rangle_S \right\rangle_n \\
& \otimes \underbrace{\left| \alpha \cos\left(\frac{\varphi_{A1}^3 - \varphi_{A2}^3}{2}\right) e^{i\left(\frac{\varphi_{A1}^3 + \varphi_{A2}^3}{2}\right)} \right\rangle_I \left| \alpha \cos\left(\frac{\varphi_{A1}^2 - \varphi_{A2}^2}{2}\right) e^{i\left(\frac{\varphi_{A1}^2 + \varphi_{A2}^2}{2} + \varphi_{B1}^2\right)} \right\rangle_S \right\rangle_3 \\
& \otimes \underbrace{\left| \alpha \cos\left(\frac{\varphi_{A1}^2 - \varphi_{A2}^2}{2}\right) e^{i\left(\frac{\varphi_{A1}^2 + \varphi_{A2}^2}{2}\right)} \right\rangle_I \left| \alpha \cos\left(\frac{\varphi_{A1}^1 - \varphi_{A2}^1}{2}\right) e^{i\left(\frac{\varphi_{A1}^1 + \varphi_{A2}^1}{2} + \varphi_{B1}^1\right)} \right\rangle_S \right\rangle_2 \\
& \otimes \underbrace{\left| \alpha \cos\left(\frac{\varphi_{A1}^1 - \varphi_{A2}^1}{2}\right) e^{i\left(\frac{\varphi_{A1}^1 + \varphi_{A2}^1}{2}\right)} \right\rangle_I \right\rangle_1 |0\rangle_S
\end{aligned} \tag{3.6}$$

Os valores usados por Bob para φ_{B1} e φ_{B2} pertencem ao conjunto $\{0, \pi/2\}$.

O resultado da interferência ocorrida em BS₂ será detectada em D₀₀ e/ou D₀₁ e pode ser escrita como:

$$|D_{00}\rangle = \left| \frac{\alpha}{\sqrt{2}} \left[\cos\left(\frac{\varphi_{A1}^{n-1} - \varphi_{A2}^{n-1}}{2}\right) e^{i\left(\frac{\varphi_{A1}^{n-1} + \varphi_{A2}^{n-1}}{2} + \varphi_{B1}^{n-1}\right)} + \cos\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) e^{i\left(\frac{\varphi_{A1}^n + \varphi_{A2}^n}{2}\right)} \right] \right\rangle \tag{3.7}$$

e

$$|D_{01}\rangle = \left| -\frac{\alpha}{\sqrt{2}} \left[\cos\left(\frac{\varphi_{A1}^{n-1} - \varphi_{A2}^{n-1}}{2}\right) e^{i\left(\frac{\varphi_{A1}^{n-1} + \varphi_{A2}^{n-1}}{2} + \varphi_{B1}^{n-1}\right)} - \cos\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) e^{i\left(\frac{\varphi_{A1}^n + \varphi_{A2}^n}{2}\right)} \right] \right\rangle. \tag{3.8}$$

Quando Alice quer transmitir o bit ‘0’ ela faz $\varphi_{A1} - \varphi_{A2} = 0$. Se houver detecção em D₀₀ ou em D₀₁ significa bit ‘0’ para o protocolo QSDC.

Quando dois bits consecutivos são iguais (casos que realmente interessam para o protocolo), temos $\varphi_{A1}^n - \varphi_{A2}^n = \varphi_{A1}^{n-1} - \varphi_{A2}^{n-1}$ e neste caso as equações (3.7) e (3.8) se tornam, respectivamente:

$$|D_{00}\rangle = \left| \sqrt{2}\alpha \cos\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) \cos\left(\frac{\sum_{n-1} - \sum_n}{4} + \frac{\varphi_{B1}^{n-1}}{2}\right) e^{i\left(\frac{\sum_{n-1} + \sum_n}{4} + \frac{\varphi_{B1}^{n-1}}{2}\right)} \right\rangle \quad (3.9)$$

e

$$|D_{01}\rangle = \left| -i\sqrt{2}\alpha \cos\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) \sin\left(\frac{\sum_{n-1} - \sum_n}{4} + \frac{\varphi_{B1}^{n-1}}{2}\right) e^{i\left(\frac{\sum_{n-1} + \sum_n}{4} + \frac{\varphi_{B1}^{n-1}}{2}\right)} \right\rangle. \quad (3.10)$$

A análise feita a partir da equação (3.4) retrata o que ocorre na parte superior do aparato de Bob. Uma análise similar pode ser feita para a parte inferior do aparato e serão obtidos os seguintes resultados:

$$|E_{BS3}\rangle = \left| -\sqrt{2}i\alpha e^{i\left(\frac{\varphi_{A1} + \varphi_{A2}}{2}\right)} \sin\left(\frac{\varphi_{A1} - \varphi_{A2}}{2}\right) \right\rangle_I |0\rangle_S, \quad (3.11)$$

$$|S_{S3}\rangle = |I_{S3}\rangle = \left| -i\alpha e^{i\left(\frac{\varphi_{A1} + \varphi_{A2}}{2}\right)} \sin\left(\frac{\varphi_{A1} - \varphi_{A2}}{2}\right) \right\rangle, \quad (3.12)$$

onde E_{BS3} representa o estado na entrada do BS₃, S_{S3} representa o estado na saída superior do BS₃ e I_{S3} representa o estado na saída inferior do BS₃. Uma vez que a interferência ocorrida em BS₃ envolve o estado vácuo, os estados nas duas saídas desse divisor de feixes serão iguais.

Assim como acontece na parte superior do aparato, a interferência em BS₄ ocorrerá entre pulsos consecutivos, devido ao atraso que o estado S_{S3} sofrerá. Dessa forma, os estados da luz na entrada do BS₄ serão

$$\begin{aligned} & \underbrace{\left| -i\alpha \sin\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) e^{i\left(\frac{\varphi_{A1}^n + \varphi_{A2}^n}{2}\right)} \right\rangle_I \left| -i\alpha \sin\left(\frac{\varphi_{A1}^{n-1} - \varphi_{A2}^{n-1}}{2}\right) e^{i\left(\frac{\varphi_{A1}^{n-1} + \varphi_{A2}^{n-1}}{2} + \varphi_{B2}^{n-1}\right)} \right\rangle_S \right|_n \dots \\ & \otimes \underbrace{\left| -i\alpha \sin\left(\frac{\varphi_{A1}^3 - \varphi_{A2}^3}{2}\right) e^{i\left(\frac{\varphi_{A1}^3 + \varphi_{A2}^3}{2}\right)} \right\rangle_I \left| -i\alpha \sin\left(\frac{\varphi_{A1}^2 - \varphi_{A2}^2}{2}\right) e^{i\left(\frac{\varphi_{A1}^2 + \varphi_{A2}^2}{2} + \varphi_{B2}^2\right)} \right\rangle_S \right|_3 \end{aligned} \quad (3.13)$$

$$\begin{aligned}
& \otimes \underbrace{\left| -i\alpha \sin\left(\frac{\varphi_{A1}^2 - \varphi_{A2}^2}{2}\right) e^{i\left(\frac{\varphi_{A1}^2 + \varphi_{A2}^2}{2}\right)} \right\rangle_I \left| -i\alpha \sin\left(\frac{\varphi_{A1}^1 - \varphi_{A2}^1}{2}\right) e^{i\left(\frac{\varphi_{A1}^1 + \varphi_{A2}^1}{2} + \varphi_{B2}^1\right)} \right\rangle_S}_{2} \\
& \otimes \underbrace{\left| -i\alpha \sin\left(\frac{\varphi_{A1}^1 - \varphi_{A2}^1}{2}\right) e^{i\left(\frac{\varphi_{A1}^1 + \varphi_{A2}^1}{2}\right)} \right\rangle_I}_{1} |0\rangle_S
\end{aligned}$$

O resultado da interferência ocorrida em BS₄ será detectada em D₁₀ e/ou D₁₁ e pode ser escrita como:

$$|D_{10}\rangle = \left| -\frac{i\alpha}{\sqrt{2}} \left[\sin\left(\frac{\varphi_{A1}^{n-1} - \varphi_{A2}^{n-1}}{2}\right) e^{i\left(\frac{\varphi_{A1}^{n-1} + \varphi_{A2}^{n-1}}{2} + \varphi_{B2}^{n-1}\right)} + \sin\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) e^{i\left(\frac{\varphi_{A1}^n + \varphi_{A2}^n}{2}\right)} \right] \right\rangle \quad (3.14)$$

e

$$|D_{11}\rangle = \left| \frac{i\alpha}{\sqrt{2}} \left[\sin\left(\frac{\varphi_{A1}^{n-1} - \varphi_{A2}^{n-1}}{2}\right) e^{i\left(\frac{\varphi_{A1}^{n-1} + \varphi_{A2}^{n-1}}{2} + \varphi_{B2}^{n-1}\right)} - \sin\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) e^{i\left(\frac{\varphi_{A1}^n + \varphi_{A2}^n}{2}\right)} \right] \right\rangle \quad (3.15)$$

Similarmente ao que ocorre no interferômetro superior, quando dois bits consecutivos são iguais, então $\varphi_{A1}^n - \varphi_{A2}^n = \varphi_{A1}^{n-1} - \varphi_{A2}^{n-1}$ e as equações (3.14) e (3.15) se tornam, respectivamente:

$$|D_{10}\rangle = \left| -i\alpha\sqrt{2} \sin\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) \cos\left(\frac{\sum_{n-1} - \sum_n}{4} + \frac{\varphi_{B2}^{n-1}}{2}\right) e^{i\left(\frac{\sum_{n-1} + \sum_n}{4} + \frac{\varphi_{B2}^{n-1}}{2}\right)} \right\rangle \quad (3.16)$$

e

$$|D_{11}\rangle = \left| -\alpha\sqrt{2} \sin\left(\frac{\varphi_{A1}^n - \varphi_{A2}^n}{2}\right) \sin\left(\frac{\sum_{n-1} - \sum_n}{4} + \frac{\varphi_{B2}^{n-1}}{2}\right) e^{i\left(\frac{\sum_{n-1} + \sum_n}{4} + \frac{\varphi_{B2}^{n-1}}{2}\right)} \right\rangle \quad (3.17)$$

Quando Alice quer transmitir o bit ‘1’ ela faz $\varphi_{A1} - \varphi_{A2} = \pi$. Se houver detecção em D_{10} ou em D_{11} significa bit ‘1’ para o protocolo QSDC.

Bob junta os bits obtidos na parte superior e inferior do seu aparato para ter uma única sequência de bits que será comparada com a de Alice para estimar a taxa de erro e, conseqüentemente, para inferir a presença ou não de Eva.

3.2. Análise da Probabilidade de Erros Causados por Eva

Para mostrar que a ação de um espião (Eva) poderia causar um erro no esquema do DQPS-QKD, deve-se considerar que Eva usa um divisor de feixes para fazer a interferência dos pulsos vindos de Alice. Desde que a diferença de fase 0 ou π seja totalmente distinguível, Eva sempre obterá o valor correto do bit enviado por Alice. Mas ocorre que Eva nunca terá certeza sobre os seus valores porque a diferença de fase usada por Alice não é suficiente para que Eva saiba quais fases ela usou. O resultado dessa incerteza de Eva é a introdução de erros no protocolo DQPS-QKD que denunciará a sua presença.

Supondo que Alice queira enviar a sequência ‘00’, ela tem que fazer $\varphi_{A1}^n - \varphi_{A2}^n = 0$ e também $\varphi_{A1}^{n-1} - \varphi_{A2}^{n-1} = 0$. As possibilidades para que Alice faça isso são mostradas no Quadro 3.1.

Quadro 3.1 - Escolhas de Alice para enviar ‘00’

$(\varphi_{A1}^n, \varphi_{A2}^n)$	$(\varphi_{A1}^{n-1}, \varphi_{A2}^{n-1})$	Σ_n	Σ_{n-1}	$(\Sigma_n - \Sigma_{n-1})/2$
(0, 0)	(0, 0)	0	0	0
(0, 0)	$(\pi/2, \pi/2)$	0	π	$-\pi/2$
(0, 0)	(π, π)	0	2π	$-\pi$
(0, 0)	$(3\pi/2, 3\pi/2)$	0	3π	$\pi/2$
(π, π)	(0, 0)	2π	0	π
(π, π)	$(\pi/2, \pi/2)$	2π	π	$\pi/2$

(π, π)	(π, π)	2π	2π	0
(π, π)	$(3\pi/2, 3\pi/2)$	2π	3π	$-\pi/2$
$(\pi/2, \pi/2)$	$(0, 0)$	π	0	$\pi/2$
$(\pi/2, \pi/2)$	$(\pi/2, \pi/2)$	π	π	0
$(\pi/2, \pi/2)$	(π, π)	π	2π	$-\pi/2$
$(\pi/2, \pi/2)$	$(3\pi/2, 3\pi/2)$	π	3π	$-\pi$
$(3\pi/2, 3\pi/2)$	$(0, 0)$	3π	0	$-\pi/2$
$(3\pi/2, 3\pi/2)$	$(\pi/2, \pi/2)$	3π	π	π
$(3\pi/2, 3\pi/2)$	(π, π)	3π	2π	$\pi/2$
$(3\pi/2, 3\pi/2)$	$(3\pi/2, 3\pi/2)$	3π	3π	0

Fonte: o autor

Analisando o primeiro caso da quadro, onde Alice faz φ_{A1}^n e φ_{A2}^n iguais a 0 e φ_{A1}^{n-1} e φ_{A2}^{n-1} também iguais a 0, tem-se que a diferença de fase entre os dois pulsos é 0.

Eva tem 16 combinações possíveis para fazer com que a diferença de fase entre os pulsos seja 0 (todos os casos do Quadro 3.1).

Supondo que Eva escolha quaisquer das quatro seguintes combinações de ângulos para os pulsos que ela enviará para Bob $(0, 0)$ e $(0, 0)$, (π, π) e (π, π) , $(\pi/2, \pi/2)$ e $(\pi/2, \pi/2)$, $(3\pi/2, 3\pi/2)$ e $(3\pi/2, 3\pi/2)$ e que Bob escolha 0 para φ_B , tem-se que a probabilidade de Eva causar erro de bit em Bob é de 0%. Esta constatação vem a partir da análise da função cosseno da equação (3.9), que terá como resultado $(\cos(\Sigma_{n-1} - \Sigma_n)/4 + \varphi_{B1}^{n-1}/2) = \cos(0) = 1$, e da função seno da equação (3.10), que terá como resultado $(\sin(\Sigma_{n-1} - \Sigma_n/4 + \varphi_{B1}^{n-1}/2) = \sin(0) = 0$.

Mas se ao invés dessas quatro combinações de ângulos, Eva escolher quaisquer das oito seguintes combinações $(0, 0)$ e $(\pi/2, \pi/2)$, $(0, 0)$ e $(3\pi/2, 3\pi/2)$, (π, π) e $(\pi/2, \pi/2)$, (π, π) e $(3\pi/2, 3\pi/2)$, $(\pi/2, \pi/2)$ e $(0, 0)$, $(\pi/2, \pi/2)$ e (π, π) , $(3\pi/2, 3\pi/2)$ e $(0, 0)$, $(3\pi/2, 3\pi/2)$ e (π, π) e Bob escolher 0 para φ_B , tem-se que a probabilidade de Eva causar erro de bit em Bob é de 50%. Analisando a função cosseno da equação (3.9), que terá como resultado $(\cos(\Sigma_{n-1} - \Sigma_n/4 + \varphi_{B1}^{n-1}/2) = \cos(\pi/4)$, e da função seno da equação (3.10), que terá como resultado $(\sin(\Sigma_{n-1} - \Sigma_n/4 + \varphi_{B1}^{n-1}/2) = \sin(\pi/4)$, percebe-se que poderá haver detecção tanto em D_{00} (e neste caso Eva não causará erro) como em D_{01} (e neste caso Eva causará erro) com a mesma probabilidade.

O último caso a ser analisado é quando Eva escolher quaisquer das quatro seguintes combinações (0, 0) e (π , π), (π , π) e (0, 0), ($\pi/2$, $\pi/2$) e ($3\pi/2$, $3\pi/2$), ($3\pi/2$, $3\pi/2$) e ($\pi/2$, $\pi/2$) e Bob escolher 0 para φ_B , tem-se que a probabilidade de Eva causar erro de bit em Bob é de 100%. Novamente analisando as equações (3.9) e (3.10), obtém-se $(\cos(\Sigma_{n-1} - \Sigma_n/4 + \varphi_{B1}^{n-1}/2)) = \cos(\pi/2) = 0$ e $(\sin(\Sigma_{n-1} - \Sigma_n/4 + \varphi_{B1}^{n-1}/2)) = \sin(\pi/2) = 1$. Neste caso, haverá detecção apenas em D_{01} , fazendo com que todos os bits estejam errados.

Calculando a probabilidade de Eva causar erro em Bob quando Alice quiser enviar a sequência '00', tem-se

$$P_e = \frac{4}{16} \cdot \frac{1}{2} \cdot 0 + \frac{8}{16} \cdot \frac{1}{2} \cdot \frac{1}{2} + \frac{4}{16} \cdot \frac{1}{2} \cdot 1 = \frac{1}{4} = 25\%. \quad (3.18)$$

Avaliando o caso de Alice enviar a sequência '11', ou seja quando $\varphi_{A1}^n - \varphi_{A2}^n = \pi$ e também $\varphi_{A1}^{n-1} - \varphi_{A2}^{n-1} = \pi$, tem-se todas as possibilidades mostradas na Quadro 3.2.

Quadro 3.2 - Escolhas de Alice para enviar '11'

$(\varphi_{A1}^n, \varphi_{A2}^n)$	$(\varphi_{A1}^{n-1}, \varphi_{A2}^{n-1})$	Σ_n	Σ_{n-1}	$(\Sigma_n - \Sigma_{n-1})/2$
(0, π) (π , 0)	(0, π) (π , 0)	π	π	0
(0, π) (π , 0)	($\pi/2$, $3\pi/2$) ($3\pi/2$, $\pi/2$)	π	2π	$-\pi/2$
($\pi/2$, $3\pi/2$) ($3\pi/2$, $\pi/2$)	(0, π) (π , 0)	2π	π	$\pi/2$
($\pi/2$, $3\pi/2$) ($3\pi/2$, $\pi/2$)	($\pi/2$, $3\pi/2$) ($3\pi/2$, $\pi/2$)	2π	2π	0

Fonte: o autor

A probabilidade de Eva causar erro em Bob também é de 25% para a sequência '11'.

Quando lasers diferentes são utilizados no mesmo esquema óptico, o processo de modulação fica muito complicado, pois além da diferença de fase entre φ_{A1} e φ_{A2} também é necessário levar em conta as fases iniciais dos lasers a fim de que se possa identificar qual a diferença de fase selecionada (0 ou π) e conseqüentemente qual o bit enviado. Para

evitar este problema e também a necessidade de ter dois *links* de fibra óptica, utiliza-se o esquema óptico apresentado na Figura 3.2, onde as polarizações horizontal e vertical fazem as vezes dos canais ópticos.

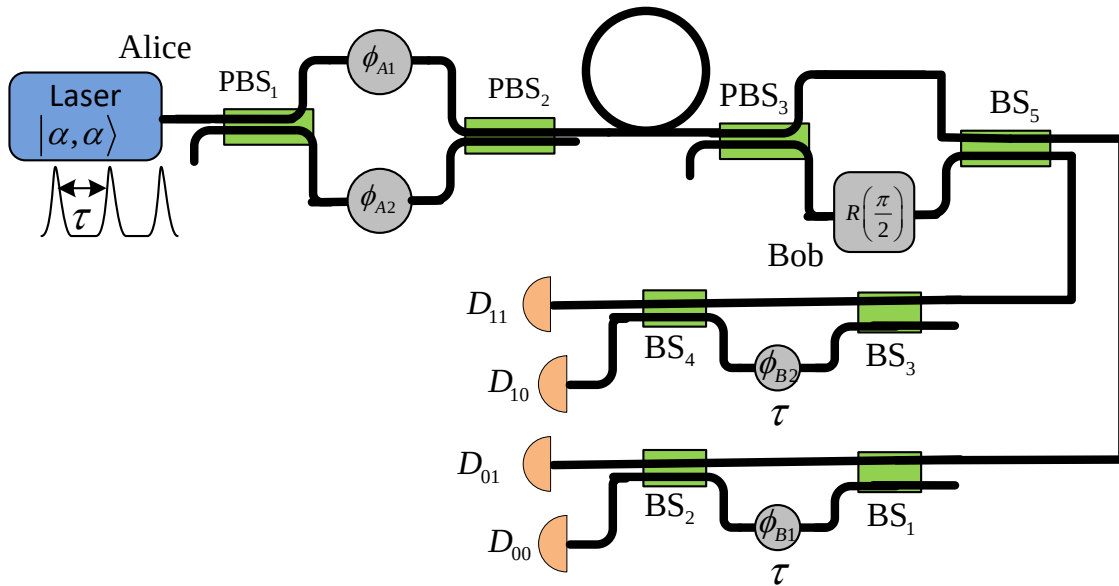


Fig. 3.2. Esquema óptico para QSDC empregando dois DQPS-QKD e usando diversidade de polarização.

Os PBS1,2,3 são divisores de feixe por polarização enquanto R é um rotacionador de polarização.

Fonte: o autor

3.3. Conclusão

A principal vantagem do esquema óptico apresentado neste capítulo é a relativa facilidade de implementação com a tecnologia atual. Com relação à segurança, apenas os ataques do tipo intercepta-reenvia foram analisados na seção 3.2, entretanto, o esquema apresentado é baseado na DQPS-QKD, portanto, é seguro contra os ataques em que este último também o é como, por exemplo, o ataque por divisão de feixes.

A desvantagem é com relação à utilização de estados coerentes com baixo número médio de fótons, pois isso implica na necessidade de ter que executar o protocolo várias vezes a fim de transmitir a informação completa.

O esquema proposto não evita que Eva conheça a informação enviada por Alice, entretanto, Alice e Bob saberão quando Eva ataca. Na prática, essa limitação reduz as

possibilidades de aplicação prática do QSDC aqui apresentado, pois a informação enviada de Alice para Bob terá que ser descartada quando um ataque for detectado.

Finalmente, além da mensagem enviada, Alice e Bob também compartilham uma chave segura ' K ' (a mesma usada para inferir sobre a presença de Eva) que pode ser usada posteriormente em algumas tarefas de criptografia, como por exemplo um desafio de Bob para Alice (Bob questiona Alice sobre a solução de um problema matemático, por exemplo). A resposta para o desafio é S . Assumindo que Alice sabe a solução, ela imediatamente dá a Bob uma informação que prova que ela conhece a resposta, mas ela só a revelará no momento apropriado. Para resolver este problema usando o esquema óptico da Figura 3.2, Alice envia, através do QSDC, o resultado da aplicação de uma função *hash* em S para Bob, $H_l(S)$, onde l determina a função *hash* usada, conhecida apenas por Alice. Quando Alice decide revelar a resposta, ela envia $K \oplus S_1$ para Bob, onde a *string* de bits S_1 é uma concatenação entre a solução S e a informação l da função *hash*. Bob, por sua vez, faz $K \oplus S_1 \oplus K$, obtendo S_1 . A partir de S_1 ele recupera l e S e calcula $H_l(S)$. A comparação dessa informação com a enviada por Alice durante a etapa do QSDC revelará se Alice conhecia a informação naquele tempo. Se elas foram iguais, Bob aceitará que Alice conhecia a resposta quando ela foi desafiada.

Capítulo 4

Conclusões e Perspectivas de Trabalhos Futuros

4.1. Conclusões

Este trabalho apresentou um esquema óptico que executa comunicação quântica segura direta (QSDC) usando distribuição quântica de chaves com deslocamento diferencial de fase em quadratura (DQPS-QKD).

O esquema proposto apresenta algumas vantagens, como:

- O esquema é totalmente implementável com a tecnologia atual;
- O esquema herda a segurança do DQPS-QKD e, como consequência, ele é seguro contra todos os ataques em que o DQPS-QKD apresenta segurança;
- No fim do protocolo, além da mensagem que foi enviada deterministicamente de Alice para Bob, eles também compartilham uma chave. Esta chave pode ser usada posteriormente por eles para realizar tarefas de criptografia. Consequentemente, o esquema óptico proposto permite a execução de dois protocolos simultaneamente: QSDC e QKD. Vale ressaltar que o QKD faz a proteção do QSDC.

Apesar de apresentar as vantagens citadas, o esquema também apresenta algumas desvantagens. Tais como:

- O protocolo proposto não evita que Eva conheça a informação enviada de Alice para Bob. Apesar deles saberem quando Eva tiver atacado, a informação que eles trocaram durante o ataque dela deve ser descartada;
- As possibilidades de aplicação prática do protocolo de QSDC proposto ficam reduzidas por causa da limitação apresentada no item anterior;

- O protocolo emprega estados coerentes com baixo número médio de fótons, consequentemente a transmissão da informação completa requererá múltiplas execuções do protocolo, uma vez que vários pulsos ópticos não possuirão fótons. Para tentar compensar essas múltiplas execuções, pode-se utilizar uma codificação simples para simplificar a realização do protocolo. Esta codificação pode ser: cada '0' ('1') lógico é representado por uma sequência de n zeros (uns). Esta repetição do código não reduz a segurança do protocolo uma vez que implica numa execução mais longa do protocolo DQPS-QKD.

4.2. Perspectivas de Trabalhos Futuros

Alguns dos trabalhos futuros que podem ser realizados a fim de complementar este trabalho são:

- Realizar a análise de segurança do protocolo de QSDC aqui proposto contra os ataques não considerados nesta dissertação como ataques do tipo personificação, do tipo negação de serviço, do tipo medição emaranhada, dentre outros;
- Verificar a viabilidade de utilizar o protocolo de QSDC aqui proposto com autenticação;
- Construir o esquema óptico de QSDC aqui proposto em laboratório a fim de realizar a sua análise do ponto de vista prático e comparar os resultados obtidos com os resultados teóricos.

Referências Bibliográficas

- [1] INTERNET.ORG BY FACEBOOK. State of Connectivity 2015 – A Report on Global Internet Access. Disponível em <https://fbnewsroomus.files.wordpress.com/2016/02/state-of-connectivity-2015-2016-02-21-final.pdf>. Acesso em 05 de jan. 2017.
- [2] DELOITTE. Pesquisa FEBRABAN de Tecnologia Bancária 2015. Disponível em <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Relatorio%20-%20Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%C3%A1ria%202015.pdf>. Acesso em 05 de jan. 2017.
- [3] BUSCAPÉ COMPANY. WEBSHOPPERS – 33ª Edição 2016. Disponível em <http://www.ebit.com.br/webshoppers>. Acesso em 05 de jan. 2017.
- [4] SHOR, P.W. Algorithms for quantum computation: discrete logarithms and factoring. In: PROCEEDINGS OF THE 35TH ANNUAL SYMPOSIUM OF FOUNDATION OF COMPUTER SCIENCE, vol. 35, 1994, IEEE Press, p. 124.
- [5] MENDONÇA, F. A. *Análise Teórica e Resultados Experimentais de Sistemas de Distribuição Quântica de Chaves Usando Fótons Isolados e Estados Coerentes Mesoscópicos*. 2006. Dissertação (Mestrado) – Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará, Ceará, 2006.
- [6] BRASSARD, G. Brief History of Quantum Cryptography: A Personal Perspective. 2005. Disponível em <https://arxiv.org/pdf/quant-ph/0604072.pdf>. Acesso em 05 de jan. 2017.
- [7] MENDONÇA, F. A. *Protocolos e Detectores de Fótons para Comunicações Quânticas*. 2011. Tese (Doutorado). – Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará, Ceará, 2011.
- [8] BENNETT, C.H.; BRASSARD, G. Quantum Cryptography: Public key distribution and coin tossing. In: INTERNATIONAL CONFERENCE ON COMPUTERS, SYSTEMS & SIGNAL PROCESSING, 1984. Bangalore, India.

- [9] INOUE, K. Differential Phase-Shift Quantum Key Distribution. *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, 2015.
- [10] MAITRA, A; PAUL, G. A Resilient Quantum Secret Sharing Scheme. *International Journal of Theoretical Physics*, vol. 54, p. 398 – 408, 2015.
- [11] QIN, H.; DAI, Y. Dynamic quantum secret sharing by using d-dimensional GHZ state. *Quantum Information Processing*, vol. 16, 2017.
- [12] PATWARDHAN, S.; MOULICK, S. R.; PANIGRAHI, P. K. Efficient Controlled Quantum Secure Direct Communication Protocols. *International Journal of Theoretical Physics*, vol. 55, p. 3280 – 3288, 2016.
- [13] BEIGE, A.; ENGLERT, B.-G.; KURTSIEFER, C.; WEINFURTER, H. Secure Communication with a Publicly Known Key. *Acta Physica Polonica A*, vol. 101, no. 3, p. 357 – 368, 2002.
- [14] YU, C.-H.; GUO, G.-D.; LIN, S. Quantum Secure Direct Communication with Authentication Using Two Nonorthogonal States. *International Journal of Theoretical Physics*, vol. 52, p. 1937 – 1945, 2013.
- [15] NASCIMENTO, J. C.; RAMOS, R. V. Quantum protocols for transference of proof of zero-knowledge systems. 2010. Disponível em <https://arxiv.org/ftp/arxiv/papers/0705/0705.2580.pdf>. Acesso em 05 de jan. 2017.
- [16] NASCIMENTO, J. C.; RAMOS, R. V. Quantum protocols for zero-knowledge systems. *Quantum Information Processing*, vol. 9, 2010.
- [17] RAMOS, R. V.; NASCIMENTO, J. C. Quantum zero-knowledge protocol using quantum bit commitment without quantum memory. Disponível em <https://arxiv.org/ftp/arxiv/papers/0801/0801.0696.pdf>. Acesso em 05 de jan. 2017.
- [18] WU, B.; SHASTRI, B. J.; PRUCNAL, P. R. Chapter 11 – Secure Communication in Fiber-Optic Networks. In: *Emerging Trends in ICT Security*. Morgan Kaufmann, 2013. p. 173 – 183.
- [19] LO, H.-K.; ZHAO, Y. Quantum Cryptography. *Encyclopedia of Complexity and Systems Science*, Springer New York, v8, p. 7265-7289, 2009.

- [20] BENNETT, C. H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, vol. 68, no. 21, p. 3121 – 2124, 1992.
- [21] SCULLY, M. O; ZUBAIRY, M. S. Quantum Optics. *Cambridge University Press*. 1997. (estados coerente)
- [22] NIELSEN, M. A.; CHUANG, I. L. *Computação Quântica e Informação Quântica*. Editora Bookman.
- [23] INOUE, K.; IWAI, Y. Differential-quadrature-phase-shift quantum key distribution. *Physical Review A*, vol. 79, 2009.
- [24] DENG, F-G.; LONG, G. L. Secure direct communication with a quantum one-time pad. *Physical Review A*, vol. 69, 2004.