DEPARTAMENTO DE CIÊNCIAS E TECNOLOGIA

MESTRADO EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

UNIVERSIDADE AUTÓNOMA DE LISBOA

"LUÍS DE CAMÕES"

O Contributo Quântico para a 4ª Revolução Industrial

Dissertação para a obtenção do grau de Mestre em Engenharia Informática e de Telecomunicações

Autor: João Manuel Grácio Diniz

Orientador: Professor Doutor Mário Pedro Guerreiro Marques da Silva

Número do Candidato: 20140089

Outubro de 2019

Lisboa

Dedicatória

Dedico esta tese a todas as pessoas que me acompanharam neste meu caminho até os dias de hoje, aos meus amigos que alguns deles lutaram para que eu não desistisse, aos professores quem sempre me acompanharam e por último, mas não menos importante, ao meu orientador da dissertação Professor Doutor Mário Marques da Silva.

"A persistência é o caminho do êxito." (Charlie Chaplin)

Resumo

A Quarta Revolução Industrial, também conhecida por Indústria 4.0, encontra-se já a modificar inúmeras áreas humanas, como a mobilidade, habitação, ensino, saúde, economia e sociedade. Usando Robôs, Inteligência Artificial (IA), Big Data, Internet das Coisas (IdC), Computação Quântica e Comunicações Quânticas, a substituição de humanos por máquinas vai ter lugar numa vasta miríade de diferentes áreas. Estas alterações irão provocar o desaparecimento de alguns empregos, com o emprego de outros, requerendo uma grande alteração humana a este novo paradigma.

Como resultado da miniaturização alcançada, e dificuldades de continuar este processo, a Lei de Moore, que definia que a velocidade dos microprocessadores duplicava a cada dois anos, já não se encontra a ser seguida. Por outro lado, a Lei de Gilder, que referia que a largura de banda dos sistemas de comunicações triplica a cada doze meses, também já não está a ser alcançada. A continuação do aumento do processamento e das comunicações tende a ser alcançada com o futuro da computação quântica e com as comunicações quânticas, que assentam na mecânica quântica, e que funcionam à escala do nanómetro. O entrelaçamento é o principal mistério deste novo paradigma, que envolve o processamento de fotões, átomos ou outros elementos, onde o elemento processado passa a ser o qubit, em vez do bit.

Palavras-chave: Quântico; Entrelaçamento; Comunicação; Criptografia.

Abstract

The Fourth Industrial Revolution, also known as Industry 4.0, is already modifying numerous human areas such as mobility, housing, education, health, economy, and society. Using Robots, Artificial Intelligence (AI), Big Data, the *Internet* of Things (IoT), Quantum Computing and Quantum Communications, the replacement of humans by machines will take place in a vast myriad of different areas. These changes will cause the disappearance of some jobs, with the employment of others, requiring a major human change to this new paradigm.

Because of the miniaturization achieved, and difficulties in continuing this process, Moore's law, which stated that the speed of microprocessors doubled every two years, is no longer being followed. On the other hand, Gilder's Law, which stated that the bandwidth of triple communications systems every twelve months, is no longer being reached either. A continued increase in processing and communications tends to be achieved with the future of quantum computing and quantum communications, based on quantum mechanics, that work at the nanometer scale. Entanglement is the main mystery of this new paradigm, which involves the processing of photons, atoms or other elements, where the processed element becomes the qubit instead of the bit.

Keywords: Quantum; Entanglement; Communication; Cryptography.

Índice

Dedicatória 3
Resumo 4
Abstract 5
Índice 6
Lista de Tabelas 10
Lista de Figuras 11
Lista de Siglas e Acrónimos 12
1 Introdução à 4ª Revolução Industrial 13
1.1 Inteligência Artificial 15
1.2 Internet das Coisas Industrial 17
1.3 Big Data 19
1.4 5G 21
1.5 Robôs 22
1.6 Impacto 23
2 Introdução à Computação Quântica 25
2.1 Computação Quântica 26
2.1.1 Tendências em Miniaturização de Computadores 28
2.1.2 Correção de Erros 29
2.1.3 Processamento de Informação Quântica 30
2.1.4 Eletrodinâmica Quântica 31
2.2 Quantização: De Bits para Qubits 32
2.2.1 Notação Bra–ket 32
2.2.2 Representação Vector Ket de um Qubit 33
2.2.3 Estados de Superposição de um Qubit Único 34
2.2.4 Ler o Valor do Bit de um Qubit 35

2.2.5 Física Quântica e Processamento de Informação 38
2.2.6 Registos de Memória Quantum Multi-qubit 39
2.3 O Que é Informação Quântica? 39
2.3.1 A Copiadora Quântica 42
2.3.2 Medição Conjunta 43
2.3.3 Teletransporte Assistido por Entrelaçamento 44
2.3.4 Entrelaçamento 46
2.4 Evolução de um Registo de Memória Quântica: a Equação de Schrödinger 47
2.4.1 Equação de Schrödinger 47
2.4.2 Hamiltonianos 48
2.4.3 Interpretação Computacional 49
2.5 Extrair Respostas de Computadores Quânticos 50
2.5.1 Observar na Mecânica Quântica 50
2.5.2 Observar na Base Computacional 51
2.5.3 Leitura Completa 51
2.5.4 Leitura parcial 52
2.5.5 Realizar Pesquisas com um Computador Quântico 53
2.5.6 Algoritmo de Grover 54
2.5.7 Algoritmo de Shor 55
3 Comunicação Quântica 57
3.1 Teletransporte Quântico 57
3.2 Teorema da Não-Comunicação 60
3.3 Interpretação de Copenhaga 60
3.4 Princípio da incerteza 62
3.5 EPR e a Desigualdade de Bell 63
3.6 Princípio da Localidade 70
3.7 Realismo 71

3.8 Realismo Local ... 72
3.9 Teoria das Variáveis Ocultas ... 72
3.10 Teoria das Variáveis Ocultas Não-Locais ... 73
3.11 Experiência da Dupla Fenda ... 74
3.12 Interpretação de Bohm ... 75
3.13 Dualidade onda-partícula ... 75
4 Criptografia Quântica ... 77
4.1 Distribuição de Chaves Quânticas ... 78
4.2 Troca de Chaves Quânticas ... 79
4.3 Protocolo BB84: Charles H. Bennett e Gilles Brassard (1984) ... 80
4.4 Protocolo E91: Artur Ekert (1991) ... 83
4.5 Reconciliação de informações e amplificação de privacidade ... 84
4.6 Como Funciona a Distribuição de Chaves de Criptografia Quântica ... 85
4.6.1 Como é Usado? ... 86
4.6.2 Transmissão de Dados Usando Fotões ... 87
4.6.3 Criação de Chaves ou Distribuição de Chaves ... 88
4.6.4 Anexando o Bit de Informação no Fotão - Troca de Chave ... 88
4.6.5 Ler Bits de Informação no Lado do Recetor ... 90
4.6.6 Verificação de Chave - Processo Key Sifting ... 90
4.6.7 Deteção de Intercetação ... 91
4.6.8 Key Distillation ... 92
4.7 Ataques ... 93
4.7.1 Interceptar e Reenviar ... 93
4.7.2 Ataque man-in-the-middle ... 95
4.7.3 Denial of Service ... 95
4.7.4 Ataques de Cavalos de Tróia ... 96
4.7.5 Provas de Segurança ... 96

4.7.6 Quantum Hacking 96
4.7.7 Futuro da Segurança 97
4.8 Criptografia Pós-Quântica 98
4.9 Algoritmos Criptográficos Pós-Quântico 99
4.9.1 Criptografia Lattice-based 99
4.9.2 Criptografia Multivariável 99
4.9.3 Criptografia Baseada em Hash 100
4.9.4 Criptografia Baseada em Código 100
4.9.5 Criptografia Isogênica da Curva Elíptica Supersingular 100
4.9.6 Resistência Quântica Chave Simétrica 101
4.9.7 Comparação de Algoritmos 101
4.10 Projeto Open Quantum Safe 102
4.11 Implementações 102
5 Simulação da Quantum Key Distribution 104
5.1 Trabalhos Anteriores e Literatura 105
5.2 Proposta de Kounteya Sarkar, Bikash K. Behera , et al 107
5.3 CNQKD: Exemplo 114
5.4 Análise de Segurança 116
5.4.1 Segurança Fornecida pela Arquitetura de Rede 116
5.4.2 Segurança ao Longo dos Canais Quânticos 118
5.4.3 Segurança ao Longo dos Canais Clássicos 118
5.5 Exemplo e Simulação 119
5.5.1 Simulação de Canal Quântico 119
6 Conclusões 123
7 Trabalho futuro 125
Bibliografia 126

Lista de Tabelas

Tabela 2.1 - Probabilidades de três qubits. 52
Tabela 4.1 - Estado de polarização dos fotões dependendo do valor do bit e da base 81
Tabela 4.2 - Tabela da discussão da chave secreta entre Alive e Bob..... 82
Tabela 4.3 - Estado de polarização dos fotões dependendo do valor do bit e da base 88
Tabela 4.4 - Tabela da discussão da chave secreta entre Alive e Bob..... 89
Tabela 4.5 - Tabela da discussão da chave secreta entre Alive e Bob com Eve. 94
Tabela 4.6 - Comparação dos Algoritmos 101
Tabela 4.7 - Algoritmos suportados para o projeto Open Quantum Safe 102
Tabela 5.1 - Exemplo de duas tabelas que A compartilha cada uma com B e C. 111
Tabela 5.2 - Tabela com a comunicação ao longo dos dois tipos de canais 114

Lista de Figuras

Figura 2.1 - Esfera de Bloch..... 37
Figura 2.2 - Teletransporte clássico..... 41
Figura 2.3 - Copiadora de uma linha de "teletransporte clássico"..... 43
Figura 2.4 - Obtendo medições conjuntas de uma copiadora 44
Figura 2.5 - Teletransporte assistido por entrelaçamento 45
Figura 3.1 - Esquema experimental esquemático para as desigualdades de Bell..... 66
Figura 3.2 - Trajetórias de Bohm. 74
Figura 5.1 - A GUI interativa do IBM Quantum Experience. 107
Figura 5.2 - A rede completa de grafo entre os quatro participantes..... 108
Figura 5.3 - Uma rede típica de canais clássicos e quânticos entre duas partes..... 116
Figura 5.4 - Probabilidade de sofrer um ataque (Y) vs. quantidade de nós (X)..... 117
Figura 5.5 - Um circuito para gerar um par Bell. 119
Figura 5.6 - Um circuito para gerar um estado de GHZ. 119
Figura 5.7 - Histograma a revelar o resultado do circuito do estado da Bell..... 120
Figura 5.8 - Histograma a revelar o resultado do circuito do estado da GHZ. 121

Lista de Siglas e Acrónimos

IA	Inteligência Artificial
IoT	Internet of Things
CEO	Chief Executive Officer
MIT	Massachusetts Institute of Technology
RFID	Radio Frequency Identification
RSSF	Rede de sensores sem fio
TCP/IP	Protocolo de Controle de Transmissão / Protocolo de *Internet*
TI	Tecnologias de Informação
LTE	Long Term Evolution
UMTS	Universal Mobile Telecommunication System
3GPP	3rd Generation Partnership Project
URLLC	Ultra-Reliable Low-Latency Communication
EPR	Einstein-Podolsky-Rosen
QKD	Quantum Key Distribution
AES	Advanced Encryption Standard
ETSI	European Telecommunications Standards Institute
GHZ	Estado Greenberger–Horne–Zeilinger
MD5	Message-digest Algorithm 5
SHA	Secure Hash Algorithms
IBM	International Business Machines Corporation

1 Introdução à 4ª Revolução Industrial

A palavra "revolução" denota uma mudança repentina e radical. Revoluções ocorrem ao longo da história, quando novas tecnologias e novas formas de perceber o mundo desencadeiam uma mudança profunda nos sistemas económicos e estruturas sociais. Dado que a história é usada como um quadro de referência, a aspereza dessas mudanças pode levar anos para se desdobrar [1].

A Primeira Revolução Industrial usou a força da água e do vapor para mecanizar a produção, a Segunda utilizou a energia elétrica para criar a produção em massa, a Terceira recorreu à eletrónica e à tecnologia de informação para automatizar a produção. Atualmente estamos perante uma Quarta Revolução Industrial, que está a erigir-se a partir da Terceira, e tem vindo a desenvolver-se desde meados do século passado e que se caracteriza por uma fusão de tecnologias que está a esbater as linhas entre as esferas física, digital e biológica. Essas novas tecnologias terão impacto em todas as disciplinas, economias e indústrias, e até mesmo desafiarão nossas ideias sobre o que significa ser humano [2].

Algumas pessoas intitulam este tópico como quarta revolução industrial outras de indústria 4.0. Ambas estão corretas. Elas representam a combinação dos sistemas ciber-físicos, a Internet das Coisas e a *Internet* dos Sistemas [2].

A ideia de que as fábricas inteligentes nas quais as máquinas são incrementadas com ligação à *web* e ligadas a um sistema que pode visualizar todas as maquinas de produção, e a tomar decisões por conta própria, é real, e está no bom caminho para mudar a maioria dos nossos trabalhos [2].

Esta tecnologia tem um grande potencial para continuar a ligar biliões de pessoas e máquinas à *Web*, melhorar drasticamente a eficiência de empresas e organizações e ajudar a regenerar o ambiente natural através de uma melhor gestão de ativos, potencialmente até mesmo desfazendo todos os danos que as revoluções industriais anteriores causaram usando energias renováveis em vez de fosseis [2].

"Estamos a bordo de uma revolução tecnológica que transformará fundamentalmente a forma como vivemos, trabalhamos e nos relacionamos. Em sua escala, alcance e complexidade, a transformação será diferente de qualquer coisa que o ser humano tenha experimentado antes", diz Klaus Schwab em [1], Fundador e Presidente Executivo do Forum Económico Mundial, publicou um livro intitulado A Quarta Revolução Industrial, no qual ele descreve como esta quarta revolução é fundamentalmente diferente das três anteriores, que foram caracterizadas principalmente por avanços na tecnologia [1].

No entanto, não se trata apenas de máquinas e sistemas inteligentes. A visão da quarta revolução tecnológica é muito mais ampla. Simultaneamente existem ondas de novos avanços em áreas que vão desde sequência genética até à nanotecnologia, de energias renováveis à computação quântica. É a fusão dessas tecnologias e a sua interação entre os domínios físicos, digitais e biológicos que tornam a quarta revolução industrial fundamentalmente diferente das revoluções anteriores [1].

Nesta revolução, as tecnologias emergentes e as inovações de base ampla estão se difundindo muito mais rapidamente e mais amplamente do que nas anteriores, que continuam a se desdobrar em algumas partes do mundo. A segunda revolução industrial ainda não foi totalmente experimentada por 17% do mundo, já que quase 1,4 bilhão de pessoas ainda não têm acesso à eletricidade. Isto também é verdade para o terceiro revolução industrial, com mais de metade da população mundial, 4 bilhões de pessoas, a maioria das quais vive no mundo em desenvolvimento, sem acesso à *Internet*. *The Spindle* (a marca da primeira revolução industrial) levou quase 120 anos para se espalhar para fora da Europa. Por outro lado, a *Internet* permeou todo o mundo em menos de uma década [1].

A lição da primeira revolução industrial ainda é válida hoje em dia, que é a transformação tecnológica estar sempre em aceleração que é um dos principais determinantes do progresso. O governo e as instituições públicas, assim como o setor privado, precisam de fazer sua parte, mas também é essencial que os cidadãos vejam os benefícios a longo prazo [1].

Klaus Schwab está convencido de que a quarta revolução industrial será tão poderosa, com um grande impacto e um marco histórico tão importante quanto as três anteriores [1].

1.1 Inteligência Artificial

Inteligência artificial é a inteligência similar à humana exibida por mecanismos ou *software*. Também é um campo de estudo académico. Os principais pesquisadores e livros didáticos definem o campo como "o estudo e projeto de agentes inteligentes", onde um agente inteligente é um sistema que percebe o seu ambiente e toma ações que maximizam as suas possibilidades de vir a ter sucesso. John McCarthy, quem criou o termo em 1956 ("numa conferência de especialistas celebrada em Darmouth Colege" Gubern, Román: O Eros Eletrónicos), define este tópico como "a ciência e engenharia de produzir máquinas inteligentes". Esta é uma área de pesquisa da computação dedicada a descobrir métodos ou dispositivos computacionais que possuam ou multipliquem a capacidade racional do ser humano em resolver problemas, pensar ou, de forma ampla, ser mais inteligente. Também pode ser definida como o ramo da ciência da computação que se ocupa do comportamento inteligente [3] ou ainda, o estudo de como fazer os computadores realizarem tarefas que, atualmente, os humanos fazem melhor [4].

O principal objetivo dos sistemas de IA, é executar funções que, caso um ser humano fosse executar, seriam consideradas inteligentes. É um conceito amplo, e que recebe tantas definições quanto damos significados diferentes à palavra Inteligência. Podemos pensar em algumas características básicas desses sistemas, como a capacidade de raciocínio (aplicar regras lógicas a um conjunto de dados disponíveis para chegar a uma conclusão), aprendizagem (aprender com os erros e acertos de forma a, no futuro, agir de maneira mais eficaz), reconhecer padrões (tanto padrões visuais e sensoriais, como também padrões de comportamento) e inferência (capacidade de conseguir aplicar o raciocínio nas situações do nosso cotidiano) [5].

Por meio da Inteligência Artificial, a produção industrial tem-se tornado mais rápida e mais eficaz em comparação a trabalho humano. Além disso, é possível que estes robôs realizem tarefas que uma pessoa não conseguiria, como é o caso de matérias-primas perigosas ou componentes microscópicos. Deixando assim de haver risco fatal para o ser humano no manuseamento destes materiais ou a falta de precisão do ser humano [6].

“A Inteligência Artificial é a combinação de várias tecnologias, que permitem que as máquinas percebam, compreendam, atuem e aprendam por conta própria ou complementem as atividades humanas” [6], explica Tiago Pereira, CEO da Data Science Academy.

“Mas devemos estar atentos, pois, muitos destes robôs não são tão inteligentes assim. Eles até podem realizar tarefas de forma mais habilidosa, mas são programados de forma limitada. Se for preciso algo mais elaborado, é necessário reprograma-lo.” [6], alerta Tiago Pereira.

De acordo com o especialista, o uso desta tecnologia veio a ser mais usada com a Indústria 4.0, e, à medida que a Inteligência Artificial evolui, os seus custos de produção vão diminuindo [6].

“A implementação de algoritmos mais complexos de Inteligência Artificial vem permitir às Indústrias avaliarem a aquisição de novas tecnologias, que permitam solucionar problemas e realizar a tomada de decisão de forma mais complexa e segura” [6], complementa Tiago Pereira.

De acordo com Jones Granatyr, especialista em Inteligência Artificial, a mesma traz 3 grandes vantagens para a indústria:

- A primeira delas é a redução de erros. “Depois de treinados, os algoritmos inteligentes conseguem desempenhar muito bem tarefas que são suscetíveis a erros em processos executados por humanos. Como os algoritmos não são suscetíveis a fatores externos, dificilmente sofrerão consequências destes fatores” [6].

- A segunda vantagem, de acordo com o especialista, está na redução de custos. “Várias lojas de comércio eletrónico ou bancos usam robôs para iniciar um atendimento com o cliente, sendo que o cliente humano só é chamado caso seja um problema mais complexo. Com isso, as empresas podem reduzir custos com funcionários ou, então, alocar os funcionários em áreas mais estratégicas, que possam aumentar o lucro e focar melhor no negócio da empresa” [6].

- A terceira vantagem da Inteligência Artificial na Indústria 4.0 está no aumento de lucro. “Com menos erros e funcionários focados em processos mais importantes, a empresa terá mais tempo para pensar no negócio e deixar outras tarefas a cargo da Inteligência Artificial” [6].

1.2 Internet das Coisas Industrial

A Internet das Coisas surgiu em consequência dos avanços de várias áreas - como sistemas embebidos, microeletrónica, comunicação e sensores. De facto, a Internet das Coisas tem recebido bastante atenção tanto das academias como aa indústria, devido ao seu potencial uso nas mais diversas áreas das atividades humanas [7].

O conceito é, em certa medida, fruto do trabalho desenvolvido pelo Laboratório de *Auto-ID* do Instituto de Tecnologia de Massachusetts (MIT), sobre o uso da identificação por radio frequência (RFID) e rede de sensores sem fio (RSSF). O objetivo do trabalho era, desde o início, criar um sistema global de registro de bens usando um sistema de numeração único - o código eletrónico do produto [7].

A Internet das Coisas é um termo criado em setembro de 1999 por Kevin Ashton, um pioneiro tecnológico Britânico que concebeu um sistema de sensores omnipresentes ligando o mundo físico à *Internet*, enquanto trabalhava em identificação por rádio frequência. Embora a Internet das Coisas é a ligação entre elas sejam os três principais componentes da *Internet*, o valor acrescentado está no preenchimento das lacunas entre o mundo físico e digital nos sistemas [7].

O primeiro dispositivo Internet das Coisas foi desenvolvido por Simon Hackett e John Romkey, após um desafio lançado por Dan Lynch, então presidente da Interop (uma feira anual de tecnologia da informação organizada pela empresa britânica UBM): se eles conseguissem desenvolver uma torradeira que pudesse ser ligada através da *Internet*, o equipamento seria colocado em exposição durante a INTEROP 1990. Motivados pelo desafio Hackett e Romkey desenvolveram uma torradeira ligada a um computador com rede *TCP/IP* que acabou sendo o grande sucesso do evento. No entanto ainda faltava desenvolver um dispositivo que colocasse

o pão na torradeira. Essa dificuldade foi superada um ano depois, com a adição de um pequeno guindaste robótico ao protótipo. Esse guindaste, controlado pela *Internet*, pegava numa fatia de pão e a inseria na torradeira, tornando o sistema totalmente automatizado [8].

Quando falamos de Internet das Coisas Industrial, a primeira coisa que temos de ter em conta são os dispositivos que a compõem – vamos chama-lo de *input*. Em 2008, já havia mais dispositivos ligadas à *Internet* do que pessoas na Terra. Até 2020, a Cisco estima que haverá 50 mil milhões de dispositivos ligados à *Internet*. A explosão de dispositivos não se deve apenas ao crescimento no número de dispositivos ligados à *Internet* a que estamos habituados. Embora o número de *smartphones*, *tablets* e *wearables* tenha aumentado, o crescimento imenso dos dispositivos ligados deve-se ao facto de muitos dispositivos se terem tornado "inteligentes". Desde lâmpadas até maquinaria industrial, passando por chaleiras até robôs – o número de dispositivos que está ligado à *Internet* e é capaz de comunicar com outros sistemas é avassalador [9].

Com dispositivos inteligentes e uma maior dependência de sistemas automatizados, os designers e fabricantes de dispositivos têm de levar em conta vários aspetos. Por exemplo, os dispositivos inteligentes são sistemas que, no fundo, estão "sempre ligados", estando constantemente a recolher dados e a comunicar. Isto requer a evolução de sistemas de baixo consumo de energia para reduzir as despesas correntes de ecossistemas inteligentes. Além disso, quando objetos tradicionais são substituídos por equivalentes "inteligentes", há potenciais problemas de segurança. Como tal, a explosão de dispositivos não só é um desafio em termos de acrescentar volume, complexidade e tráfego ao ecossistema industrial conectado, como cada novo dispositivo representa um potencial ponto fraco a nível de segurança [9].

Os milhares de milhões de dispositivos e redes de elevado desempenho que compõem a Internet das Coisas Industrial vão permitir uma maior automatização, melhores comunicações e maior produtividade. Todavia, o segredo para retirar valor estratégico da Internet das Coisas Industrial que vai revolucionar as indústrias, inovar nos modelos de negócio e concretizar a quarta revolução industrial está nos dados. No ambiente da Internet das Coisas Industrial, os dados de milhares de milhões de dispositivos serão recolhidos em tempo real, transportado através de redes para sistemas TI e de armazenamento [9].

Gerir estes dados é um desafio monumental, uma vez que a vasta maioria deles não será nem valioso nem claramente útil. Por isso, serão necessários algoritmos e análises complexas para decidir que conjuntos de dados específicos vale a pena armazenar e quais devem ser descartados. Além do mais, é necessário fazer perguntas aos dados para os contextualizar face a outros conjuntos de dados. Também precisamos de compreender que os dados precisam de ter prioridade ou ser tratados com um cuidado extremo em termos de privacidade e segurança, tendo por base a sua importância e sensibilidade. As empresas que forem capazes de aproveitar o poder dos dados da Internet das Coisas serão capazes de trabalhar de uma forma que tem mais curiosidade acerca do cliente: utilizando dados para informar as vendas, o marketing, a comunicação e a estratégia [9].

A gestão e análise de dados está no cerne da Internet das Coisas Industrial, pois as empresas precisam de reunir inteligência a partir dos dados produzidos pelos dispositivos para melhor informar as tomadas de decisão operacionais e estratégicas. Os dados são um dos bens mais valiosos que as empresas têm ao seu dispor. Havendo dados a ser recolhidos em tempo real numa escala tão grande, o valor dos dados vai aumentar exponencialmente à medida que a Internet das Coisas Industrial começa a tomar forma [9].

1.3 Big Data

Ao longo das últimas décadas, a quantidade de dados gerados tem crescido de forma exponencial. O surgimento da *Internet* fez sairmos da era do *terabyte* para o *petabyte*, e a Internet das Coisas aumentou de forma abrupta a quantidade de dados gerada [10]. Em 2015, entramos na era do *zetabytes*, e atualmente geramos mais de 2,5 quintiliões de bytes diariamente. A esta quantidade enorme de dados foi dada o nome de *Big Data*. Este termo surgiu em 1997 e o seu uso foi utilizado para nomear essa quantidade cada vez mais crescente e não estruturadas de dados sendo gerados a cada segundo [11].

Quanto mais dados são gerados, maior é o esforço para extrair informações [12], e os centros de dados tiveram que aprender a lidar com o crescimento exponencial de dados gerados e tiveram que desenvolver ferramentas que fossem para além de bancos de dados relacionais e sistemas paralelos de bancos de dados [10]. Sendo assim, a velocidade para obter a informação faz parte do sucesso que o *Big Data* pode proporcionar em sua empresa [12]. O conceito de

Big Data foi definido inicialmente por 3'V [12] mas a literatura mostrou que seu conceito pode ser expandido para 5'V [13], representados pelos seguintes conceitos [12]:

Volume: relacionado à grande quantidade de dados gerados;

Variedade: as fontes de dados são muito variadas, o que aumenta a complexidade das análises;

Velocidade: Devido ao grande volume e variedade de dados, todo o processamento deve ser ágil para gerar as informações necessárias;

Veracidade: A veracidade está ligada diretamente ao quanto uma informação é verdadeira;

Valor: Este conceito está relacionado com o valor obtido desses dados, ou seja, com a "informação útil".

É por isto que o *Big Data* na Indústria é tão importante. Com esta tecnologia uma fábrica pode, por exemplo, armazenar dados de todas as máquinas, robôs, colaboradores, transações comerciais, vendas e transformá-las em informações valiosas. Isso permite uma análise detalhada de toda a cadeia de produção de uma indústria e impacta diretamente na gestão da empresa, nas tomadas de decisão e no funcionamento pleno do sector [14].

Para trabalhar da melhor forma com *Big Data*, é necessário garantir algumas coisas antes. Para armazenar os dados adequadamente, existe uma etapa crucial de *data preparation*, que é o processo de reunir, combinar, estruturar e organizar dados para que possam ser analisados. Esta fase é determinante para uma aplicação de *Big Data* de sucesso. Depois desse processo acontece a mineração dos dados ou *data mining*. É nessa etapa que, com os dados preparados, começam à busca por padrões ou anomalias que possam gerar insights para a Indústria. Numa etapa mais avançada, entram as tecnologias como *machine learning*, para tornar as tomadas de decisão mais inteligentes e automatizadas [14].

O uso de *Big Data* na Indústria permite, principalmente, transformar dados em informações para otimizar produtos e serviços prestados. O que antes era desperdiçado por falta de profissionais capacitados (como cientistas e engenheiros de dados) e estrutura de armazenamento e análise, agora pode ser usado de ponta a ponta. Esta ferramenta permite entender o passado, identificando erros de planeamento, gerir possibilidades de análise do que

acontece hoje dentro e fora da empresa e ainda possibilita olhar com mais certeza para o futuro do negócio, antecipando erros e prever o comportamento dos consumidores. Com isto, existe uma diminuição de erros na produção, redução de custos, operações com melhor desempenho, planeamento estratégico mais preciso por parte dos gestores e criação de sistemas preditivos para manutenção de máquinas. Esses são só alguns dos exemplos das possibilidades do *Big Data* na Indústria [14].

1.4 5G

As comunicações 5G são o novo padrão de comunicações móvel. Tal como nos padrões de comunicação, como o Long Term Evolution (LTE) e o Universal Mobile Telecommunication System (UMTS), os requisitos mínimos de desempenho do 5G foram declarados pela International Telecommunication Union (ITU) sob o nome IMT-2020, em 2015. Para atender a esses requisitos, o Third Generation Partnership Project (3GPP) iniciou o estudo do 5G no lançamento 14 do 3GPP, dedicado principalmente à evolução do LTE. Diferentemente das gerações anteriores de comunicações, o 5G não será apenas um padrão para comunicações sem fio de banda larga. Na verdade, envolverá diferentes casos de uso projetados para cenários muito diferentes. Por esse motivo, a palavra-chave "flexibilidade" estava presente desde os estágios iniciais dos itens de estudo 5G e itens de trabalho do 3GPP [15].

O novo paradigma da indústria 4.0 irá ser beneficiado pelo 5G, não apenas no sentido de ter comunicações, mas também dos diferentes casos de uso, que foram especificamente definidos para permitir novos serviços que vão consideravelmente além do que foi oferecido pelas comunicações moveis sem fio tradicionais [15].

O processo de padronização do 5G começou no lançamento 15 do 3GPP e está dividido em duas fases:

Na primeira fase, o 3GPP uniu esforços para especificar o caso de uso do Enhanced Mobile Broadband (eMBB), que é o caso de uso associado à evolução do 4G. Esta fase foi concluída no último trimestre de 2018 [15].

Na segunda fase, que será associado ao lançamento 16 do 3GPP e será concluído até o final de 2019, será responsável pelos padrões dos restantes casos de uso, nomeadamente ultra-reliable low-latency communications (URLLC) e massive machine-type communications (mMTC). Esta linha do tempo permite que o 3GPP faça uma apresentação final das especificações técnicas do 5G à ITU em 2020 [15].

1.5 Robôs

Um robô é um dispositivo, ou grupo de dispositivos, eletromecânicos ou biomecânicos capazes de realizar trabalhos de maneira autónoma ou pré-programada. Os robôs são comumente utilizados na realização de tarefas em locais mal iluminados, ou em tarefas perigosas para os seres humanos. Os robôs industriais utilizados nas linhas de produção são a forma mais comum de robôs, uma situação que está mudando recentemente com a popularização dos robôs comerciais, desde aspiradores a cortadores de gramas. Outras aplicações são: tratamento de lixo tóxico, exploração subaquática e espacial, cirurgias microscópicas, mineração perigosa, resgate, e localização de minas terrestres. Os robôs também aparecem nas áreas do entretenimento e tarefas caseiras [16].

Ao longo dos últimos anos, Portugal desenvolveu capacidades relevantes de inovação e desenvolvimento no domínio da robótica. Têm emergido atividades empresariais neste domínio e em boa parte devido à atividade de formação e investigação em diferentes universidades e Institutos do Sistema de Ensino Superior Português. Muitas destas atividades são fruto da dinâmica gerada pelo crescente envolvimento em projetos internacionais financiados em regime de competição, e realizados em parceria com instituições de investigação e empresas com relevância mundial em Investigação e Desenvolvimento Tecnológico (I&DT). Este envolvimento é estimulado por um aumento considerável da atenção dada pelas agências de financiamento, como a Comissão Europeia ou a Agência Espacial Europeia, que consideram a robótica como um domínio chave para o desenvolvimento tecnológico para a sociedade do futuro [17].

Alguns cientistas acreditam que os robôs serão capazes de se aproximar a uma inteligência semelhante à humana [18] na primeira metade do século XXI. Mesmo antes destes níveis de inteligência teóricos serem obtidos, especula-se que os robôs podem começar a

substituir os humanos em muitas carreiras com trabalho intensivos. O pioneiro da cibernética Norbert Wiener discutiu alguns destes temas no seu livro *The human use of human beings* em 1950, onde ele especulou que a tomada de trabalhos humanos pelos robôs pode levar a um aumento no desemprego e problemas sociais a curto prazo, porém que a médio prazo isto pode trazer uma riqueza material às pessoas na maioria das nações.

O conceito de que os robôs podem competir ou rivalizar com os humanos é comum. No filme "Eu, Robô" de Isaac Asimov, ele cria as Três Leis da Robótica numa tentativa literária de controlar a competição dos robôs com os seres humanos, estas leis são:

1. Um robô não pode ferir um ser humano, ou, por omissão, permitir que um ser humano seja ferido.
2. Um robô deve obedecer às ordens recebidas dos seres humanos, a não ser no caso de estas ordens entrarem em conflito com a Primeira Lei.
3. Um robô pode proteger a sua própria existência, contanto que tal proteção não entre em conflito com a Primeira ou Segunda Leis.

Infelizmente, este problema pode não ser tão simples de se resolver. Mesmo sem uma programação maliciosa, os robôs e os humanos simplesmente não possuem as mesmas tolerâncias e capacidades corporais, o que pode levar a acidentes [19].

1.6 Impacto

A Quarta Revolução Industrial já está entre nós e precisamos de uma visão holística para entender os seus processos. O nosso relacionamento com a tecnologia é histórico. Pensadores como o filósofo italiano Umberto Galimberti defendem que, sem a tecnologia, não teríamos sobrevivido à magnitude da natureza, pois teria sido graças à tecnologia que pudemos caçar, criar abrigos, vestir, deslocar pelo território em veículos [20].

Na linha do tempo desta relação, o intervalo entre as inovações disruptivas tem sido cada vez mais curto. As transformações que vivemos são tão velozes que temos a sensação de que não conseguimos acompanhá-la. Tal angústia resulta de um facto: o avanço tecnológico é incontornável [20].

A questão é que chegamos a um patamar em que desenvolvemos tecnologias com características inéditas como a autonomia, a capacidade de processamento de dados inalcançável para os humanos tal como *Big Data*, Inteligência Artificial, *Machine Learning*, *Deep Learning*, Impressoras 3D de materiais bio sintéticos não são mais ficção, mas realidades. As consequências desta Transformação Digital são imprevisíveis, no entanto, para compreendermos minimamente o que já está a acontecer, precisamos de observar atentamente os debates, experiencias, acordos e transações internacionais, seja no âmbito político, económico ou científico [20].

"A Quarta Revolução Industrial, finalmente, mudará não apenas o que fazemos, mas também quem somos. Isso afetará a nossa identidade e todas as questões associadas a ela: a sensação de privacidade, as noções do que é nosso, os padrões de consumo, o tempo que dedicamos ao trabalho e ao lazer e como desenvolvemos as nossas carreiras, cultivando as nossas habilidades, como conhecemos as pessoas, e cultivamos os nossos relacionamentos." [1] diz Klaus Schwab no seu livro da Quarta Revolução Industrial.

2 Introdução à Computação Quântica

Nos últimos 50 anos tem havido uma surpreendente miniaturização na tecnologia dos computadores. Considerando que um microprocessador em 1971 continha cerca de 2.300 transístores, um microprocessador moderno do mesmo tamanho contém mais de um bilhão de transístores. Ao longo desta evolução, embora tenha havido várias mudanças de como o *hardware* do computador é implementado, o mesmo modelo matemático fundamental de um computador dominou. No entanto, se as tendências atuais continuarem, os componentes básicos de um computador serão do tamanho dos átomos individuais em tais escalas que a teoria matemática à informática moderna deixará de ser válida. Em vez disso, os cientistas estão a criar uma nova teoria, chamada computação quântica, que é construído sobre o reconhecimento de que um dispositivo de computação que é governado por leis físicas, e em escalas muito pequenas, as leis apropriadas são os da mecânica quântica.

Há duas atitudes que podemos adotar mediante a necessidade exigida ao incorporar os efeitos da mecânica quântica numa máquina de computação. Uma é tentar suprimir os efeitos quânticos e ainda preservar a aparência, mesmo que os elementos computacionais sejam muito pequenos. A outra abordagem é adotar os efeitos quânticos e tentar encontrar formas inteligentes de aprimorá-los e sustentá-los para alcançar objetivos computacionais antigos de novas maneiras. A computação quântica tenta seguir a última estratégia, aproveitando os efeitos quintessenciais quânticos.

Notavelmente, esta nova teoria da ciência quântica da computação prevê que os computadores quânticos serão capazes de executar certas tarefas computacionais em passos fenomenais a menos do que qualquer computador convencional (“clássico”) - incluindo qualquer supercomputador a ser inventado! Essa afirmação ousada é justificada porque os algoritmos disponíveis para computadores quânticos podem aproveitar fenómenos físicos que não estão disponíveis para os computadores clássicos, por mais sofisticados que sejam. Como resultado, os computadores quânticos podem realizar cálculos de maneiras fundamentalmente novas que, na melhor das hipóteses, só podem ser imitados de maneira ineficiente pelos computadores clássicos. Assim, a computação quântica representa uma mudança qualitativa em como a computação é feita, tornando-a de um carácter diferente de todos os avanços anteriores em ciência da computação. Em particular, os computadores quânticos podem realizar

tarefas verdadeiramente sem precedentes, como teletransportar informações, quebrar códigos supostamente “inquebráveis”, gerar números aleatórios reais e durante a comunicação existem mensagens que denunciam a presença de invasores. Capacidades contraintuitivas similares têm sido descobertas, tornando a computação quântica um campo muito ativo e empolgante.

2.1 Computação Quântica

Será que os computadores quânticos podem realizar tarefas impossíveis para os computadores clássicos atualmente? Na verdade, não, porque, em princípio, podemos resolver as equações dinâmicas da mecânica quântica num computador clássico e simular todos os resultados. Daí que problemas classicamente insolúveis, como o problema das máquinas de Turing e a palavra problema na teoria de grupos, também não podem ser resolvidos em computadores quânticos. Mas esse argumento mostra apenas a possibilidade de emular todos os cálculos quânticos num computador clássico e omite a possibilidade de que a eficiência desse procedimento possa ser terrível. A grande promessa da computação quântica reside, portanto, na redução do tempo de exponencial ao tempo polinomial no caso do algoritmo de fatorização de Shor. Essa redução é comparável a substituir a tarefa de contar todo o caminho até um número de 137 dígitos simplesmente tendo que escrevê-lo. Não importa quais sejam as constantes nas leis de crescimento para o tempo de computação (e elas provavelmente não serão muito favoráveis para o concorrente quântico), o tempo polinomial vai vencer se estivermos realmente interessados em fatorizar números muito grandes [21].

Uma palavra de cautela é necessária aqui sobre a impossível / possível. Embora seja verdade que nenhum algoritmo de fatorização clássica em tempo polinomial é conhecido, e isso é o que conta do ponto de vista prático, não há prova de que tal algoritmo não exista. Este é um estado de coisas típico na teoria da complexidade, porque a inexistência de um algoritmo é uma afirmação sobre o conjunto bastante desajeitado de todos os programas da máquina de Turing. Uma prova, inspecionando todos eles, obviamente está fora, então teria que ser baseada em algum princípio de “conservação de dificuldades”, que raramente existe para problemas da vida real. Um problema em que isso é possível é identificar qual elemento (único) de uma lista grande tem uma certa propriedade (“agulha em um palheiro”). Neste caso, a estratégia óbvia de inspecionar cada elemento, por sua vez, pode ser mostrada como sendo a ótima clássica, e tem um tempo de execução proporcional ao comprimento N da lista. Mas o algoritmo quântico

de Grover realiza a tarefa na ordem de √N etapas, um ganho incrível, mesmo que não seja exponencial. Portanto, existem problemas para os quais os computadores quânticos são comprovadamente mais rápidos do que qualquer computador clássico [21].

Então, o que faz a redução do tempo de funcionamento funcionar? Isso não é tão fácil de responder, mesmo depois de trabalhar com o algoritmo de Shor e verificar a alegação de aceleração exponencial. Entrelaçamento maciço é usado no algoritmo, então este é certamente um elemento importante. Em seguida, há uma técnica conhecida como paralelismo quântico, em que uma computação quântica é executada numa superposição coerente de todas as entradas clássicas possíveis e, em certo sentido, todos os valores de uma função são computados simultaneamente. Uma paráfrase cativante, atribuída a D. Deutsch, é chamar isso de computação nos mundos paralelos da interpretação de muitos mundos [21].

Mas talvez a melhor maneira de descobrir o que é a computação quântica de poderes é revogá-la e tentar realmente a emulação clássica. A dificuldade prática que se torna imediatamente evidente é que as dimensões do espaço de Hilbert crescem extremamente rápido. Para N qubits (sistemas de dois níveis), deve-se operar em um espaço de Hilbert com dimensões de 2^N. O espaço correspondente das matrizes de densidade tem 22 dimensões. Para bits clássicos, tem-se um espaço de configuração de 2 pontos discretos, e o análogo das matrizes de densidade, as densidades de probabilidade, vivem num espaço meramente 2^N-dimensional. Simulações de força bruta de todo o sistema, tendem a parar mesmo em sistemas relativamente pequenos. Feynman foi o primeiro a inverter isso, talvez e apenas um sistema quântico possa ser usado para simular um sistema quântico, e talvez, enquanto estivermos nisso, possamos ir além da simulação e fazer alguns cálculos interessantes também. Então, colocando-o positivamente, num sistema quântico, nós temos exponencialmente mais dimensões para trabalhar, há muito espaço em Hilbert e a complexidade adicional das correlações quântica versus clássica. Ou seja, o fenómeno do entrelaçamento, também é uma consequência disso. Mas não é tão fácil usar essas dimensões extras. Por exemplo, para transmissão de informação clássica um sistema N-qubit não é melhor do que um sistema clássico de N-bit. Apenas a ajuda do entrelaçamento da codificação superdensa traz as dimensões adicionais. Da mesma forma, os computadores quânticos não aceleram todos os cálculos, mas são bons somente em tarefas específicas em que as dimensões extras podem ser colocadas em jogo [21].

2.1.1 Tendências em Miniaturização de Computadores

A tecnologia dos computadores foi levada a escalas cada vez menores porque, em última análise, o fator limitante na velocidade dos microprocessadores é a velocidade com que as informações podem ser movimentadas dentro do dispositivo. Ao juntar os transístores mais próximos e evoluir para mecanismos cada vez mais rápidos de comutação, pode-se acelerar a taxa de computação. Mas há um preço a pagar. À medida que os transístores são colocados juntos, torna-se mais desafiador remover o calor que eles dissipam. Assim, em qualquer estágio do desenvolvimento tecnológico, existe uma densidade ótima de transístores que comercializa o tamanho para a componente térmica [22].

Em 1965, Gordon Moore, cofundador da Intel, notou que as densidades dos transístores economicamente mais favoráveis em circuitos integrados pareciam ter dobrado aproximadamente a cada 18 meses. Ele previu que esta tendência continuaria no futuro. De facto, a escala antecipada de Moore ficou conhecida como a mais oficial "Lei de Moore". No entanto, não é uma lei no sentido científico adequado, pois a natureza não a aplica. Em vez disso, a Lei de Moore é meramente uma observação empírica de uma regularidade de escala no tamanho dos transístores e na dissipação de energia que a indústria havia alcançado, e Gordon Moore extrapolou para o futuro. No entanto, há incerteza na indústria de chips que hoje em dia ponham em causa a Lei de Moore ou que ela possa ser sustentada [22].

No entanto, nos 40 anos desde que a Lei de Moore foi inventada, sucessivas gerações de *chips* da Intel aderiram a ela surpreendentemente. Isso é ainda mais surpreendente quando se percebe o quanto a tecnologia dos transístores fundamentalmente mudou [22].

Hoje, muitos especialistas do sector vêm a Lei de Moore por apenas duas ou três gerações de microprocessadores na melhor das hipóteses. Em um valente esforço para sustentar o Moore's Law, os fabricantes de chips estão usando arquiteturas de microprocessadores *multi-core* e novos materiais semicondutores exóticos. Além desses avanços, uma mudança para a nanotecnologia pode ser necessária [22].

Seja qual for a estratégia adotada pela indústria para manter a Lei de Moore, é claro que, com o passar do tempo, cada vez menos átomos serão usados para implementar mais e mais bits [22].

2.1.2 Correção de Erros

Num computador clássico, a solução para este problema é a digitalização: cada bit é realizado por um circuito biestável, e qualquer desvio dos dois estados desejados é restaurado pelo circuito às custas de alguma energia e com alguma geração de calor. Isso funciona separadamente para cada bit, então, de certa forma, cada bit tem o seu próprio banho de calor. Mas essa estratégia não funcionará para computadores quânticos: para começar, há agora uma continuação de estados puros que teriam que ser estabilizados para cada qubit e, em segundo lugar, um banho de calor por qubit destruiria rapidamente o entrelaçamento e, portanto, a computação quântica seria impossível de existir. Há muitas indicações de que o entrelaçamento é de facto mais facilmente destruído pelo ruído térmico e outras fontes de erros; isto é sumariamente referido como *Quantum decoherence*. Por exemplo, um canal gaussiano (este é um tipo especial de canal infinito-dimensional) tem capacidade infinita para informação clássica, não importa quanto ruído adicionemos. Mas a sua capacidade quântica cai para zero se adicionarmos mais ruído clássico do que o especificado pelas relações de incerteza de Heisenberg. Uma técnica padrão para estabilizar a informação clássica é a redundância: basta enviar um bit clássico três vezes e decidir no final por maioria de votos qual bit a tomar. É fácil ver que isso reduz a probabilidade de erro da ordem ε para a ordem ε^2. Mas, mecanicamente quântica, este procedimento é proibido pelo teorema da não-clonagem: nós simplesmente não podemos fazer três cópias para iniciar o processo [21].

Felizmente, a correção quântica de erros é possível apesar de todas as dúvidas. Como a correção de erros clássica, ela também funciona distribuindo a informação quântica por vários canais paralelos, mas faz isso de uma maneira muito mais subtil do que a cópia. Usando cinco canais paralelos, pode-se obter uma redução similar de erros da ordem ε para a ordem ε^2 [21].

2.1.3 Processamento de Informação Quântica

O estado de um qubit contém todas as suas informações. Este estado é frequentemente expresso num vetor na esfera de Bloch. Esse estado pode ser alterado aplicando transformações lineares ou portas quânticas a eles. Estas transformações unitárias (mecânica quântica) são descritas como rotações na Esfera de Bloch. Enquanto as portas clássicas correspondem às operações familiares da lógica booleana, as portas quânticas são operadores físicos unitários como se pode analisar nos seguintes parágrafos:

- Devido à volatilidade dos sistemas quânticos e à impossibilidade de copiar estados, o armazenamento de informações quânticas é muito mais difícil do que armazenar informações clássicas. No entanto, com o uso de informações quânticas de correção de erros quânticos ainda podem ser armazenadas de forma confiável, em princípio. A existência de códigos de correção de erro quântico também levou à possibilidade de computação quântica tolerante a falhas [21].

- Bits clássicos podem ser codificados e subsequentemente recuperados de configurações de qubits, através do uso de portas quânticas. Por si só, um único qubit não pode transmitir mais que um bit de informação clássica acessível sobre sua preparação. No entanto, na codificação superdensa, um emissor, agindo num dos dois qubits entrelaçados, pode transmitir dois bits de informações acessíveis sobre o seu estado conjunto a um recetor (superposição) [21].

- A informação quântica pode ser movida, num canal quântico, semelhante ao conceito de um canal de comunicação clássico. As mensagens quânticas têm um tamanho finito, medido em qubits. Os canais quânticos têm uma capacidade de canal finito, medida em qubits por segundo [21].

- A informação quântica, e as mudanças na informação quântica, podem ser medidas quantitativamente usando algo semelhante à entropia de Shannon, chamado entropia de von Neumann [21].

- Em alguns casos, algoritmos quânticos podem ser usados para realizar cálculos mais rapidamente do que em qualquer algoritmo clássico conhecido. O exemplo mais famoso disso é o algoritmo de Shor que pode fatorizar números em tempo polinomial, comparado aos melhores algoritmos clássicos que tomam tempo sub-exponencial. Como a fatorização é uma parte importante da segurança da criptografia RSA, o algoritmo de Shor provocou o novo campo da criptografia pós-quântica que tenta encontrar esquemas de criptografia que permanecem seguros mesmo quando computadores quânticos estão em jogo. Outros exemplos de algoritmos que demonstram a supremacia quântica incluem o algoritmo de busca de Grover, onde o algoritmo quântico fornece uma aceleração quadrática sobre o melhor algoritmo clássico possível. A classe de complexidade de problemas eficientemente solucionáveis por um computador quântico é conhecida como BQP (do inglês B*ounded Error Quantum Polynomial Time*) [21].

- A *Quantum Key Distribution* (QKD) permite a transmissão incondicionalmente segura das informações clássicas, ao contrário da criptografia clássica, que pode ser quebrada em teoria, se não na prática. Alguns pontos sobre a segurança do QKD ainda estão a ser debatidos com grande entusiasmo [21].

2.1.4 Eletrodinâmica Quântica

Na física de partículas, a *Quantum Electrodynamics* (EDQ) é a teoria do campo quântico relativista da eletrodinâmica. Em suma, descreve como a luz e a matéria interagem e é a primeira teoria em que se alcança uma concordância total entre a mecânica quântica e a relatividade especial. A EDQ descreve matematicamente todos os fenómenos envolvendo partículas eletricamente carregadas interagindo por meio de troca de fotões e representa a contrapartida quântica do eletromagnetismo clássico, fornecendo uma descrição completa da interação de matéria e luz [23].

Em termos técnicos, o EDQ pode ser descrito como uma teoria de perturbação do vácuo quântico eletromagnético. Richard Feynman chamou-a de "a joia da física" pelas suas previsões extremamente precisas de grandezas como o momento magnético irregular do eletrão e o desvio de *Lamb* dos níveis de energia do hidrogênio [23].

2.2 Quantização: De Bits para Qubits

Felizmente, os sistemas quânticos possuem certas propriedades que servem para codificar bits como estados físicos. Quando medimos o *spin* de um eletrão, um valor é chamado de *spin up* ou $|\uparrow\rangle$ que significa que o spin foi encontrado como paralelo ao eixo ao longo da qual a medição foi feita. A outra possibilidade, *spin-down* ou $|\downarrow\rangle$, significa que o spin foi encontrado como anti-paralelo ao eixo ao longo da qual a medição foi feita. Essa discrição intrínseca de uma manifestação de quantização permite que o spin de um eletrão seja considerado como um dígito binário natural ou bit [24].

Esta discrição intrínseca não é exclusiva nos sistemas de spin. Qualquer sistema quântico de dois estados, como o plano de polarização de um fotão polarizado linearmente, a direção de rotação de um fotão polarizado circularmente ou os níveis discretos de energia em um átomo excitado, funcionariam igualmente bem. Qualquer que seja a forma física exata escolhida, se um sistema quântico for usado para representar um bit, chamamos o sistema resultante de um bit quântico, ou apenas qubit [24].

2.2.1 Notação Bra–ket

Na mecânica quântica, a notação bra-ket é uma notação padrão para descrever estados quânticos. Também pode ser usado para indicar vetores abstratos e funcionais lineares em matemática. A notação usa *angle bracket* (os símbolos $\langle$ e $\rangle$) e uma barra vertical (o símbolo |), para indicar o produto escalar de vetores ou a ação de um funcional linear num vetor num espaço vetorial complexo. O produto ou ação escalar é escrito como: $\langle\Phi|\Psi\rangle$ [25]

A parte direita é chamada de *ket* que é tipicamente representado como um vetor de coluna, e escrito por $|\Psi\rangle$ [25].

A parte esquerda é chamada de *bra* é o operador adjunto do ket com o mesmo rótulo, tipicamente representado como um vetor de linha, e escrito por $\langle\Phi|$ [25].

2.2.2 Representação Vector Ket de um Qubit

Como já se falou sobre bits e qubits, então, será melhor encontrarmos uma maneira de distingui-los. Para isso, adotamos uma notação inventada pelo físico britânico Paul Dirac, que desde então se tornou conhecida como *Dirac-notation* [25].

Na *Dirac-notation*, quando estamos a falar de um qubit (um bit quântico) num estado físico que representa o valor de bit 0, escreveremos o estado do qubit usando um *angle bracket*, $|0\rangle$, que é chamado de *ket* vetor. Da mesma forma, um qubit em um estado físico representando o valor de bit 1 será escrito $|1\rangle$. O que estas notações significam fisicamente dependerá da natureza do sistema que as codifica. Por exemplo, um $|0\rangle$ poderia se referir a um fotão polarizado, ou a um estado excitado de um átomo, ou à direção de circulação de uma corrente supercondutora, etc. A notação fala apenas da abstração computacional que atribuímos a um sistema quântico de dois estados e não nos fornece nenhuma informação direta sobre a incorporação física subjacente do sistema que codifica esse qubit [25].

Matematicamente, os *kets* são uma notação abreviada para vetores de coluna, com $|0\rangle$ e $|1\rangle$ correspondendo a:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

Pode-se pensar nas seguintes perguntas: “Por que precisamos de representar um único bit quântico como um vetor de coluna de dois elementos?” “Não é um dígito binário suficiente para especificá-lo completamente?” A resposta está no facto de que bits quânticos não são restritos. Ou seja, totalmente 0 ou totalmente 1 em um dado instante. Na física quântica, se um sistema quântico puder ser encontrado num conjunto discreto de estados, que escrevemos como $|0\rangle$ ou $|1\rangle$, então, sempre que ele não estiver a ser observado, ele também pode existir numa superposição ou mistura desses estados simultaneamente, $|\psi\rangle = a|0\rangle + b|1\rangle$ tal que $|a|^2 + |b|^2 = 1$ [25].

2.2.3 Estados de Superposição de um Qubit Único

Assim, enquanto num qualquer instante um bit clássico pode ser um 0 ou um 1, um qubit pode ser uma sobreposição de ambos a $|0\rangle$ e $|1\rangle$ simultaneamente, ou seja, um estado como:

$$|\psi\rangle = a|0\rangle + b|1\rangle \equiv \begin{pmatrix} a \\ b \end{pmatrix} \tag{2.2}$$

Onde a, e b são números complexos com a propriedade de $|a|^2 + |b|^2 = 1$ [25]

O coeficiente "a" é chamado de amplitude do componente $|0\rangle$ e o coeficiente "b" é chamado de amplitude do componente $|1\rangle$. A exigência de que $|a|^2 + |b|^2 = 1$ é para garantir que o qubit seja devidamente normalizado. A normalização adequada garante que quando formos finalmente ler um qubit, ele será encontrado, com a probabilidade de $|a|^2$ estar no estado $|0\rangle$ ou, com probabilidade de $|b|^2$ estar no estado $|1\rangle$ e nada mais [25].

Assim, as somas das probabilidades dos possíveis resultados somam um. A notação de Dirac facilita a gravação de descrições compactas de estados quânticos e operadores. Alguns exemplos comuns são os seguintes:

Notação de Dirac: *Bras*, *Kets*, produto interno e produto externo [25].

Para cada *ket* $|\psi\rangle$ existe um *bra* correspondente $\langle\psi|$ (que pode ser visto como um atalho para um vetor de linha). O *ket* e o *bra* contêm informações equivalentes sobre o estado quântico em questão. Matematicamente, eles são o dual um do outro, ou seja:

$$\begin{gathered} |\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \\ \langle\psi| = a^*\langle 0| + b^*\langle 1| = (a^* b^*) \end{gathered} \tag{2.3}$$

Note que as amplitudes no espaço do *bra* são os conjugados complexos das amplitudes no espaço do *ket*. Isto é, se $z = x + iy$ que é um número complexo com parte real x e parte imaginária y, então o complexo conjugado de z é $z^* = x - iy$ [25].

Qual é o propósito de introduzir vetores de *bra* na discussão se eles não contêm nenhuma informação nova sobre o estado quântico? Acontece que os produtos de *bra* e *ket* dão-nos uma visão sobre as semelhanças entre dois estados quânticos. Especificamente, para um par de qubits nos estados $|\psi\rangle = a|0\rangle + b|1\rangle$ e $|\Phi\rangle = c|0\rangle + d|1\rangle$, assim podemos definir seu produto interno, $\langle\Psi|\Phi\rangle$ como:

$$\langle\Psi|\Phi\rangle = (\langle\Psi).(\Phi\rangle) = (a^*b^*).\begin{pmatrix} c \\ d \end{pmatrix} = a^*c + b^*d \tag{2.4}$$

O produto interno $\langle\Psi|\Phi\rangle$ que é também chamado de sobreposição entre estados (normalizados) $|\psi\rangle$ e $|\Phi\rangle$ porque varia de zero para estados ortogonais para um estado normalizado idêntico. Podemos verificar isso com um cálculo direto: $\langle\Psi|\Phi\rangle = (a^*b^*).\begin{pmatrix} a \\ b \end{pmatrix} = a^*a + b^*b = |a|^2 + |b|^2 = 1$ [25].

Um segundo produto por ser definido pelo estado $|\psi\rangle = a|0\rangle + b|1\rangle$ e $|\Phi\rangle = c|0\rangle + d|1\rangle$, é o produto externo de $|\Psi\rangle\langle\Phi|$:

$$|\Psi\rangle\langle\Phi| = (|\Psi\rangle).(\langle\Phi|) = \begin{pmatrix} a \\ b \end{pmatrix}.(c^*d^*) = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix} \tag{2.5}$$

que é uma matriz. O produto externo fornece uma maneira muito interessante de descrever a estrutura de operadores unitários, que, como veremos mais adiante, correspondem a portas lógicas quânticas. Por exemplo, uma porta NOT tem uma matriz unitária correspondente NOT = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Em termos de produtos externos, isso também pode ser escrito como NOT = $|0\rangle\langle 1| + |1\rangle\langle 0|$. A fatorização do produto externo da porta NOT mostra uma transformação que ela executa explicitamente. De facto, todas as portas quânticas podem ser melhor entendidas como uma soma de tais produtos externos [25].

2.2.4 Ler o Valor do Bit de um Qubit

No mundo clássico cotidiano, quando lemos, medimos ou observamos, algo que normalmente não a perturbamos no processo. Por exemplo, quando lemos um jornal, não mudamos as palavras na página apenas lendo-as. Além disso, se dez pessoas lessem dez cópias

diferentes da mesma edição do mesmo artigo, todas veriam as mesmas palavras. No entanto, no mundo quântico, não é isso que acontece [25].

Os estados $|0\rangle$ e $|1\rangle$ correspondem aos polos Norte e Sul da esfera de Bloch (Figura 2.1), respetivamente, o eixo que passa por esses pontos é o eixo z. Assim, o ato de ler o valor do bit de um qubit equivale a determinar o alinhamento do seu spin em relação a este eixo z. Se a partícula estiver alinhada *spin-up*, ela está no estado $|0\rangle$. Se estiver alinhado *spin-down*, está no estado $|1\rangle$ [25].

Quando um único qubit no estado $a|0\rangle + b|1\rangle$ é lido (ou "medido" ou "observado"), com relação a algum eixo através do centro da esfera de Bloch, a probabilidade de encontrá-lo no estado $|0\rangle$ ou estado $|1\rangle$ depende dos valores de a e b e da orientação desse eixo. O eixo mais comum a ser usado é aquele que passa pelos pólos norte e sul correspondentes aos estados $|0\rangle$ e $|1\rangle$. Uma medida de um qubit em relação a este eixo é chamada de medida "na base computacional" porque a resposta que obtemos será um dos valores de bit $|0\rangle$ ou $|1\rangle$. O resultado que obtemos, em geral, não é certo, mas depende das amplitudes a e b. Especificamente, a medição do valor de bit de $a|0\rangle + b|1\rangle$ na base computacional produzirá a resposta $|0\rangle$ com probabilidade $|a|^2$ e a resposta $|1\rangle$ com probabilidade $|b|^2$. Estas duas probabilidades somam 1, isto é, $|a|^2 + |b|^2 = 1$ [25].

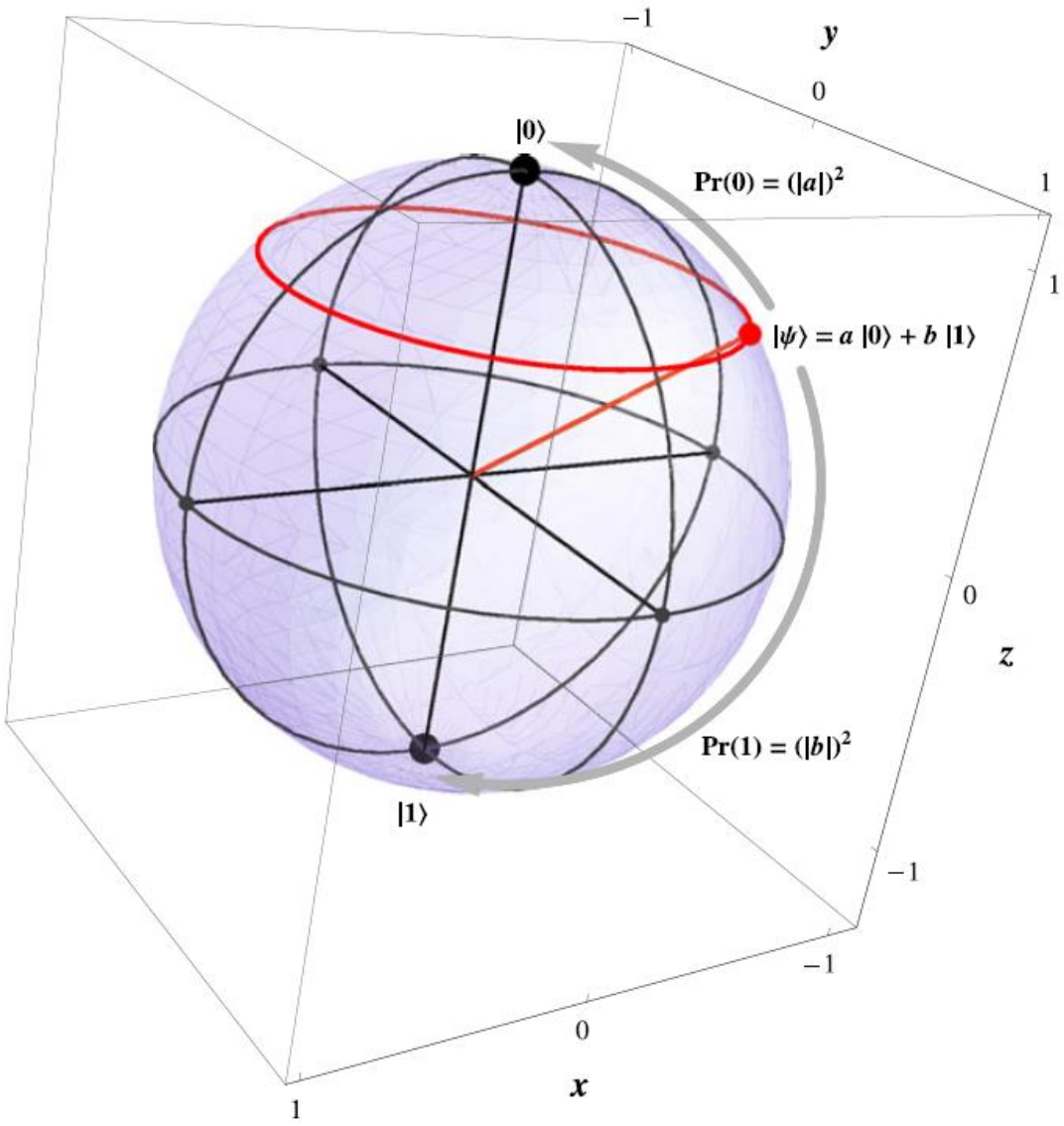

Figura 2.1 - Esfera de Bloch

Fonte: Imagem retirada do documento da Ref. [25]

Assim, um único registo de memória quântica no qubit exibe uma interessante propriedade que mesmo que o seu conteúdo possa ser definido, isto é, pode estar precisamente no estado $|\psi\rangle = a|0\rangle + b|1\rangle$, assim sendo o resultado obtido da leitura é não determinístico. Às vezes, vamos encontrá-lo no estado $|0\rangle$ e, às vezes, vamos encontrá-lo no estado $|1\rangle$. No entanto, no instante após a medição ser feita, o estado é conhecido com certeza de ser $|0\rangle$ ou $|1\rangle$ consistente com o resultado obtido. Além disso, se mantivermos a medição rápida e repetidamente no mesmo estado, poderemos suprimir sua evolução e congelá-la em um estado quântico fixo $|\Psi\rangle \rightarrow|0\rangle \rightarrow |0\rangle \rightarrow|0\rangle\ldots$ ou $|\Psi\rangle \rightarrow|1\rangle \rightarrow|1\rangle \rightarrow|1\rangle\ldots$ esta é uma variante do

chamado efeito Quantum Zeno. Mas, se permitirmos que exista um tempo entre as medições o estado irá evoluir ou ter um desvio, de acordo com a equação de Schrödinger [25].

2.2.5 Física Quântica e Processamento de Informação

Quais são as características comuns desses primeiros desenvolvimentos? O elemento comum desses primeiros desenvolvimentos em criptografia quântica e computação quântica é que todos eles envolvem o processamento prático da informação e são todos fundados e facilitados por fenômenos quânticos característicos. Esses fenómenos, entre os quais o mais proeminente é o entrelaçamento, estão em conflito com os conceitos clássicos de realidade física e localidade. Obviamente, esses primeiros desenvolvimentos sugerem uma ligação profunda entre o conceito de informação e alguns conceitos fundamentais da teoria quântica, o que também é promissor do ponto de vista tecnológico [25].

São esses aspetos tecnologicamente orientados da teoria da informação que estão no cerne do processamento da informação quântica.

Métodos para processar informação quântica desenvolveram-se rapidamente durante os últimos anos. Devido a avanços significativos, fenómenos básicos de interferência e entrelaçamento, que são de interesse central para o processamento de informações quânticas, foram realizados em laboratório em vários sistemas físicos. Esquemas básicos para comunicação quântica foram demonstrados com fotões. Realizações de operações lógicas quânticas elementares foram baseadas em iões aprisionados e em ressonância magnética nuclear. Experiências recentes indicam que, além de configurações eletrodinâmicas quânticas da cavidade, átomos neutros aprisionados que são guiados ao longo de fios magnéticos (chips de átomos) também podem ser úteis para o processamento de informações quânticas. Também tem havido propostas teóricas sobre o uso de átomos *ultracold* em redes óticas, sobre iões em uma matriz de *microtraps* e em dispositivos de estado sólido para a implementação de portas lógicas quânticas [25].

Até agora, o processamento de informação quântica tornou-se um assunto interdisciplinar que atrai não apenas físicos, mas também pesquisadores de outras comunidades. O interesse comum é a aplicação prática e tecnologicamente orientada de

fenômenos quânticos característicos. Neste estágio de desenvolvimento, parece necessário examinar as conquistas recentes e enfatizar os conceitos básicos, gerais e subjacentes, que vêm sendo desenvolvidos gradualmente e que são comumente adotados por todos os pesquisadores neste campo [25].

2.2.6 Registos de Memória Quantum Multi-qubit

Até agora, temos lidado apenas com qubits únicos, mas um dispositivo computacional quântico útil precisará de ter um registador de memória quântico de múltiplos qubits. Em geral, isto é assumido como consistindo numa coleção de n-qubits, que são assumidos como ordenados, indexados e endereçáveis, de modo a que, as operações seletivas possam ser aplicadas a qualquer qubit individual ou a qualquer par de qubits à vontade. Se dois qubits selecionados para uma operação não são fisicamente adjacentes, geralmente há uma sequência operacional que cria uma interação entre eles como se fossem. Esse detalhe é tipicamente omisso do modelo abstrato da memória quântica, já que é mais uma questão de implementação do que qualquer coisa fundamental para o modelo computacional [25].

Assim como um único qubit pode ser encontrado numa superposição dos possíveis valores de bit, ele pode assumir tanto $|0\rangle$ e $|1\rangle$, assim também pode ser encontrado um registo de n-qubit numa superposição de todas as 2^n possíveis sequências de bits $|000...0\rangle$, $|000\ldots1\rangle$, $|111\ldots1\rangle$ que podem ser assumidos. No entanto, os estados de superposição mais interessantes envolvem tipicamente contribuições não uniformes de auto-estados [25].

2.3 O Que é Informação Quântica?

Vamos começar com uma definição preliminar:

“Quantum information is that kind of information which is carried by quantum systems from the preparation device to the measuring apparatus in a quantum mechanical experiment.”[24]

Assim, um "transmissor" de informação quântica nada mais é do que um dispositivo que prepara partículas quânticas, e um "recetor" é apenas um dispositivo de medição. Esta é uma afirmação estranha do ponto de vista da teoria da informação clássica: nesta teoria, uma

pessoa geralmente não se importa com a portadora física da informação, ou então teria que distinguir “informação eletrodinâmica”, “informação impressa”, “Informação magnética” entre muitas outras [24]. De facto, o sucesso da teoria da informação (clássica) depende, em grande parte, da abstração do portador físico e, em vez disso, dos princípios gerais subjacentes a qualquer troca de informações. Então, por que a "informação quântica" deve ser diferente?

Um momento de reflexão deixa claro por que a abstração do portador físico de informações leva a uma teoria bem-sucedida: a razão é que é tão fácil converter informações entre todos esses portadores. A conversão de bytes num disco rígido, para ser gravado num chip, para sinais num cabo, para ondas de rádio via satélite e talvez, finalmente, para uma imagem de um ecrã de computador noutro continente acontece essencialmente sem perdas, e se houver, são perdas pouco significativas, são bem compreendidas e sabe-se como corrigi-las [24]. Portanto, a questão crucial é: a “informação quântica” no texto acima também pode ser convertida nos tipos clássicos de informação, e de volta, sem perda? Ou: há limitações fundamentais para tal tradução e, portanto, a informação quântica é realmente um novo tipo de informação?

A informação quântica é de facto um novo tipo de informação. Mas para tornar isso preciso, vamos ver o que seria necessário para uma tradução bem-sucedida. Vamos começar com a conversão da informação quântica para a informação clássica: um dispositivo para essa conversão tomaria um sistema quântico e produziria como saída alguma informação clássica. Isso não é nada além de uma maneira complicada de dizer “medição”. A tradução reversa, da informação clássica à informação quântica, obviamente envolve alguma preparação de sistemas quânticos. A entrada clássica para tal dispositivo é usada para controlar as configurações do dispositivo de preparação, e qualquer dependência do processo de preparação na informação clássica é admissível. Existem dois tipos de dispositivos que podemos combinar a partir desses dois elementos. Vamos primeiro considerar um dispositivo que vai da informação clássica à quântica e clássica. Esta é uma operação pouco comum. Por exemplo, pode-se codificar um bit clássico no grau de liberdade de polarização de um fotão (claramente um sistema quântico), escolhendo uma das duas polarizações ortogonais para o fotão, dependendo do valor do bit clássico. A leitura é feita por um fotomultiplicador combinado com um filtro de polarização em uma das direções correspondentes. Em princípio, isso permite uma transmissão perfeita. Em certo sentido, toda transmissão de informação clássica é desse tipo,

porque todo sistema físico, em última análise, obedece às leis da mecânica quântica, mesmo que muitas vezes possamos desconsiderar este facto e tratá-lo classicamente [24]. Assim, a informação clássica pode ser traduzida em informação quântica (e de volta).

Mas e o inverso? Isso hipotético (e de facto, impossível)

O processo passou a ser conhecido como teletransporte clássico (Figura 2.2). Isto envolveria um dispositivo de medição M, operando nalguns sistemas quânticos de entrada.

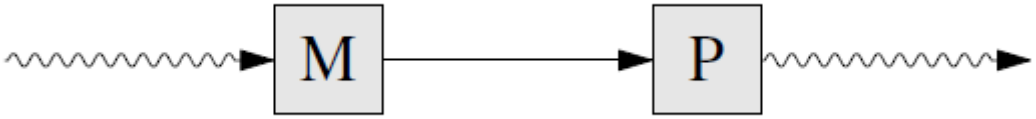

Figura 2.2 - Teletransporte clássico.
Fonte: Imagem retirada do documento da Ref. [24]

Os resultados das medições são subsequentemente introduzidos em uma preparação dispositivo P, que produz a saída final do dispositivo combinado. A tarefa é configurar as coisas de forma que as saídas do dispositivo combinado sejam indistinguíveis das entradas quânticas. Claro, temos que dizer precisamente o que "indistinguível" deve significar. Claramente, isso não pode significar que o “mesmo sistema” saia do outro lado. No caso clássico, isso também não é exigido. O que só pode ser significado na mecânica quântica é que nenhum teste estatístico verá a diferença. Em outras palavras, não importa qual seja a preparação dos sistemas de entrada e, independentemente do que seja observável, medimos as saídas do dispositivo de teletransporte, sempre obteremos a mesma distribuição de probabilidade dos resultados, como se as entradas tivessem sido medidas diretamente. Note também que este critério não envolve os estados de sistemas individuais, mas apenas estados na forma de parâmetros de distribuição de conjuntos de sistemas preparados de forma idêntica [24].

A impossibilidade do teletransporte clássico será tratada extensivamente na seção seguinte, onde está relacionada a uma hierarquia de máquinas impossíveis. No momento, no entanto, vamos dar como certo, e ver o que tudo isso diz sobre o novo conceito de informação quântica [24].

Não é fácil evitar a confusão com um conceito diferente de “informação” usado na linguagem cotidiana, ou seja, o tipo disponível num balcão de informações. A teoria da

informação não se importa se um canal de TV é usado para “desinformação”, mas pode dizer tudo sobre o que é necessário para garantir a qualidade técnica das imagens finais. Assim, as medidas quantitativas de "informação" referem-se todas à capacidade de armazenamento e transmissão, às possibilidades de compressão e correção de erros e assim por diante. Na mesma linha, a teoria da informação quântica não nos dirá qual é o significado de uma "mensagem quântica", e isso provavelmente não tem sentido, porque uma mensagem que foi "lida" é clássica quase que por definição. Mas a teoria quântica da informação tem noções precisas dos recursos necessários para transmitir fielmente essas informações [24].

Em segundo lugar, a transmissão de informação quântica não é de todo um exótico conceito no contexto da física moderna. Pode ser parafraseado de várias maneiras, talvez mais familiares, por exemplo, como “transmissão de estados quânticos intactos”, como “transmissão coerente de sistemas quânticos” ou como transmissão “preservando todas as possibilidades de interferência” do sistema. No entanto, a metáfora da informação é útil, não só porque sugere novas aplicações, mas também porque leva a fazer novas perguntas e leva a noções quantitativas, onde anteriormente havia apenas uma compreensão qualitativa. E possivelmente isso até fornece uma maneira de ver de uma maneira mais clara os velhos enigmas dos fundamentos da mecânica quântica [24].

2.3.1 A Copiadora Quântica

Esta é a máquina mencionada no conhecido artigo de Wootters e Zurek intitulado “Um único quantum não pode ser clonado”. Por definição, uma copiadora seria um dispositivo que toma um sistema quântico como entrada e transforma dois sistemas do mesmo tipo. A condição para chamar isto de uma copiadora é que não seriamos capazes de distinguir um sistema proveniente da saída do sistema de entrada por qualquer teste estatístico, isto é, por meio das probabilidades medidas para qualquer observação, e para qualquer preparação do estado inicial. Portanto, o dispositivo precisa operar em estados "desconhecidos" arbitrários. Claro que uma copiadora no sentido comum, é um retransmissor de e-mail distribuindo e-mail para vários destinatários, de facto, satisfazem essa condição no domínio da informação clássica. Note que poderíamos testar esse dispositivo em eventos únicos, ou mesmo assumir alguma “identidade”

ontológica de entrada e saída: o critério para cópia quântica provem de uma estatística e pode ser verificada por meio de uma coleção direta de testes estatísticos [24].

Dado um dispositivo de teletransporte, construir uma copiadora é muito fácil (Figura 2.3). Tudo o que temos a fazer é lembrar que as informações clássicas obtidas no estágio intermediário do processo de teletransporte podem ser copiadas perfeitamente. Assim, podemos aplicar o dispositivo de medição da linha de teletransporte ao sistema de entrada, copiar os resultados e simplesmente executar a preparação de reconstrução do processo em cada uma dessas cópias [24].

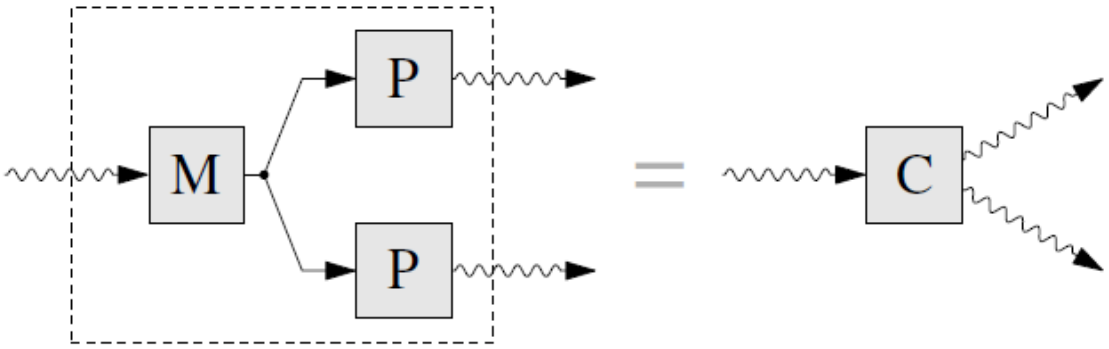

Figura 2.3 - Copiadora de uma linha de "teletransporte clássico".
Fonte: Imagem retirada do documento da Ref. [24]

2.3.2 Medição Conjunta

Esta é a tarefa de combinar dois dispositivos de medição separados em um único dispositivo, ou a “medição simultânea” de dois observáveis quânticos A e B. Assim, um dispositivo de medição conjunto “A & B” é um dispositivo que fornece um par (a, b) de saídas clássicas a cada vez que é operado, tal que a é uma saída possível de A, e b é uma saída possível de B. (Usamos o símbolo A para denotar tanto um observável quanto um dispositivo que mede este observável e similar para B exigimos que as estatísticas dos resultados a sozinhos sejam as mesmas que para o dispositivo A, e similarmente para B. Note que mais uma vez que o nosso critério é estatístico, e pode ser testado sem recorrer a condicionais contra factuais como “o resultado que resultaram se B e “não-A” foram medidos nesta partícula quântica em particular”. Muitos observáveis quânticos não são conjuntamente mensuráveis nesse sentido. Os exemplos mais famosos, posição e momento, diferentes componentes do momento angular

e posições de uma partícula livre em momentos diferentes, provavelmente estão contidos em todo curso de mecânica quântica. Portanto, a impossibilidade de medições conjuntas nada mais é do que uma afirmação precisa de um aspeto de “complementaridade” [24].

No entanto, um dispositivo de medição conjunto para qualquer um destes poderia ser facilmente construído, dado uma copiadora quântica funcional (Figura 2.4): seria simplesmente executar a copiadora C no sistema quântico e, em seguida, aplicar os dois dispositivos de medição, A e B, para as cópias. É fácil ver que a definição da copiadora garante que as estatísticas de a e b saem separadamente. Em outras palavras, uma copiadora pode ser vista como um dispositivo de medição de juntas universais [24].

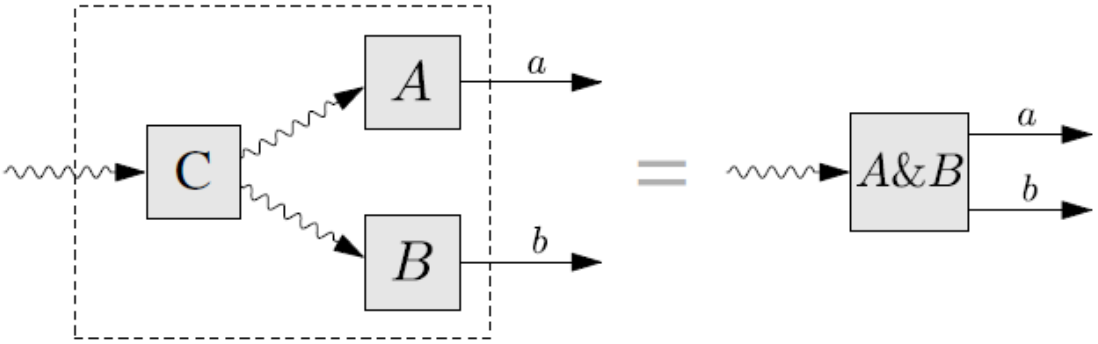

Figura 2.4 - Obtendo medições conjuntas de uma copiadora
Fonte: Imagem retirada do documento da Ref. [24]

2.3.3 Teletransporte Assistido por Entrelaçamento

Esta é sem dúvida a primeira grande descoberta no campo da informação quântica. Os teoremas de não-clonagem e não-teletransporte, embora não tivessem formulado em tais termos, dificilmente teria sido uma surpresa para as pessoas que trabalhavam nos fundamentos da mecânica quântica nos anos 60, digamos. Mas a ajuda do entrelaçamento foi realmente uma reviravolta inesperada. Foi visto pela primeira vez por Bennett et al. Que também cunhou o termo "teletransporte". É gratificante ver, embora não seja uma surpresa na mesma escala, que essa previsão da mecânica quântica também tenha sido implementada experimentalmente [24].

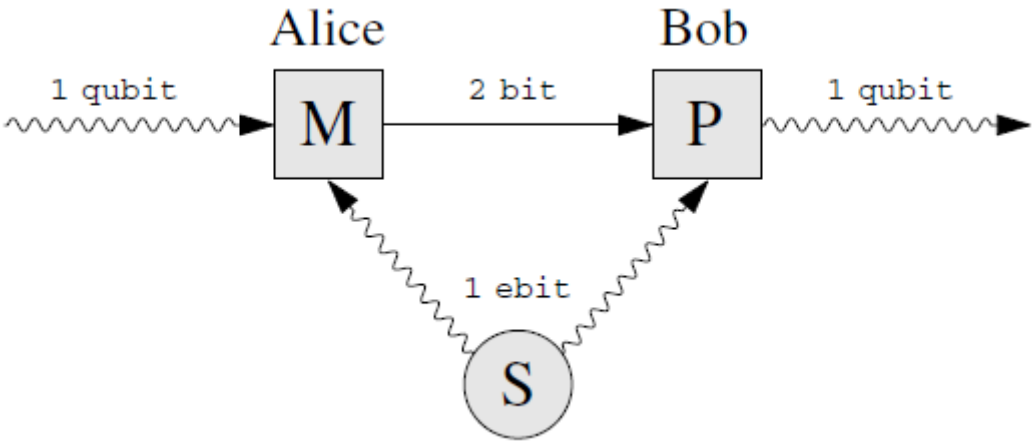

Figura 2.5 - Teletransporte assistido por entrelaçamento

Fonte: Imagem retirada do documento da Ref. [24]

O que o esquema de teletransporte tem de tão surpreendente é que combina duas máquinas cuja impossibilidade foi discutida na seção anterior: omitindo a distribuição do estado de entrelaçamento (a metade inferior da Figura 2.5), obtemos o impossível processo de teletransporte clássico. Por outro lado, se omitirmos o canal clássico, teremos uma tentativa de transmitir informações apenas por meio de correlações, ou seja, uma versão do telefone da Bell. Como a dimensão de tempo não está representada neste diagrama, vamos considerar as etapas na ordem correta. O primeiro passo é que Alice e Bob recebem uma metade de um sistema entrelaçado. A fonte pode ser de terceiros ou pode ser o laboratório de Bob, sendo esta talvez a melhor escolha para fins ilustrativos, porque deixa claro que nenhuma informação está a ser transmitida da Alice para Bob nesse estágio. Agora, Alice irá enviar uma mensagem no sistema quântico cujo estado (que é desconhecido para ela) e para finalidade de teletransporte. Alice então faz uma medição no sistema, combinando a entrada e a sua metade do sistema entrelaçado. Assim, ela envia os resultados através de um canal clássico para Bob, que posteriormente usa-os para ajustar as configurações no seu dispositivo, que então realiza alguma transformação na sua metade do sistema entrelaçado. O sistema resultante desse ajuste é a saída, e, se tudo for escolhido da maneira correta, esses sistemas de saída são, de facto, indistinguíveis estatisticamente das saídas. Para ver exatamente como o estado entrelaçamento S, a medida M e a preparação P precisam de ser escolhidas, é necessário o arcabouço matemático da teoria quântica. No exemplo padrão, um teletransporte de um estado de um qubit, usando um sistema de dois qubits entrelaçados ("1(um) ebit") e enviando 2(dois) bits clássicos de Alice para Bob [24].

2.3.4 Entrelaçamento

Outra maneira pela qual os registos de memória quânticos podem diferir dos registos clássicos de memória é sua capacidade de existir em estados entrelaçados. Este é um estado de um sistema quântico composto que envolve correlações fortes entre partes do sistema. Atualmente, há um debate considerável sobre a natureza do entrelaçamento, especialmente em sistemas que envolvem mais de duas partículas, e se o entrelaçamento é estritamente necessário para obter uma vantagem de complexidade sobre um computador clássico. No entanto, neste momento, parece que o entrelaçamento é crucial para obter as acelerações exponenciais vistas em alguns algoritmos quânticos E o que é exatamente um estado entrelaçado? Em termos mais simples, podemos definir um estado entrelaçado da seguinte maneira:

Definição: Entrelaçamento no estado puro - o estado puro do multi-qubit é entrelaçado se e somente se não puder ser fatorizado no produto direto de um estado definido para cada qubit individualmente. Assim, um par de qubits, A e B, estão entrelaçados se e somente se, o seu estado conjunto $|\Psi\rangle_{AB}$ não puder ser escrito como o produto de um estado para qubit A e um estado para qubit B, isto é, se e somente se $|\Psi\rangle_{AB} \neq |\Psi\rangle_A \otimes |\Psi\rangle_B$ para qualquer escolha de estados $|\Psi\rangle_A$ e $|\Psi\rangle_B$ [24].

Num registo de memória de múltiplos qubits, se os qubits estiverem entrelaçados, as ações executadas em um subconjunto de qubits podem ter um impacto em outro subconjunto de qubits "intocado". Por exemplo, considere um registo de memória de 2 qubits, composto de qubits A e B, no estado $\frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B$. Se o qubit A for medido na base computacional e for encontrado no estado 1, então, mesmo que o qubit B ainda não tenha sido tocado, o seu estado quântico agora está determinado a ser também 1. Assim, uma medição do qubit A teve um efeito colateral no valor de qubit B [24].

O entrelaçamento é um fenómeno generalizado em registos de memória quântica de múltiplos qubits. É também a *cornerstone* de muitos algoritmos quânticos. Por exemplo, podemos preparar dois quânticos entrelaçados, A e B dizem que o registo A contém um conjunto de índices que vão de 0 a 2^n-1 e o registo B contém um conjunto de valores de uma função cujo comportamento depende do valor de o índice no registo A. Então, o estado conjunto (ignorando o fator de normalização) pode ser algo como: $\sum_{i=0}^{2n-1} |i\rangle_A |f(i)\rangle_B$. Medindo

o valor da função (no registo B) como sendo o valor “c”, podemos projetar o conjunto de índices (no registo A) consistente com o valor da função observada, dando-nos uma superposição da forma $\sum_{\{i':f(i')=c\}} |i'\rangle_A|c\rangle$. Isto é um limpo truque porque num tiro obtemos todos os valores de índice (no registo A) que dão o mesmo valor para a função (no registo B) [24].

2.4 Evolução de um Registo de Memória Quântica: a Equação de Schrödinger

Até agora temos discutido as propriedades de bits quânticos individuais (como superposição), e os de registos quânticos de memória multi-qubit (como superposição e entrelaçamento). O artigo lido, supõe que o estado instantâneo de um registo de memória quântica, $|\Psi(t)\rangle$, mantem o estado instantâneo da computação quântica. Mas como este estado evolui com o tempo e como podemos controlar essa evolução para executar uma computação quântica intencional? É ai que a equação de Schrödinger entra [24].

2.4.1 Equação de Schrödinger

Notavelmente em 1929, muito antes de alguém ter pensado em computadores quânticos, o físico Erwin Schrödinger descobriu uma equação que descreve como qualquer sistema quântico isolado evolui no tempo. Desde que um registo de memória quântica é nada mais do que um sistema quântico isolado, também deve ser descrito pela equação de Schrödinger [24].

A equação de Schrödinger é uma equação diferencial parcial determinística linear de primeira ordem que envolve o estado instantâneo do registo de memória quântica $|\Psi(t)\rangle$, uma matriz hermética independente do tempo H, chamada hamiltoniana (o observável para a energia total do sistema), e uma constante igual à constante de Planck dividida por 2π. O facto da equação de Schrödinger ser "linear" significa que as somas da solução para a equação são também soluções para a equação, que é a origem fundamental do princípio da superposição. O facto de a equação de Schrödinger ser determinística significa que, se souber o seu estado instantâneo a qualquer momento, poderá prever com certeza os estados futuros com os estados passados (desde que o sistema não seja observado) [24].

Independentemente dos detalhes precisos do sistema físico, a equação de Schrödinger assume sempre a forma:

$$i\hbar \frac{\partial|\Psi(t)\rangle}{\partial t} = Ĥ|\Psi(t)\rangle \tag{2.6}$$

Como ħ é uma constante, e $|\Psi(t)\rangle$ descreve o estado instantâneo do registo de memória quântica, a forma desta equação implica que todos os detalhes pertencentes ao sistema físico em questão devem ser agrupados no operador Ĥ - o hamiltoniano [24]. Então, o que significa exatamente este hamiltoniano?

2.4.2 Hamiltonianos

Na mecânica quântica, os observáveis são descritos pelos operadores, que por sua vez podem ser representados como matrizes Hermitianas. Os valores permitidos para um observável são os autovalores da sua matriz Hermitiana associada. O Hamiltoniano, Ĥ, é o observável correspondente à energia total do sistema, e os autovalores são os valores possíveis que se pode obter quando se mede (ou se "observa") a energia total do sistema. Dependendo da situação física, um Hamiltoniano pode ser dependente do tempo ou independente do tempo. O Hamiltoniano Ĥ para um sistema físico quântico em particular é construído a partir do conhecimento das interações elementares disponíveis no sistema, e pode ser escrito em termos de produtos de operador como os que encontramos no capítulo "Estados de superposição de um Qubit único". Por exemplo, o processador quântico supercondutor da Hidra [24] tem o Hamiltoniano:

$$Ĥ(t) = \sum_{i=1}^{N} h_i Z_i + \sum_{i<j=2}^{N} J_{ij} Z_i Z_j + \sum_{i=1}^{N} \Delta_i(t) X_i \tag{2.7}$$

Onde $Z_i = \sigma_z^i$ e $X_i = \sigma_x^i$ são as matrizes Paul-Z e Pauli-X para qubit i, h_i é a polarização aplicada ao qubit i, $\Delta_i(t)$ é o elemento da matriz de encapsulamento para qubit i, e J_{ij} é o acoplamento entre os qubits i e j. O facto de que Ĥ é o observável para a energia total do sistema n-qubit significa que Ĥ é uma matriz herita de $2^n \times 2^n$ dimensional tal que exista auto estados de energia $|\Psi_i\rangle$, e auto valores de energia E_i tais que $Ĥ|\Psi i\rangle = E_i|\Psi i\rangle$. Os auto

valores E_i são os únicos valores permitidos na energia total do sistema. Assim, há sempre alguma base (a energia $\{|\Psi_i\rangle\}$) na qual Ħυ é uma $E_2{}^n{}_{-1}$ matriz diagonal $Ħυ = \sum_i E_i\ |\Psi i\rangle\langle\Psi i|$ [24].

$$Ħυ = \begin{pmatrix} E_0 & 0 & 0 & 0 \\ 0 & E_1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & E_2{}^n{}_{-1} \end{pmatrix} \tag{2.8}$$

No entanto, o Hamiltoniano, respeita a relação com algumas outras bases, por exemplo, a base computacional, $\{|00\ldots0\rangle, |00\ldots1\rangle, ..., |11\ldots1\rangle\}$. Assim, às vezes é necessário mudar a base usada para descrever estados e operadores em computação quântica [24].

2.4.3 Interpretação Computacional

Um computador clássico segue essencialmente um ciclo LOAD-RUN-READ, em que um deles carrega dados na máquina, executa um programa usando esses dados como entrada e depois lê o resultado. Para um computador quântico o ciclo é similar, PREPARE-EVOLVE-MEASURE, em que prepara-se um estado quântico, evolui-se o mesmo no computador quântico e mede-se o resultado [24].

Cada aspeto da operação do computador quântico oferece novas oportunidades indisponíveis na fase similar da operação de um computador clássico. Por exemplo, enquanto em um computador clássico só se pode carregar uma entrada por vez, num computador quântico pode preparar exponencialmente muitas entradas na mesma quantidade de tempo. Enquanto num computador clássico só se pode executar uma computação em uma entrada, num computador quântico pode desenvolver uma superposição de cálculos em todas as entradas no mesmo tempo. Finalmente, enquanto num computador clássico só se pode ler uma saída, podemos realizar medições mais sofisticadas do estado de saída de um computador quântico para calcular certas propriedades conjuntas de todas as respostas a um problema computacional específico no tempo que um computador clássico leva para encontrar apenas uma das respostas. Isso dá aos computadores quânticos o potencial de serem muito mais rápidos do que qualquer computador clássico, até mesmo um estado de um supercomputador [24].

2.5 Extrair Respostas de Computadores Quânticos

O processo de extrair respostas de computadores quânticos pode ser mais complicado do que se imagina. Para extrair o resultado na computação quântica, devemos ler o registo de memória quântica que o contém. Tal ato é mais apropriadamente pensado como realizar uma medição num certo estado quântico (ou seja, o resultado da computação quântica) numa determinada base (tipicamente, mas não necessariamente, a base computacional) [24].

2.5.1 Observar na Mecânica Quântica

Uma medição de um registo na memória quântica de um computador quântico não é assim tão fácil como se pensa, é necessário ligar um dispositivo de medição que temporariamente irá capturar informações na memória quântica registada que transferida para o aparelho de medição, após esse processo, a informação é convertida em informação clássica e amplificada para uma escala detetável pelos sentidos humanos (computação clássica). Neste ponto, dizemos que o observável foi "lido" ou "medido". Portanto, o ato de ler um registo de memória quântico é mais uma determinação experimental do valor de algo observável no sistema do que obter um valor exato da operação [24].

Na mecânica quântica, uma observação para qualquer propriedade de um sistema de n-qubit é representada por uma matriz hermitiana de 2^n x 2^n. A propriedade hermitiana significa que $O=O^{\dagger}$ e, assim, os autovalores de O são garantidos como reais. O significado disto é que a mecânica quântica diz que quando a propriedade associada com O observável é medida que a resposta que obtemos tem que ser um dos autovalores de O, e o estado imediatamente após a medição é o autovetor que emparelha com este autovalor. Assim, se $\{|\Psi_i\rangle\}$ são a família de autovetores de O e $\{\lambda i\}$ são a família correspondente de autovalores, [24] tal que:

$$O|\Psi i\rangle = \lambda i|\Psi i\rangle \tag{2.9}$$

Então os únicos valores possíveis que podemos obter para a propriedade associada com O observável são um dos λi's e, tendo obtido tal resultado, o estado imediatamente após esta medição será$|\Psi i\rangle$. Além disso, se repetidamente preparássemos e medíssemos várias preparações do estado $|\Psi\rangle$ então o valor médio que obteríamos seria:

$$\langle O\rangle = \langle\Psi|O|\Psi\rangle \tag{1.10}$$

Onde |Ψi⟩ e O deve ser descrito respetivamente com a mesma base [24].

2.5.2 Observar na Base Computacional

O tipo mais comum de medição que é feito na computação quântica é medir um conjunto de qubits "na base computacional". Com isto queremos dizer que a orientação do spin de cada qubit no registo de memória quântica é medida ao longo de um eixo paralelo ao eixo z da esfera de Bloch, que é o eixo que passa pelos seus polos norte e sul. Quando tal medição é feita, cada qubit será encontrado para ser alinhado ou anti-alinhado com o eixo z correspondente a ser *spin-up* (ou seja, no estado |0⟩) ou *spin-down* (ou seja, no estado |1⟩) respetivamente. Quando tal medição é aplicada a cada qubit num registo de memória quântica de n-qubit, será obtida uma das 2^n configurações de *string* de bit possíveis que o registo pode assumir. A probabilidade de obter resultados diferentes depende da amplitude com a qual cada configuração de cadeia de bits aparece no estado de superposição do registo imediatamente anterior a ela sendo medido [24].

Considere, por exemplo, um registo de memória quântica de n-qubit no estado (normalizado) $\sum_{i=0}^{2^n-1} c_i|i\rangle$ aqui usamos a notação abreviada que |1⟩ realmente significa uma cadeia de bits $|i\rangle \equiv |\mathrm{i}_{n-1} i_{n-2} \ldots . i_2 i_1 i_0\rangle$ tal como $i = 2^0 i_0 + 2^1 i_1 + \cdots + 2^{n-1} i_{n-1}$. O resultado que obtemos dependerá das amplitudes e se medimos alguns ou todos os qubits [24].

2.5.3 Leitura Completa

Se todos os qubits forem medidos na base computacional, obteremos o resultado $|i\rangle$ com probabilidade $|c_i|^2$. Consequentemente, se uma das amplitudes é zero, isto é, existe um valor de índice i' tal que $c_{i'} = 0$, não há qualquer hipótese de obter a resposta da medição. Inversamente, se uma das amplitudes é uma unidade, isto é, existe um valor de índice i'' tal que $c_{i''} = 1$, então se o estado é apropriadamente normalizado, o resultado da medição é garantido como sendo o correspondente ao autoestado [24].

Considere um registo de memória quântica de 3 qubits que inicialmente está no estado

$$|\Psi\rangle = c_0|000\rangle + c_1|001\rangle + c_2|010\rangle + c_3|011\rangle + c_4|100\rangle + c_5|101\rangle + c_6 + c_7|111\rangle \quad (2.11)$$

onde $\sum_{i=0}^{7}|c_i|^2 = 1$. Por conveniência, imagine inserir uma etiqueta no qubit A o mais à esquerda, o qubit B no meio e o qubit C o mais à direita. Quando fazemos uma medição completa de todos os qubits neste registo de memória, esperamos encontrar o resultado |i⟩ com probabilidade $|c_i|^2$ [24]. Ou seja, obtemos os resultados mostrados na tabela seguinte:

Tabela 2.1 - Probabilidades de três qubits.

Qubit A	Qubit B	Qubit C	Probabilidade
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|c_0\|^2$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|c_1\|^2$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|c_2\|^2$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|c_3\|^2$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|c_4\|^2$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|c_5\|^2$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|c_6\|^2$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|c_7\|^2$

Fonte: Tabela retirada do documento da Ref. [24]

2.5.4 Leitura parcial

Em alternativamente, podemos medir apenas o qubit, B no estado |1⟩. Tal medida projeta os qubits numa forma que limita o qubit B a ser |1⟩, mas deixa os outros qubits indeterminados (já que nem os qubits A nem C foram medidos). Além disso, o estado resultante ainda deve ser devidamente normalizado. Assim, após a medição, o estado do registrador de memória de 3 qubits é $\frac{c_2|010\rangle+c_3|011\rangle+c_6|110\rangle+c_7|111\rangle}{\sqrt{|c_2|^2+|c_3|^2+|c_6|^2+|c_7|^2}}$ [24].

Devidamente normalizado - Uma função de onda normalizada significa que a probabilidade de a partícula ser encontrada no domínio considerado é igual a 1 e, portanto, o integral do quadrado da função de onda no domínio é igual a 1 (lembre-se que a função de onda é uma função do complexo variável) [24].

2.5.5 Realizar Pesquisas com um Computador Quântico

"Pesquisar" é uma das tarefas mais universal na ciência da computação. Muitos problemas importantes podem ser resolvidos enumerando as soluções possíveis e, em seguida, pesquisando entre eles, sistematicamente ou aleatoriamente, para determinar quais estão corretas. Em alguns casos, determinar que certas possibilidades são incorretas permite eliminar outras e, portanto, restringir a busca por uma solução verdadeira. Esses problemas de busca são ditos "estruturados". Alternativamente, existem outros problemas de pesquisa nos quais não se aprende nada útil ao descobrir que certas possibilidades são incorretas, além da inutilidade de tentar essas possibilidades novamente. Esses problemas de pesquisa são considerados "não estruturados". Assim, a pesquisa “não estruturada” é um problema de igual modo a tentar “encontrar-a-agulha-no-palheiro” [24].

O algoritmo de Grover fornece um método quântico para resolver problemas de pesquisa não estruturados em aproximadamente a raiz quadrada do número de etapas necessárias usando um computador clássico. Isto equivale a uma aceleração polinomial sobre o que é possível classicamente. Embora essa aceleração não seja tão impressionante quanto a observada em outros algoritmos quânticos, como o algoritmo Deutsch-Jozsa, para o qual é obtido um aumento exponencial, o algoritmo de Grover é aplicável a uma gama muito maior de problemas computacionais. Além disso, um aumento de velocidade quadrático também não é mau. Embora não se consiga resolver problemas com uma escala exponencial de complexidade, poderia, no entanto, permitir que instâncias de problemas significativamente maiores fossem resolvidas do que seria possível de outra forma. Por exemplo, num problema de agendamento de uma companhia aérea, qualquer companhia aérea tem apenas uma quantidade finita de aeronaves e muitas rotas. É bem possível que uma aceleração quadrática seja suficiente para resolver um problema de escalonamento (desde que qualquer sobrecarga de correção de erro quântico requerida não seja muito grande) [24].

2.5.6 Algoritmo de Grover

O algoritmo de Grover é um algoritmo quântico que encontra com alta probabilidade a entrada exclusiva para uma função de caixa preta[1] que produz um valor de saída específico, usando apenas $O(\sqrt{N})$ avaliações da função, onde N é o tamanho do domínio da função. Este algoritmo foi criado por Lov Grover em 1996 [26].

Um problema idêntico na computação clássica não pode ser resolvido em menos de $O(N)$ avaliações (porque, no pior dos casos, o domínio de N pode ser o membro correto). Aproximadamente na mesma época em que Grover publicou o algoritmo, Bennett, Bernstein, Brassard e Vazirani provaram que qualquer solução quântica para o problema precisa avaliar a função $\Omega(\sqrt{N})$ vezes, portanto, o algoritmo de Grover é assintoticamente ótimo [26].

Um computador quântico de variável oculta não local poderia implementar uma pesquisa de um banco de dados N-item no máximo $O(\sqrt[3]{N})$ etapas. Estas etapas são mais rápido que as etapas $O(\sqrt{N})$ tomadas pelo algoritmo de Grover. Nenhum método de busca permitirá que computadores quânticos resolvam problemas NP-Complete em tempo polinomial [27].

Ao contrário de outros algoritmos quânticos, que podem fornecer aceleração exponencial sobre as suas contrapartes clássicas, o algoritmo de Grover fornece apenas um aumento de velocidade quadrático. No entanto, mesmo o aumento de velocidade quadrático é considerável quando N é grande. O algoritmo de Grover poderia forçar brutalmente uma chave criptográfica simétrica de 128 bits em aproximadamente 264 iterações (as iterações chave podem ser usadas apenas com criptografia simétrica). Se um arquivo / texto for criptografado usando a frase secreta, o HASH é calculado e criptografado com o AES por 'n' número de vezes. Se as iterações selecionadas forem 100, isso será feito 100 vezes. Isso é feito para se defender contra-ataques de força bruta), ou uma chave de 256 bits em aproximadamente 2128 iterações. Como resultado, às vezes é sugerido [27] que os comprimentos de chave simétrica sejam duplicados para proteger contra futuros ataques quânticos.

[1] Em teoria dos sistemas, Ciências, Computação e Engenharia, denomina-se caixa preta um sistema fechado de uma complexidade potencialmente alta, no qual a sua estrutura interna é desconhecida ou não é levada em consideração ou em análise, que se limita, assim, a medidas de entrada e saída

Como muitos algoritmos quânticos, o algoritmo de Grover é probabilístico no sentido de dar a resposta correta com uma probabilidade menor que 1. Embora não haja, tecnicamente, um limite superior sobre o número de repetições que pode ser necessário antes que a resposta correta seja obtida, o número esperado de repetições é um fator constante que não cresce com N. O artigo original de Grover descreveu o algoritmo como um algoritmo de procura em bases de dados, e essa descrição ainda é comum. A base de dados nesta analogia é uma tabela de todas as saídas da função, indexada pela entrada correspondente.

2.5.7 Algoritmo de Shor

O algoritmo de Shor é um algoritmo de computador quântico para fatorização inteira. Informalmente, resolve o seguinte problema: dando um número inteiro N, irás encontrar os fatores primos. Que foi inventado em 1994 pelo matemático americano Peter Shor.

Num computador quântico, para fatorizar um inteiro N, o algoritmo de Shor é executado em tempo polinomial (o tempo gasto é polinomial em logN, o tamanho do inteiro dado como entrada). Especificamente, são necessárias portas quânticas de ordem $O((\log N)^2\ (\log\log N)(\log\log\log N))$ usando multiplicação rápida, demonstrando assim que o problema de fatorização inteira pode ser eficientemente resolvido num computador quântico e, consequentemente, na classe de complexidade *bounded-error quantum polynomial time* (BQP). É exponencialmente mais rápido do que o algoritmo mais eficiente de fatorização conhecida, $O(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}})$ [28].

A eficiência do algoritmo de Shor é devida à eficiência da transformação quântica de Fourier e à exponenciação modular por repetidas funções polinomiais.

Se um computador quântico com um número suficiente de qubits pudesse operar sem sucumbir ao ruído quântico e a outros fenómenos de decaimento quântico, o algoritmo de Shor poderia ser usado para quebrar a criptografia da chave pública. O algoritmo Rivest–Shamir–Adleman (RSA) é baseado na suposição de que fatorizar inteiros grandes é computacionalmente intratável. Tanto quanto se sabe, esta suposição é válida para computadores clássicos (não-quânticos). Não se conhece nenhum algoritmo clássico que possa

fatorizar inteiros em tempo polinomial. No entanto, o algoritmo de Shor mostra que os inteiros de fatorização são eficientes num computador quântico ideal, portanto, pode ser viável partir o RSA construindo um grande computador quântico. Foi também um motivador poderoso para o design e construção de computadores quânticos e para o estudo de novos algoritmos de computador quântico. Também facilitou a pesquisa sobre novos sistemas de criptografia que são seguros de computadores quânticos, chamados coletivamente de criptografia pós-quântica [28].

Em 2001, o algoritmo de Shor foi demonstrado por um grupo da IBM, que calculou 15 em 3×5 usando uma implementação NMR de um computador quântico com 7 qubits [29]. Após a implementação da IBM, dois grupos independentes implementaram o algoritmo de Shor usando qubits com fotões, enfatizando que o entrelaçamento multi-qubit fosse observado durante a execução dos circuitos do algoritmo de Shor [30]. Em 2012, a fatorização de 15 foi realizada com qubits no estado sólido. Além disso, em 2012, a fatorização de 21 foi alcançada, estabelecendo o recorde para o maior número inteiro fatorizado com o algoritmo de Shor [31]. Em abril de 2012, a fatorização de $143 = 11 \times 13$ foi alcançada, embora isso usasse computação quântica adiabática em vez do algoritmo de Shor [32]. Em novembro de 2014, descobriu-se que esse cálculo quântico impenetrável de 2012 também havia contabilizado números maiores, sendo o maior número 56153 [33].

3 Comunicação Quântica

3.1 Teletransporte Quântico

Teletransporte quântico é um processo pelo qual informações quânticas (por exemplo, o estado exato de um átomo ou fotão) podem ser transmitidas de um local para outro, com a ajuda de comunicação clássica e entrelaçamento quântico previamente compartilhado entre o envio e local de receção. Como depende da comunicação clássica, que não pode ser executada mais rápida que a velocidade da luz, ela não pode ser usada para transporte ou comunicação. Embora tenha sido possível teletransportar um ou mais qubits de informação entre dois quanta (entrelaçados) [34][35][36].

Teletransporte quântico foi realizado pela primeira vez em fotões individuais, sendo posteriormente demonstrado em vários sistemas de materiais como átomos, iões, eletrões e circuitos supercondutores. A mais recente distância recorde para teletransporte quântico é de 1.400km pelo grupo de Jian-Wei Pan usando o satélite MICIUS para teletransporte quântico baseado no espaço [34][37].

Vários grupos científicos, incluindo um deles liderado pelo Dr. H. J. Kimble do Instituto de Informação Quântica e Matéria da Califórnia, conseguiu teletransportar fotões. Cientistas da Universidade de Arhus, na Dinamarca, reportaram em 2001 que haviam teletransportado o campo magnético produzido por nuvens de átomos. Nas novas experiências, ambas as equipas de cientistas trabalharam com trigêmeos de átomos carregados presos em campos magnéticos. A equipa da Colorado usou berílio, os pesquisadores da Innsbruck usaram cálcio [37].

A proeza do teletransporte é transferir informações do átomo A para o átomo C sem as duas se reunirem. Onde o terceiro átomo, B, é um intermediário. Os três átomos podem ser considerados como caixas que podem conter um 1 ou um 0. A promessa dos computadores quânticos é que tanto um 0 quanto um 1 podem existir ao mesmo tempo, exatamente como a premissa perplexa descrita pelo físico austríaco Erwin Schrödinger em que um gato em uma caixa pode estar simultaneamente vivo e morto até que alguém olhe para dentro [37].

Primeiro, os átomos B e C foram reunidos, tornando-os entrelaçados, criando uma ligação invisível entre os dois átomos, não importando o quão distante eles estão. O átomo C foi afastado. Em seguida, A e B estavam igualmente entrelaçados. Então os cientistas mediram os estados de energia de A e B, essencialmente abrindo as caixas para ver se cada um continha um 1 ou um 0. Como B estava entrelaçado com C, a abertura A e B criaram uma mudança instantânea no átomo C, o que Albert Einstein chamou de "ação assustadora à distância"(Spooky Action), e isso, em essência, estabeleceu uma combinação no átomo C, com os dados de A e B a servir de combinação para a etapa final, transforma o átomo C quase magicamente numa réplica do original A. Assim o átomo A foi teletransportado para o átomo C [37].

"É uma maneira de transferir a informação" [37], disse Rainer Blatt, líder da equipa de Innsbruck.

Um computador quântico poderia usar o teletransporte para mover os resultados dos cálculos de uma parte do computador para outra. "O teletransporte, em princípio, pode ser feito bem rápido", disse o Dr. David J. Wineland, chefe da equipa do Colorado, observando que a movimentação direta de átomos contendo resultados intermediários seria quase certamente lenta demais.

Nas experiências atuais, as distâncias de teletransporte eram uma fração de milímetro, mas, em princípio, os átomos podiam ser teletransportados por distâncias muito maiores. O teletransporte também não foi perfeito, sucedendo cerca de três quartos do tempo [37].

"Ainda não estamos a ir muito bem" e "Todas estas operações precisam de ser melhoradas" [37], disse Dr. David J. Wineland, chefe da equipa do Colorado.

Teletransportar um objeto muito maior, como uma pessoa, parece improvável, se não inteiramente impossível, porque muita informação teria que ser capturada e transmitida. [37].

Mas, o teletransporte está firmemente situado no reino da ficção científica. Podemos nunca ser capazes de teletransportar objetos ou pessoas de um lugar para outro num instante, mas há cenários em que o teletransporte pode ser alcançado. Temos que ter cuidado com o que

exatamente queremos dizer quando dizemos "teletransporte". Existem três tipos diferentes de teletransporte: teletransporte através de um buraco de negro, ou algo similar, onde o corpo é simplesmente transferido para outro lugar. Na serie “Star Trek”, onde as moléculas são desmontadas, irradiadas noutro lugar e remontadas da mesma maneira. E o tipo de problema filosófico em que o corpo é lido e a informação é transmitida para um outro lugar e usada para construir um corpo inteiramente novo a partir de diferentes materiais [38].

Obviamente, teletransportar grandes objetos ou pessoas provavelmente não acontecerá tão cedo. Manter as partículas entrelaçadas por um longo período de tempo, a longas distâncias ou junto com objetos maiores que alguns átomos é muito além do que a tecnologia atual é capaz de fazer. No entanto, esta experiência foi realizado várias vezes com pequenas partículas, e os cientistas conseguiram teletransportar vários eletrões, fotões e até mesmo moléculas inteiras a dezenas de quilômetros. Talvez esta mesma tecnologia seja usada para mandar-nos a nós ou os nossos netos para a lua algum dia. Mas, atualmente o teletransporte quântico ainda não foi alcançado entre algo maior que as moléculas [38].

Um especto importante da teoria da informação quântica é o entrelaçamento, que impõe correlações estatísticas entre sistemas físicos distintos. Essas correlações mantêm-se mesmo quando as medidas são escolhidas e executadas de forma independente, fora do contacto causal entre si, como verificado em experiências de teste de Bell (é uma experiência de física do mundo real projetado para testar a teoria da mecânica quântica em relação ao conceito de realismo local de Einstein). Assim, uma observação resultante de uma escolha de medição feita em um ponto no espaço-tempo parece afetar instantaneamente os resultados em outra região, mesmo que a luz ainda não tenha tido tempo de percorrer a distância. Uma conclusão aparentemente em desacordo com a relatividade especial (descreve a física do movimento na ausência de campos gravitacionais). No entanto, tais correlações nunca podem ser usadas para transmitir quaisquer informações mais rapidamente que a velocidade da luz, uma declaração encapsulada no teorema da não-comunicação. Assim, o teletransporte, como um todo, nunca pode ser superluminal (mais rápido que a luz), pois um qubit não pode ser reconstruído até que a informação clássica que o acompanha chegue.[38].

A compreensão do teletransporte quântico requer uma boa fundamentação em álgebra linear de dimensão finita, espaços de Hilbert e matrizes de projeção. Um qubit é descrito usando

um espaço vetorial bidimensional de valor complexo (um espaço de Hilbert), que é a base primária para as manipulações formais dadas abaixo. Um conhecimento prático da mecânica quântica não é absolutamente necessário para entender a matemática do teletransporte quântico, embora sem tal conhecimento, o significado mais profundo das equações possa permanecer bastante misterioso [38].

3.2 Teorema da Não-Comunicação

Na física, o teorema da não-comunicação ou o princípio de não sinalização é um teorema da teoria da informação quântica que afirma que, durante a medição de um estado quântico entrelaçado, não é possível para um observador, medindo um subsistema do estado total, para comunicar informações a outro observador. O teorema é importante porque, na mecânica quântica, o entrelaçamento quântico é um efeito pelo qual certos eventos amplamente separados podem ser correlacionados de maneiras que sugerem a possibilidade de comunicação instantânea. O teorema da não-comunicação fornece condições sob as quais essa transferência de informação entre dois observadores é impossível. Estes resultados podem ser aplicados para compreender os chamados paradoxos da mecânica quântica, como o paradoxo EPR, ou violações do realismo local obtidas em testes do teorema de Bell. Nessas experiências, o teorema da não-comunicação mostra que a falha do realismo local não leva ao que poderia ser chamado de "comunicação assustadora à distância" (em analogia com a rotulação de Einstein do entrelaçamento quântico como "ação fantasmagórica à distância") [39].

3.3 Interpretação de Copenhaga

A interpretação de Copenhaga é uma expressão do significado da mecânica quântica que foi em grande parte inventada entre 1925 e 1927 por Niels Bohr e Werner Heisenberg. Continua sendo uma das interpretações mais comuns da mecânica quântica.

De acordo com a interpretação de Copenhaga, os sistemas físicos geralmente não têm propriedades definidas antes de serem medidos, e a mecânica quântica só pode prever a distribuição de probabilidade dos resultados possíveis de uma dada medição. O ato de medir afeta o sistema, fazendo com que o conjunto de probabilidades reduza para apenas um dos

valores possíveis imediatamente após a medição. Esse recurso é conhecido como colapso da função de onda [40].

Houve muitas objeções à interpretação de Copenhaga ao longo dos anos. Estes incluem: saltos descontínuos quando há uma observação, o elemento probabilístico introduzido após observação, a subjetividade de requerer um observador, a dificuldade de definir um dispositivo de medição, e a necessidade de invocar a física clássica para descrever o "laboratório" no qual os resultados são medidos [40].

Não há uma declaração exclusivamente definitiva da interpretação de Copenhaga. Ela consiste nas visões desenvolvidas por um número de cientistas e filósofos durante o segundo quarto do século 20. Bohr e Heisenberg nunca concordaram totalmente em como entender o formalismo matemático da mecânica quântica. Bohr uma vez distanciou-se do que ele considerou ser a interpretação mais subjetiva de Heisenberg [40].

Diferentes comentadores e pesquisadores associaram várias ideias a ele. Asher Peres observou que pontos de vista muito diferentes, às vezes opostos, são apresentados como "a interpretação de Copenhaga" por diferentes autores [41].

Alguns princípios básicos geralmente aceitos como parte da interpretação incluem:

- A descrição dada pela função de onda é probabilística. Este princípio é chamado de regra de Born, após Max Born [40].

- As propriedades do sistema estão sujeitas a um princípio de incompatibilidade. Certas propriedades não podem ser definidas em conjunto para o mesmo sistema ao mesmo tempo. A incompatibilidade é expressa quantitativamente pelo princípio da incerteza de Heisenberg. Por exemplo, se uma partícula em um determinado instante tem uma localização definida, não faz sentido falar do seu momento naquele instante [40].

- O funcionamento interno dos processos atômicos e subatômicos é necessariamente e essencialmente inacessível à observação direta, porque o ato de observá-los os afetaria muito [40].

- Quando os números quânticos são grandes, eles referem-se a propriedades que se aproximam muito da descrição clássica. Este é o princípio da correspondência de Bohr e Heisenberg [40].

- Uma função de onda Ψ representa o estado do sistema. Ele encapsula tudo o que pode ser conhecido sobre esse sistema antes de uma observação, não existem "parâmetros ocultos" adicionais. A função de onda evolui suavemente no tempo enquanto está isolada de outros sistemas. [41]

- Durante uma observação, o sistema deve interagir com um dispositivo de laboratório. Quando esse dispositivo faz uma medição, diz-se que a função de onda dos sistemas colapsa ou reduz irreversivelmente a um auto-estado do observável registado [41].

- Os resultados fornecidos pelos dispositivos de medição são essencialmente clássicos e devem ser descritos na linguagem comum. Isto foi particularmente enfatizado por Bohr, e foi aceita por Heisenberg [41].

- A função de onda expressa uma dualidade onda-base necessária e fundamental. Isso deve ser refletido em relatórios de experiências de linguagem comuns. Uma experiência pode vir a mostrar propriedades parecidas com partículas, ou propriedades semelhantes a ondas, de acordo com o princípio de complementaridade de Niels Bohr [41].

3.4 Princípio da incerteza

Na mecânica quântica, o princípio da incerteza (também conhecido como princípio da incerteza de Heisenberg) é uma variedade de desigualdades matemáticas que afirma um limite fundamental para a precisão com certos pares de propriedades físicas de uma partícula, conhecidas como variáveis complementares ou canonicamente variáveis conjugadas, como posição X e momento P, podem ser conhecidas.

Introduzido pela primeira vez em 1927, pelo físico alemão Werner Heisenberg, afirma que quanto mais precisamente a posição de alguma partícula é determinada, com menos precisão o seu momento pode ser conhecido, e vice-versa. A desigualdade formal que relaciona

o desvio padrão da posição σ_x e o desvio padrão do momento σ_p foi derivada por Earle Hesse Kennard mais tarde naquele ano e por Hermann Weyl em 1928

$$\sigma_x \sigma_p \geq \frac{\hbar}{2} \tag{3.1}$$

Onde ħ é a constante reduzida de Planck, h / (2π) [42].

3.5 EPR e a Desigualdade de Bell

Anybody who is not shocked by quantum theory has not understood it.
– Niels Bohr

I recall that during one walk Einstein suddenly stopped, turned to me and asked whether I really believed that the moon exists only when I look at it. The rest of this walk was devoted to a discussion of what a physicist should mean by the term 'to exist'.
– Abraham Pais

...quantum phenomena do not occur in a Hilbert Space[2], they occur in a laboratory.
– Asher Peres

...what is proved by impossibility proofs is lack of imagination.
– John Bell

Quando falamos de um objeto como uma pessoa ou um livro, assumimos que as propriedades físicas desse objeto têm uma existência independente da observação. Isto é, as medições apenas agem para revelar tais propriedades físicas. Por exemplo, uma bola de ténis tem como uma de suas propriedades físicas a sua posição, que normalmente medimos usando a luz a partir da superfície da bola. Quando a mecânica quântica estava a ser desenvolvida nas décadas de 1920 e 1930, surgiu um ponto de vista estranho que difere substancialmente da visão clássica. De acordo com a mecânica quântica, uma partícula não observada não possui propriedades físicas que existam independentemente da observação. Pelo contrário, tais

[2] Na matemática, um espaço de Hilbert é uma generalização do espaço euclidiano que não precisa estar restrita a um número finito de dimensões. É um espaço vetorial dotado de produto interno, ou seja, com noções de distância e ângulos

propriedades físicas surgem como consequência de medições realizadas no sistema. Por exemplo, de acordo com a mecânica quântica, um qubit não possui propriedades definidas de 'spin na direção z, σ_z' e 'spin na direção x, σ_x', cada uma delas pode ser revelada se executarmos a medição apropriada. Em vez disso, a mecânica quântica fornece um conjunto de regras que especificam, dado o vetor de estado, as probabilidades para os possíveis resultados de medição quando o σ_z observável é medido, ou quando o σ_x observável é medido [43].

Muitos físicos rejeitaram esta nova visão da natureza. O objetor mais proeminente foi Albert Einstein. No famoso "EPR paper", em co-autoria com Nathan Rosen e Boris Podolsky, Einstein propôs uma experiência mental que, acreditava ele, demonstrando que a mecânica quântica não é uma teoria completa da natureza [43].

A essência do argumento EPR é a seguinte. O EPR estava interessado no que chamavam de "elementos da realidade". O objetivo do argumento era mostrar que a mecânica quântica não é uma teoria física completa, identificando elementos da realidade que não foram incluídos na mecânica quântica. A maneira como eles tentaram fazer isto, foi introduzir o que eles chamavam ser uma condição suficiente para uma propriedade física ser um elemento da realidade, a saber, que é possível prever com certeza o valor que a propriedade terá, imediatamente antes da medição [43].

Considere, por exemplo, um par entrelaçado de qubits pertencentes a Alice e Bob, respetivamente:

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{3.2}$$

Suponha-se que Alice e o Bob estejam longe um do outro. Alice realiza uma medição de spin ao longo do eixo υ, isto é, ela mede a observação de $\upsilon.\sigma$ (3.1). Suponha-se que Alice receba o resultado +1. Então, um simples cálculo da mecânica quântica, mostra que ela pode prever com certeza que Bob medirá -1 no seu qubit caso ele também meça o spin ao longo do eixo υ. Da mesma forma, se Alice medir -1, então ela pode prever com certeza que Bob medirá +1 no seu qubit. Como é que é possível para a Alice prever o valor do resultado da medição

registado quando o qubit de Bob é medido na direção υ, esta é uma propriedade física que deve corresponder a um elemento da realidade, pelo critério EPR, e deve ser representada em qualquer condição completa da teoria física. No entanto, a mecânica quântica padrão, como a apresentada, apenas informa como calcular as probabilidades dos respetivos resultados de medição de υ.σ. A mecânica quântica padrão não inclui nenhum elemento fundamental destinado a representar o valor de υ.σ, para todos os vetores unitários υ [43].

O objetivo do EPR era mostrar que a mecânica quântica está incompleta, demonstrando que a mecânica quântica carecia de algum elemento essencial da realidade. Eles esperavam forçar um retorno a uma visão mais clássica do mundo, na qual os sistemas poderiam ter propriedades atribuídas que existiam independentemente das medições realizadas nesses sistemas. Infelizmente para o EPR, a maioria dos físicos não aceitou o raciocínio acima como convincente. A tentativa de impor à Natureza propriedades que depende da confiança e que ela deve obedecer parece um modo muito peculiar de estudar as leis [43].

De facto, a natureza riu-se para o artigo EPR. Quase trinta anos após a publicação do artigo EPR, foi proposto um teste experimental que poderia ser usado para verificar se a imagem do mundo em que o EPR esperava forçar o retorno é válida ou não. Acontece que a natureza invalida experimentalmente esse ponto de vista, ao mesmo tempo em que concorda com a mecânica quântica [43].

A chave para esta invalidação experimental é um resultado conhecido como desigualdade de Bell. A desigualdade de Bell não é um resultado da mecânica quântica, então a primeira coisa que precisamos fazer é esquecer momentaneamente todo o nosso conhecimento de mecânica quântica. Para obter a desigualdade de Bell, vamos fazer uma experiência mental, que será analisar o uso das nossas noções do senso comum de como o mundo funciona - o tipo de noções que Einstein e os seus colaboradores pensavam que a natureza deveria obedecer. Depois de se fazer a análise do senso comum, realiza-se uma análise da mecânica quântica que se pode mostrar que não é consistente com a análise do senso comum. A natureza pode então ser questionada, por meio de uma experiência real, a decidir entre as nossas noções de senso comum de como o mundo funciona e a mecânica quântica [43].

Imagine que se realiza a seguinte experiência, ilustrado na figura em infra. Onde Charlie prepara duas partículas. Não importa como ele prepara as partículas, apenas que ele é capaz de repetir o procedimento experimental que ele usa. Depois de realizar a preparação, ele envia uma partícula para Alice e a segunda partícula para Bob [43].

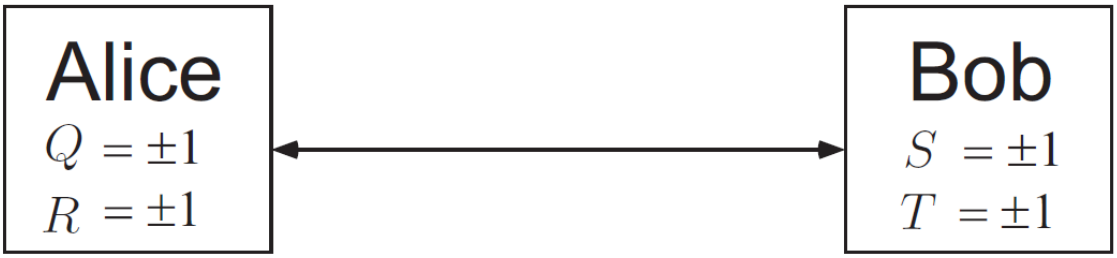

Figura 3.1 - Esquema experimental esquemático para as desigualdades de Bell.
Fonte: Imagem retirada do documento da Ref. [43]

Uma vez que Alice recebe a sua partícula, ela realiza uma medição nela. Imagine que ela tenha disponível dois aparelhos de medição diferentes, para que ela possa escolher entre duas medições diferentes. Essas medições são de propriedades físicas que devemos inserir uma etiqueta com P_Q e P_R, respetivamente. Alice não sabe de antemão qual a medida que irá escolher para realizar a experiência. Em vez disso, quando ela recebe a partícula, ela vira uma moeda ou usa algum outro método aleatório para decidir qual medida realizar. Supomos, por simplicidade, que as medidas podem ter um de dois resultados, +1 ou -1. Suponha que a partícula de Alice tenha um valor Q para a propriedade P_Q. Q é assumido como uma propriedade objetiva da partícula de Alice, que é simplesmente revelada pela medida, da mesma forma que imaginamos a posição de uma bola de tênis a ser revelada pelas partículas de luz espalhada por ela. Da mesma forma, seja R o valor revelado por uma medida da propriedade P_R [43].

Da mesma forma, suponha que Bob seja capaz de medir uma das duas propriedades, P_S ou P_T, mais uma vez revelando um valor S ou T objetivamente existente para a propriedade, cada um tendo valor +1 ou −1. Bob não decide de antemão qual propriedade que ele irá medir, mas espera até que ele tenha recebido a partícula e então escolhe aleatoriamente. A hora exata da experiência é organizada de modo a que, a Alice e o Bob façam as suas medições ao mesmo tempo (ou, para usar a linguagem mais precisa da relatividade, de uma maneira causalmente desconectada). Portanto, à medida que Alice a realiza não pode perturbar o resultado da

medição de Bob (ou vice-versa), uma vez que as influências físicas não se podem propagar mais rapidamente que a luz [43].

Vamos fazer uma simples álgebra com a quantidade QS + RS + RT - QT. Notar que

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T \tag{3.3}$$

Como R, Q = ± 1, segue-se que (Q + R) S = 0 ou (R - Q) T = 0. Em ambos os casos (3.3), é fácil ver que QS + RS + RT - QT = ± 2. Suponha que p (q, r, s, t) seja a probabilidade de que, antes de as medições serem realizadas, o sistema esteja em um estado onde Q = q, R = r, S = s e T = t. Essas probabilidades podem depender de como Charlie realiza a sua preparação e do ruído experimental. Deixando E(·) denotar o valor médio de uma quantidade, temos

$$E(QS + RS + RT - QT) = \sum_{qrst} p(q,r,s,t)(qs + rs + rt - qt) \tag{3.4}$$

$$\leq \sum_{qrst} p(q,r,s,t)\, x2 \tag{3.5}$$

$$= 2 \tag{3.6}$$

Além disso,

$$\begin{aligned} \mathrm{E}(QS + RS + RT - QT) & \\ &= \sum_{qrst} p(q,r,s,t)qs + \sum_{qrst} p(q,r,s,t)rs \\ &+ \sum_{qrst} p(q,r,s,t)rt - \sum_{qrst} p(q,r,s,t)qt \end{aligned} \tag{3.7}$$

$$= \mathrm{E}(QS) + \mathrm{E}(RS) + \mathrm{E}(RT) - \mathrm{E}(QT). \tag{3.8}$$

Comparando (3.7) e (3.8) obtemos a desigualdade de Bell,

$$\mathrm{E}(QS) + \mathrm{E}(RS) + \mathrm{E}(RT) - \mathrm{E}(QT) \leq 2. \tag{3.9}$$

Este resultado também é conhecido como a desigualdade do CHSH após as iniciais de seus quatro descobridores. Faz parte de um conjunto maior de desigualdades conhecidas genericamente como desigualdades de Bell, uma vez que a primeira foi encontrada por John Bell [43].

Repetindo a experiência muitas vezes, Alice e Bob podem determinar cada quantidade no lado esquerdo da desigualdade de Bell. Por exemplo, depois de concluir um conjunto de experiências, Alice e Bob reúnem-se para analisar os seus dados que obtiveram na experiência. Olham para todas elas onde Alice mediu P_Q e Bob mediu P_S. Multiplicando os resultados das experiências juntos, obtiveram uma amostra de valores para QS. Ao calcular a média dessa amostra, eles podem estimar E(QS) com uma precisão limitada apenas pelo número de experiências que realizam. Da mesma forma, podem estimar todas as outras quantidades no lado esquerdo da desigualdade de Bell e, assim, verificar se ela é obedecida numa experiência real. Agora com um pouco de mecânica quântica. Imagine que realizamos a seguinte experiência de mecânica quântica. Charlie prepara um sistema quântico de dois qubits no estado [43]

$$|\Psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{3.10}$$

Ele passa o primeiro qubit para Alice e o segundo qubit para Bob. Após isso, realizam as medições dos seguintes observáveis:

$$Q = Z1 \quad S = \frac{-Z2 - \sqrt{}X2}{\sqrt{2}} \tag{3.11}$$

$$R = X1 \quad T = \frac{Z2 - X2}{\sqrt{2}} \tag{3.12}$$

Cálculos simples mostram que os valores médios do que foi observável, escritos em forma de notação quântica $\langle . \rangle$ são:

$$\langle \mathrm{QS} \rangle = \frac{1}{\sqrt{2}};\ \langle \mathrm{RS} \rangle = \frac{1}{\sqrt{2}};\ \langle \mathrm{RT} \rangle = \frac{1}{\sqrt{2}};\ \langle \mathrm{QT} \rangle = -\frac{1}{\sqrt{2}}; \tag{3.13}$$

Portanto,

$$\langle \mathrm{QS} \rangle + \langle \mathrm{RS} \rangle + \langle \mathrm{RT} \rangle - \langle \mathrm{QT} \rangle = 2\sqrt{2} \tag{3.14}$$

Aprendemos em (3.9) que o valor médio de QS mais o valor médio de RS mais o valor médio de RT menos o valor médio de QT nunca pode exceder dois. No entanto, aqui, na mecânica quântica prevê-se que essa soma das médias aponta para $2\sqrt{2}$ [43].

Felizmente, podemos pedir à natureza que resolva o aparente paradoxo para nós. Experiências inteligentes usando fotões (partículas de luz) foram feitos para validar a previsão

(3.14) da mecânica quântica versus a desigualdade de Bell (3.9) à qual somos levados pelo nosso raciocínio de senso comum. Os detalhes da experiência estão fora do âmbito da dissertação, mas os resultados foram inquestionavelmente a favor da previsão da mecânica quântica. A desigualdade de Bell (3.9) não é obedecida pela natureza [43].

O que será que isto significa? Significa que uma ou mais das suposições que entraram na derivação da desigualdade de Bell devem estar incorretas. Grandes livros foram escritos analisando as várias formas em que os tipos de argumento podem ser usados, e analisando as suposições sutilmente diferentes que devem ser feitas para alcançar as desigualdades semelhantes a Bell. Nesta dissertação só resumo os principais pontos [43].

Há duas suposições feitas na desigualdade de Bell (3.9) que são questionáveis:

1. A suposição de que as propriedades físicas P_Q, P_R, P_S, P_T possuem valores definidos Q, R, S, T que existem independentemente da observação. Isso às vezes é conhecido como a suposição de realismo.

2. A suposição de que Alice esteja a realizar uma medição, não influência o resultado da medição do Bob. Isso às vezes é conhecido como a suposição de localidade.

Estas duas suposições juntas são conhecidas como as suposições do realismo local. Elas são certamente suposições intuitivamente e plausíveis sobre como o mundo funciona e encaixam-se na nossa experiência cotidiana. No entanto, a desigualdade de Bell mostra que pelo menos uma dessas suposições não está correta [43].

O que podemos aprender com a desigualdade de Bell? Para os físicos, a lição mais importante é que suas intuições de senso comum sobre como o mundo funciona estão erradas. O mundo não é localmente realista. A maioria dos físicos toma o ponto de vista de que é a suposição de realismo que precisa ser retirada de nossa visão de mundo da mecânica quântica, embora outros tenham argumentado que a suposição de localidade deveria ser abandonada. Independentemente disso, a desigualdade de Bell, juntamente com evidências experimentais substanciais, agora aponta para a conclusão de que uma ou ambas as localidades e realismo devem ser descartados da nossa visão do mundo caso se queira desenvolver uma boa compreensão intuitiva da mecânica quântica [43].

Uma tarefa importante da computação quântica e da informação quântica é explorar este novo recurso para executar tarefas de processamento de informações impossíveis ou muito mais difíceis com recursos clássicos.

3.6 Princípio da Localidade

Na física, o princípio da localidade afirma que um objeto é diretamente influenciado apenas pelo seu meio de imediato. Uma teoria que inclui o princípio da localidade é considerada uma "teoria local". Esta é uma alternativa ao antigo conceito de "ação à distância" instantânea. A localidade evoluiu a partir das teorias de campo da física clássica. O conceito é que, para que uma ação num ponto possa ter uma influência noutro ponto, algo no espaço entre esses pontos, como um campo, deve mediar a ação. Para exercer uma influência, algo, como uma onda ou partícula, deve percorrer o espaço entre os dois pontos, carregando a influência [44].

A teoria especial da relatividade limita a velocidade com que todas essas influências podem viajar para a velocidade da luz, C. Portanto, o princípio de localidade implica que um evento num ponto não pode causar um resultado simultâneo em outro ponto. Um evento no ponto A não pode causar um resultado no ponto B num tempo menor que $T = \frac{D}{C}$, onde D é a distância entre os pontos [44].

Em 1935, Albert Einstein, Boris Podolsky e Nathan Rosen, no seu paradoxo EPR, teorizaram que a mecânica quântica pode não ser uma teoria local, porque uma medição feita num par de partículas separadas, mas entrelaçadas, causa um efeito simultâneo, o colapso da função de onda, numa partícula remota (isto é, um efeito que excede a velocidade da luz). Mas devido à natureza probabilística do colapso da função de onda, essa violação de localidade não pode ser usada para transmitir informações mais rapidamente que a luz. Em 1964, John Stewart Bell formalizou a "desigualdade de Bell", que, se violada em experimentos reais, implica que a mecânica quântica viola a localidade ou o realismo, outro princípio que se relaciona com o valor de quantidades não mensuradas. Os dois princípios são comumente referidos como um único princípio, o realismo local [44].

Testes experimentais da desigualdade de Bell, começando com as experiências de Alain Aspect em 1972, mostram que a mecânica quântica parece violar a desigualdade, por isso deve violar a localidade ou o realismo. No entanto, os críticos notaram que essas experiências continham "lacunas", o que impedia uma resposta definitiva a essa questão. Esta questão pode agora ser resolvida: em 2015, o Dr. Ronald Hanson, da Universidade de Delft, realizou o que foi chamado de primeira experiência livre de lacunas. Por outro lado, algumas lacunas podem persistir, e podem continuar a persistir a ponto de serem fundamentalmente não-testáveis [44].

3.7 Realismo

O realismo, no sentido usado na física, é a ideia de que a natureza existe independentemente da mente humana: mesmo que o resultado de uma medida possível não exista antes do ato de medi-la, isso não significa que é uma criação da mente do observador (ao contrário da teoria da "consciência causa colapso" na mecânica quântica) [45].

Uma propriedade da mente-independente (mente-independente é algo cuja existência não é dependente do pensamento / percepção das coisas e, portanto, existiria ou não existiam quaisquer coisas pensantes (mentes)) não precisa de ser um valor de uma variável física, como posição ou momento (produto da massa pela velocidade de um objeto). Uma propriedade pode ser potencial (ou seja, pode ser uma capacidade), da mesma forma que um objeto de vidro tem o potencial (ou capacidade) de se partir, se for submetido a uma força específica, caso contrario, ele não se irá partir [45].

Mesmo que o resultado de partir um objeto de vidro com um martelo não exista antes do ato de parti-lo, isso não significa que o vidro partido será uma criação do observador. Um acelerador de partículas é um tipo sofisticado de martelo, e as partículas alvo podem terminar como um amontoado de fragmentos partidos [45].

Aplicando a sistemas quânticos, Schrödinger reconheceu que também tem uma resposta condicional: uma tendência a responder (ou seja, uma probabilidade específica de responder) a uma força de medição particular com um valor particular. Tal resultado seria realista num sentido metafísico, sem ser realista no sentido físico do realismo local (o que requer que um único valor seja produzido com certeza) [45].

3.8 Realismo Local

O princípio do realismo local de Einstein é a combinação do princípio da localidade (limitando causa-e-efeito à velocidade da luz) com a suposição de que uma partícula deve objetivamente ter um valor pré-existente (isto é, um valor real) para qualquer medida possível, ou seja, um valor existente antes que a medição seja feita. No entanto, o teorema de Fine mostra que essa atribuição determinística de propriedades não é necessária para provar o teorema de Bell [46]. Isso ocorre porque o conjunto de distribuições estatísticas para medições em duas partes, uma vez que a localidade tenha sido assumida, é independente de se o determinismo também é ou não assumido. Esse resultado demonstra que se pode considerar o realismo local como a afirmação de que os estados reais existem independentemente do observador (realismo), combinados com a suposição de que dois sistemas separados têm os seus próprios estados com dinâmicas locais (localidade).

O realismo local é uma característica da mecânica clássica e da eletrodinâmica clássica, mas as teorias da mecânica quântica rejeitam o princípio, baseado na evidência experimental de envolvimentos quânticos distantes: uma interpretação que Einstein rejeitou (como sendo um paradoxo), mas que é apoiada por uma experiência de 1972 baseado no teorema da desigualdade de Bell de 1964.[47] Não está clara se a experiência de 1972 demonstra uma violação genuína, porque não foi testada a subclasse de desigualdades e por causa das limitações no teste.

3.9 Teoria das Variáveis Ocultas

A teoria das variáveis ocultas para a mecânica quântica é defendida por um grupo de físicos que argumentam que a natureza estatística da mecânica quântica é incompleta, havendo a necessidade de se considerar variáveis adicionais. Deste modo, novos fenómenos físicos, além dos descritos pela mecânica quântica, serão necessários para explicar um evento individual. A mecânica quântica tornar-se-ia, então, uma mecânica estatística no sentido clássico [48].

3.10 Teoria das Variáveis Ocultas Não-Locais

Uma teoria das variáveis ocultas, com o seu dito determinismo, que é consistente com a mecânica quântica deve ser não-local, mantendo a existência de relações causais instantâneas entre entidades físicas separadas. Teorias não-locais, isto é, teorias que permitem aos sistemas interagirem à distância com velocidades maiores do que a velocidade da luz, não poderiam ser desconsideradas. A primeira teoria de variáveis ocultas foi a teoria da onda piloto proposta por Louis de Broglie no final de 1920. A teoria atualmente mais bem conhecida de variáveis ocultas é a mecânica Bohmiana, do físico e filosofo David Bohm, criada em 1952, chamada de teoria de variáveis ocultas não-local [49].

A interpretação de Bohm da mecânica quântica é de forma inevitável não-local, o que no passado seria um golpe contra ela, mas isso mudou nos últimos tempos, pois a não-localidade tem vindo a se tornar mais convincente devido a verificação experimental da desigualdade de Bell. Físicos como Alain Aspect têm realizado experiência que podem ser interpretados como uma demonstração que as considerações de Bell são corretas, o que fortifica a teoria de ações não-locais. Tendo uma certa popularidade entre os físicos, embora a maioria ache que ela seja teoricamente deselegante. Porem, não há consenso do que o Bohm fez, baseado na ideia original de de Broglie, que foi posicionar a partícula quântica, por exemplo, um eletrão, e um “onda guia” oculta que visualiza o seu movimento. Portanto, nesta teoria os eletrões são claramente definidos como partículas. Quando se realiza uma experiência de dupla fenda, ele irá passar através de uma fenda ou da outra. Contudo, a sua escolha de fenda não é aleatória, mas orientada pela onda guia, resultando no padrão de onda observável [49].

O aspeto da teoria de Bohm é que ela foi deliberadamente criada para fornecer predições as quais são, em todos detalhes, idênticas às da mecânica quântica. Sua intenção não era fazer uma contraproposta definitiva, mas demonstrar que uma teoria de variáveis ocultas para a mecânica quântica também era possível. Este cenário era realmente importante nas pesquisas futuras. A esperança de Bohm era a de que isto poderia levar a novos insights e experiências que poderiam levar a física além da teoria quântica atual [49].

3.11 Experiência da Dupla Fenda

A experiência da dupla fenda é uma ilustração da dualidade onda-partícula. Nele, um feixe de partículas (como eletrões) viaja através de uma barreira que tem duas fendas. Se alguém colocar uma pelicula de deteção além da barreira, o padrão de partículas detetadas mostra varias interferências características das ondas que chegam à pelicula. No entanto, o padrão de interferência é composto de pontos individuais correspondentes às partículas que chegaram à pelicula. O sistema parece exibir o comportamento de ambas, as ondas (padrões de interferência) e partículas (pontos na pelicula) como se pode ver na figura seguinte [50].

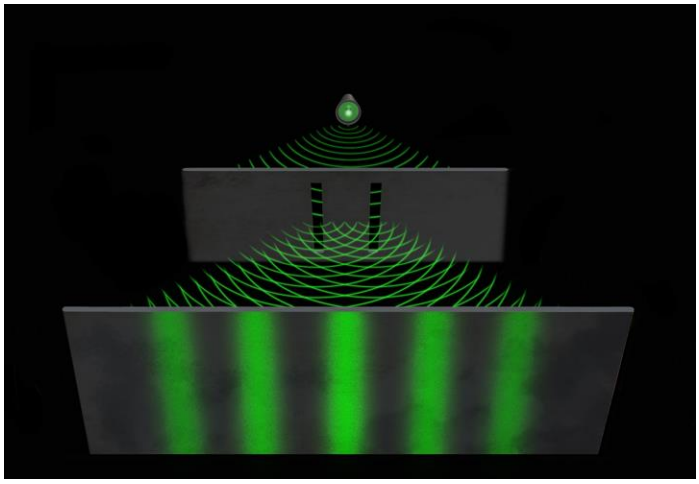

Figura 3.2 - Trajetórias de Bohm.

Fonte: Imagem retirada de https://mybigtoe.com.br/experimento-dupla-fenda-quantica/

Se modificarmos essa experiência para que uma fenda seja fechada, nenhum padrão de interferência será observado. Assim, o estado de ambas as fendas afeta os resultados finais. Também podemos organizar um detetor minimamente invasivo numa das fendas para detetar qual fenda a partícula passou. Quando fazemos isso, o padrão de interferência desaparece [50].

A interpretação de Copenhaga afirma que as partículas não estão localizadas no espaço até que sejam detetadas, de modo que, se não houver nenhum detetor nas fendas, não há informações sobre qual fenda a partícula passou. Se uma fenda tiver um detetor, a função de onda entra em colapso devido a essa deteção [50].

Na teoria de Broglie-Bohm, a função de onda é definida em ambas as fendas, mas cada partícula tem uma trajetória bem definida que passa exatamente por uma das fendas. A posição

final da partícula na pelicula do detetor e a fenda através da qual a partícula passa é determinada pela posição inicial da partícula. Tal posição inicial não é cognoscível ou controlável pelo experimentador, portanto há uma aparência aleatória no padrão de deteção. Nos trabalhos de 1952 de Bohm, ele usou a função de onda para construir um potencial quântico que, quando incluído nas equações de Newton, forneceu as trajetórias das partículas que fluíam pelas duas fendas. Com efeito, a função de onda interfere consigo mesma e guia as partículas pelo potencial quântico de tal forma que as partículas evitam as regiões nas quais a interferência é destrutiva e são atraídas para as regiões nas quais a interferência é construtiva, resultando no padrão de interferência na pelicula do detetor [50].

3.12 Interpretação de Bohm

A interpretação de Bohm da mecânica quântica generaliza a teoria da onda piloto de Louis de Broglie de 1927, a qual apresenta que ambos, onda e partícula, são reais. David Bohm, aluno de Robert Oppenheimer e contemporâneo de Albert Einstein em Princeton, após publicar Teoria Quântica, elogiada por Einstein como a mais clara explicação que lera sobre o tema, reinterpretou a física quântica de forma divergente da interpretação de Copenhaga [50].

Segundo a interpretação de Bohm, a função de onda evolui de acordo com a equação de Schrödinger, que de algum modo "guia" a partícula. Isto assumindo um universo simples e determinístico, e não dividido (diferindo da interpretação de Copenhaga e da interpretação de muitos mundos). Isto quer dizer que o estado do universo evolui suavemente através do tempo, sem o colapso da função de onda quando uma medição ocorre, como na interpretação de Copenhaga. Contudo, deve-se assumir a existência de um grande número de variáveis ocultas, as quais nunca poderiam ser diretamente mensuradas [50].

3.13 Dualidade onda-partícula

A dualidade onda-partícula é o conceito da mecânica quântica de que cada partícula ou entidade quântica pode ser parcialmente descrita em termos não apenas de partículas, mas também de ondas. Ela expressa a incapacidade dos conceitos clássicos de "partícula" ou "onda" para descrever completamente o comportamento de objetos em escala quântica. Como Albert Einstein escreveu:

“It seems as though we must use sometimes the one theory and sometimes the other, while at times we may use either. We are faced with a new kind of difficulty. We have two contradictory pictures of reality; separately neither of them fully explains the phenomena of light, but together they do.”

Através do trabalho de Max Planck, Albert Einstein, Louis de Broglie, Arthur Compton, Niels Bohr e muitos outros, a teoria científica atual sustenta que todas as partículas exibem uma natureza ondulatória e vice-versa. Este fenómeno foi verificado não apenas para partículas elementares, mas também para partículas compostas como átomos e até moléculas. Para partículas macroscópicas, devido aos seus comprimentos de onda extremamente curtos, as propriedades de onda geralmente não podem ser detetadas [51].

Embora o uso da dualidade onda-partícula tenha funcionado bem na física, o significado ou interpretação não foi satisfatoriamente resolvido.

Bohr considerava o "paradoxo da dualidade" como um facto fundamental ou metafísico da natureza. Um determinado tipo de objeto quântico exibirá por vezes um caractere de onda, às vezes de partícula ou em diferentes configurações físicas. Ele via tal dualidade como um aspecto do conceito de complementaridade [52]. Bohr considerou a renúncia da relação de causa-efeito, ou complementaridade, do quadro espaço-temporal, como essencial para a explicação da mecânica quântica [53].

Werner Heisenberg considerou a questão ainda mais longe. Ele via a dualidade como presente para todas as entidades quânticas, mas não exatamente na conta da mecânica quântica usual considerada por Bohr. Ele viu isso no que é chamado de segunda quantização, que gera um conceito inteiramente novo de campos que existem no espaço-tempo, a causalidade ainda sendo visualizável. Valores de campo clássicos (por exemplo, as forças do campo elétrico e magnético de Maxwell) são substituídos por um tipo inteiramente novo de valor de campo, como considerado na teoria quântica de campos. Voltando ao raciocínio, a mecânica quântica comum pode ser deduzida como uma consequência especializada da teoria quântica de campos [54][55].

4 Criptografia Quântica

A criptografia quântica é a ciência de explorar as propriedades da mecânica quântica para realizar tarefas criptográficas. O exemplo mais conhecido de criptografia quântica é a distribuição de chaves quântica, que oferece uma solução teoricamente segura em termos de informação para o problema de troca de chaves. A vantagem da criptografia quântica reside no facto de permitir a conclusão de várias tarefas criptográficas que são provadas ou pressupostas como sendo impossíveis utilizando apenas comunicações clássicas (isto é, não quânticas). Por exemplo, é impossível copiar dados codificados num estado quântico. Se alguém tentar ler os dados codificados, o estado quântico será alterado (teorema no-cloning). Isso poderia ser usado para detetar espionagem na distribuição de chaves quânticas.

Criptografia quântica começou a ser desenvolvida por Stephen Wiesner e Gilles Brassard. Wiesner, na Columbia University, em Nova York, que, no início dos anos 70, introduziu o conceito de codificação quântica. O trabalho intitulado por *Conjugate Coding* foi rejeitado pela IEEE Information Theory Society, mas acabou só a ser publicado em 1983 na SIGACT News [56]. Onde neste artigo, foi mostrado como armazenar ou transmitir duas mensagens, codificando-as em dois "observáveis conjugados", como a polarização linear e circular dos fotões [57], de modo que cada uma, e não ambas, possam ser recebidos e descodificados. Em 1984, Bennett e Brassard propuseram um método de comunicação segura, que agora se chama BB84 [58]. Em 1991, Artur Ekert desenvolveu uma abordagem diferente para a distribuição das chaves quânticas baseada em correlações quânticas peculiares conhecidas como entrelaçamento quântico [59]. Rotações aleatórias da polarização por ambas as partes foram propostas no protocolo de três estágios de Kak [60]. Este método pode ser usado para criptografia contínua e inquebrável de dados se forem usados unicamente fotões [61]. Onde o esquema básico da rotação da polarização seja implementado [62]. Isto representa um método de criptografia puramente baseado em quantum, contra a distribuição de chaves quântica, onde a criptografia real é clássica [63].

O método BB84 está na base dos métodos de distribuição de chaves quântica. Algumas das empresas que fabricam sistemas de criptografia quântica são: MagiQ Technologies, Inc. (Boston, Massachusetts, Estados Unidos), ID Quantique (Genebra, Suíça), QuintessenceLabs (Canberra, Austrália) e SeQureNet (Paris, França).

4.1 Distribuição de Chaves Quânticas

A distribuição de chaves quânticas (QKD) é um método seguro de comunicação que implementa um protocolo criptográfico envolvendo componentes da mecânica quântica. Permite que duas partes produzam uma chave secreta aleatória compartilhada e conhecida apenas por ambas as partes, que pode ser usada para criptografar e descriptografar mensagens.

Uma propriedade importante e exclusiva da distribuição de chaves quânticas é a capacidade de os dois pontos de comunicação conseguirem detetar a presença de qualquer terceiro que tente obter o conhecimento da chave. Isso resulta num aspeto fundamental da mecânica quântica: o processo de medir um sistema quântico em geral perturba o sistema. Um terceiro ponto tentando espionar a chave deve, de alguma forma, medi-la, e assim irá introduzir anomalias detetáveis. Usando superposições quânticas ou entrelaçamento quântico e transmitindo informações em estados quânticos, o sistema de comunicação pode detetar espionagem. Se o nível de intercetação estiver abaixo de um certo limite, uma chave pode ser produzida com garantia de segurança (ou seja, o intercetador não tem nenhuma informação sobre isso), caso contrário, nenhuma chave segura será encontrada e a comunicação será cancelada [56].

A segurança da criptografia que usa a distribuição de chaves quânticas depende dos fundamentos da mecânica quântica, em contraste com a criptografia de chave pública tradicional, que se baseia na dificuldade computacional de certas funções matemáticas e não fornece nenhuma prova matemática da real complexidade de reverter a mecânica ou funções unidirecionais usadas. O QKD tem segurança comprovada com base na teoria da informação e sigilo antecipado [56].

A principal desvantagem da distribuição de chaves quânticas é que ela geralmente depende de ter um canal de comunicações clássico autenticado. Na criptografia moderna, ter um canal clássico autenticado significa que alguém já tenha trocado uma chave simétrica de tamanho suficiente ou chaves públicas de nível de segurança suficiente. Com essas informações já disponíveis, é possível obter comunicações autenticadas e seguras sem usar o QKD [56].

A distribuição de chaves quânticas é usada apenas para produzir e distribuir uma chave, não para transmitir dados de mensagens. Essa chave pode ser usada com qualquer algoritmo de criptografia escolhido para criptografar (e descriptografar) uma mensagem, que pode então ser transmitida através de um canal de comunicação padrão. O algoritmo mais comumente associado ao QKD é o One-time pad[3], já que é comprovadamente seguro quando usado com uma chave secreta e aleatória [56]. Em situações no mundo real, muitas vezes também é usado com criptografia usando algoritmos de chave simétrica, como o algoritmo Advanced Encryption Standard (AES).

4.2 Troca de Chaves Quânticas

A comunicação quântica envolve a codificação de informações em estados quânticos, ou qubits, em oposição ao uso de bits por comunicação clássica. Normalmente, os fotões são usados para esses estados quânticos. A distribuição de chaves quânticas tenta explorar certas propriedades dos estados quânticos para garantir a sua segurança [64]. Existem várias abordagens diferentes para a distribuição de chaves quânticas, mas elas podem ser divididas em duas categorias principais, dependendo de quais propriedades desejam explorar:

- Preparar e medir protocolos - Em contraste com a física clássica, o ato de medir é parte integrante da mecânica quântica. Em geral, medir um estado quântico desconhecido muda o estado quântico de alguma forma. Isto é, uma consequência da indeterminação quântica e pode ser explorada a fim de detetar qualquer escuta sobre a comunicação (que envolve necessariamente a medição) e, mais importante, calcular a quantidade de informação que foi intercetada [64].

- Protocolos baseados em entrelaçamento - Os estados quânticos de dois (ou mais) objetos separados podem ser unidos de tal maneira que eles devem ser descritos por um estado quântico combinado, não como objetos individuais. Este efeito é conhecimento como entrelaçamento, e significa que ao se tentar realizar uma medição numa das partes, a ligação é quebrada de entrelaçamento e a segunda parte fica afetado com esta medição. Se um par de objetos entrelaçados é compartilhado entre duas partes, qualquer

[3] Para garantir que a criptografia seja imperscrutável, a chave só deve ser usada uma única vez, sendo imediatamente destruída após o uso

um que intercete um objeto altera o sistema geral, revelando a presença de terceiros (e a quantidade de informação que ele ganhou) [64].

Estas duas abordagens podem ser divididas em três famílias de protocolos: variável discreta, variável contínua e codificação de referência de fase distribuída. Protocolos variáveis discretos foram os primeiros a serem inventados e continuam a ser os mais implementados. As outras duas famílias estão preocupadas principalmente em superar limitações já existentes. No capitulo seguinte será abordado o protocolo BB94 e E91, que usam codificação de variáveis discretas [64].

4.3 Protocolo BB84: Charles H. Bennett e Gilles Brassard (1984)

Este protocolo, conhecido como BB84, foi originalmente criado usando estados de polarização de fotões para transmitir a informação [65]. No entanto, quaisquer dois pares de estados unidos podem ser usados para o protocolo, e muitas implementações baseadas em fibra ótica descritas como BB84 usam *phase encoded states*. O remetente (tradicionalmente referido como Alice) e o recetor (Bob) são ligados por um canal de comunicação quântica que permite que os estados quânticos sejam transmitidos. No caso dos fotões, este canal é geralmente uma fibra. Além disso, eles comunicam-se por meio de um canal público clássico, por exemplo, usando uma transmissão de rádio ou a *Internet*. O protocolo é projetado com a suposição de que um terceiro (conhecido como Eve) possa vir a interferir de alguma forma com o canal quântico, enquanto pela via do canal clássico é feita a autenticação [66][67].

A segurança do protocolo vem da codificação da informação em estados não ortogonais. A indeterminação quântica significa que esses estados não podem, em geral, ser medidos sem perturbar o estado original (teorema no-cloning). BB84 usa dois pares de estados, com cada par unido com o outro par e os dois estados dentro de um par ortogonal entre si. Pares de estados ortogonais são referidos como base. Os pares de estados de polarização usuais utilizados são a base retilínea de vertical (0º) e horizontal (90º), a base diagonal de 45º e 135º (ou -45º) ou a base circular de destro e canhoto. Quaisquer duas dessas bases são unidas entre si e, portanto, quaisquer duas podem ser usadas no protocolo [65].

O primeiro passo no BB84 é a transmissão quântica. Alice cria um bit aleatório (0 ou 1) e, em seguida, seleciona aleatoriamente uma de suas duas bases (retilínea ou diagonal neste caso) para transmiti-lo. Então a Alice prepara um estado de polarização dos fotões dependendo

do valor do bit e da base, como mostrado na tabela 4.1. Assim, por exemplo, um 0 é codificado na base retilínea (+) como um estado de polarização horizontal, e um 1 é codificado na base diagonal (x) como um estado de 135º. Alice então transmite um único fotão no estado especificado para Bob, usando o canal quântico. Este processo é então repetido a partir do estágio de bit aleatório, com Alice registando o estado, a base e o tempo de cada fotão enviado [65].

Tabela 4.1 - Estado de polarização dos fotões dependendo do valor do bit e da base

Bits Bases	0	1
+	↑	→
x	↗	↘

Fonte: Tabela retirada do documento da Ref. [65].

De acordo com a mecânica quântica, não existe nenhuma medida possível que consiga distinguir entre os 4 estados de polarização diferentes, pois eles não são todos ortogonais. A única medida possível é entre dois estados ortogonais (numa base ortonormal). Assim, por exemplo, a medição na base retilínea dá um resultado horizontal ou vertical. Se o fotão foi criado como horizontal ou vertical (como um auto-estado retilíneo), então mede o estado correto, mas se foi criado como 45º ou 135º (auto-estado diagonal), a medida retilínea retorna horizontal ou vertical ao acaso. Além disso, após essa medição, se o fotão foi polarizado no estado em que foi medido (horizontal ou vertical), a informação é dada como valida [65].

Como Bob não sabe a base em que os fotões foram codificados, tudo o que ele pode fazer é selecionar uma base ao acaso para medir, seja retilínea ou diagonal. Ele faz isso para cada fotão que recebe, registando o tempo, a base de medição usada e o resultado da medição. Depois que Bob mediu todos os fotões, ele comunica com Alice pelo canal público clássico. Alice transmite a base para a qual cada fotão foi enviado, e o Bob envia a base de cada um que foi medido. Ambos descartam medidas de fotões (bits), onde Bob usou uma base diferente, que é metade na média, deixando metade dos bits como chave compartilhada [65].

Tabela 4.2 - Tabela da discussão da chave secreta entre Alive e Bob

O bit aleatório da Alice	0	1	1	0	1	0	0	1
A base de envio aleatório da Alice	+	+	×	+	×	×	×	+
Polarização dos fotões que a Alice enviou	↑	→	↘	↑	↘	↗	↗	→
Base de medição aleatória do Bob	+	×	×	×	+	×	+	+
Medição da polarização do fotão do Bob	↑	↗	↘	↗	→	↗	→	→
DISCUSSÃO PÚBLICA DA BASE								
Chave secreta compartilhada	0		1			0		1

Fonte: Tabela retirada do documento da Ref. [65].

Para verificar a presença de um terceiro, Alice e Bob agora comparam um subconjunto predeterminado das suas sequências de bits restantes. Se um terceiro (geralmente chamado de Eve) tiver obtido alguma informação sobre a polarização dos fotões, isso introduz erros nas medidas do Bob. Outras condições ambientais podem causar erros de maneira semelhante. Se mais do que p bits diferirem, eles abortam a chave e tentam novamente, possivelmente com um canal quântico diferente, já que a segurança da chave não pode ser garantida. p é escolhido de modo que, se o número de bits conhecido por Eve for menor que isso, a amplificação de

privacidade pode ser usada para reduzir o conhecimento de Eve da chave a uma quantidade arbitrariamente pequena, com o custo de reduzir o tamanho da chave [65].

4.4 Protocolo E91: Artur Ekert (1991)

O esquema de Artur Ekert usa pares entrelaçados de fotões. Estes podem ser criados por Alice, por Bob, ou por alguma fonte separada de ambos, incluindo Eve. Os fotões são distribuídos de modo que Alice e Bob acabem com um fotão de cada par. O esquema depende de duas propriedades do entrelaçamento. Primeiro, os estados entrelaçados são perfeitamente correlacionados no sentido de que se Alice e Bob medem se suas partículas têm polarizações verticais ou horizontais, eles sempre obtêm a mesma resposta com 100% de probabilidade. O mesmo é verdadeiro se ambos medirem qualquer outro par de polarizações complementares (ortogonais). Isso exige que as duas partes distantes tenham sincronização exata de direccionalidade. No entanto, os resultados particulares são completamente aleatórios, é impossível para Alice prever se ela (e, portanto, Bob) obterá polarização vertical ou polarização horizontal. Segundo, qualquer tentativa de escutar por Eve destrói essas correlações de uma forma que Alice e Bob podem detetar [65].

Similarmente ao BB84, o protocolo envolve um protocolo particular de medição antes de detetar a presença de Eva. O estágio de medição envolve Alice medindo cada fotão que ela recebe usando alguma base do conjunto $Z_0, Z_{\frac{\Pi}{8}}, Z_{\frac{\Pi}{4}}$ enquanto bob escolhe a partir do conjunto $Z_0, Z_{\frac{\Pi}{8}}, Z_{\frac{\Pi}{8}}$ onde Z_Θ é a $\{|\uparrow\rangle, |\rightarrow\rangle\}$ base rotativa de Θ. Alice e Bob mantêm a sua série de opções de base privadas até que as medições sejam concluídas. Dois grupos de fotões são feitos: o primeiro consiste em fotões medidos usando a mesma base por Alice e Bob, enquanto o segundo contém todos os outros fotões. Para detetar a espionagem, eles podem calcular a estatística de teste S usando os coeficientes de correlação entre as bases de Alice e as de Bob [65].

Os fotões maximamente entrelaçados resultariam em $S = 2\sqrt{2}$. Se este não fosse o caso, Alice e Bob podem concluir que Eve introduziu o realismo local ao sistema, violando o Teorema de Bell. Se o protocolo for bem-sucedido, o primeiro grupo pode ser usado para gerar chaves, já que esses fotões são completamente anti-alinhados (que não estão alinhados) entre Alice e Bob [65].

4.5 Reconciliação de informações e amplificação de privacidade

Os protocolos de distribuição de chave quântica descritos acima fornecem a Alice e Bob chaves compartilhadas quase idênticas, e também com uma estimativa da discrepância entre as chaves. Essas diferenças podem ser causadas por espionagem, mas também por imperfeições na linha de transmissão e nos detetores. Como é impossível distinguir entre esses dois tipos de erros, a garantia de segurança requer a suposição de que todos os erros são devidos à intercetação. Desde que a taxa de erro entre as chaves seja menor que um certo limiar (20% a partir de abril de 2007 [68]), duas etapas podem ser executadas para primeiro remover os bits errados e reduzir o conhecimento de Eve da chave para um valor arbitrário pequeno. Essas duas etapas são conhecidas como reconciliação de informações e amplificação de privacidade, respetivamente, e foram descritas pela primeira vez em 1992 [69].

A reconciliação de informações é uma forma de correção de erros realizada entre as chaves de Alice e Bob, para garantir que ambas as chaves sejam idênticas. É conduzido através do canal público e, como tal, é vital minimizar as informações enviadas sobre cada chave, para que não seja lido por Eve. Um protocolo comum usado para a reconciliação de informações é o protocolo em cascata, proposto em 1994 [70]. Opera em várias voltas, com as duas chaves divididas em blocos em cada volta e a comparação de paridade desses blocos. Se uma diferença de paridade for encontrada, uma pesquisa binária será executada para localizar e corrigir o erro. Se um erro for encontrado num bloco de uma volta anterior que tenha paridade correta, então outro erro deverá estar contido nesse bloco, esse erro é encontrado e corrigido como antes. Este processo é repetido recursivamente, que é a origem do nome da cascata. Depois que todos os blocos serem comparados, Alice e Bob reordenam as suas chaves da mesma maneira aleatória, e uma nova volta começa. No final de várias voltas, Alice e Bob possuem chaves idênticas com uma probabilidade alta, mas, no entanto, Eva tem informações adicionais sobre a chave das informações de paridade trocadas. Do ponto de vista da teoria de codificação, a reconciliação de informações é essencialmente a codificação de fontes com informações secundárias, em consequência, qualquer esquema de codificação que funcione para esse problema pode ser usado para reconciliação de informações. Ultimamente os *turbocodes*, [71] códigos LDPC [72] e códigos polares [73] têm sido utilizados para este fim, melhorando a eficiência do protocolo em cascata.

A amplificação de privacidade é um método para reduzir (e efetivamente eliminar) as informações parciais de Eve sobre a chave de Alice e Bob. Essa informação parcial poderia ter

sido obtida tanto por espionagem no canal quântico durante a transmissão de chaves (introduzindo assim erros detetáveis), quanto no canal público durante a reconciliação de informações (onde se assume que Eve obtém todas as informações de paridade possíveis). A amplificação de privacidade usa a chave de Alice e Bob para produzir uma nova chave mais curta, de tal forma que Eve tenha apenas informações insignificantes sobre a nova chave. Isto pode ser feito usando uma função *hash* universal, escolhida aleatoriamente a partir de um conjunto conhecido publicamente de tais funções, que recebe como entrada uma string binária de comprimento igual à tecla e gera uma string binária de tamanho menor. A quantia pela qual esta nova chave é encurtada é calculada, com base em quanta informação Eve poderia ter obtido sobre a chave antiga (que é conhecida devido aos erros que isto introduziria), a fim de reduzir a probabilidade de Eve ter qualquer conhecimento de a nova chave para um valor muito baixo [74].

4.6 Como Funciona a Distribuição de Chaves de Criptografia Quântica

A distribuição de chaves quânticas é a parte mágica da criptografia quântica. Todas as outras partes deste novo mecanismo de criptografia permanecem as mesmas das técnicas de criptografia padrão usadas atualmente.

Usando partículas quânticas que se comportam sob regras da mecânica quântica, as chaves podem ser geradas e distribuídas para o lado do recetor de maneira completamente segura (desde obedecendo a certas regras já mencionadas anteriormente). O princípio da mecânica quântica, que descreve a regra básica que protege a troca de chaves, é o Princípio da Incerteza de Heisenberg [75].

O Princípio da Incerteza de Heisenberg afirma que é impossível medir a velocidade e a posição atual das partículas quânticas ao mesmo tempo. Além disso, afirma que o estado da partícula observada mudar-se-á quando medida. Esta doutrina bastante negativa, que diz que a medição não pode ser feita sem perturbar o sistema, é usado de maneira positiva pela distribuição de chaves quânticas que é um sistema de comunicação real, mesmo que alguém tente intercetar a comunicação ativada por fotões para obter a chave de criptografia que está sendo gerada por essa transferência de fotões, será preciso espremer fotões transferidos através do seu filtro de polarização para se ler as informações codificadas neles. Assim que ele tentar com um filtro errado, enviará o fotão errado. Remetente e destinatário perceberão a disparidade

nos dados trocados e os interpretarão como deteção de interceção. Eles então farão um novo ciclo de processo de nova geração de chave de criptografia [75].

4.6.1 Como é Usado?

- Fotão - A menor partícula de luz é um fotão. Possui três tipos de spins: horizontal, vertical e diagonal, que podem ser imaginados como polarização da direita para a esquerda [75].

- Polarização - A polarização é usada para polarizar um fotão. Polarize os meios de fotões para filtrar a partícula através do filtro de polarização, a fim de filtrar os tipos indesejados de spins. O fotão tem todos os três estados de spin ao mesmo tempo. Podendo manipular o giro de um fotão colocando o filtro no seu caminho. O fotão, quando passado pelo filtro de polarização, tem um giro específico que o filtro deixa passar [75].

- Spin - O Spin é geralmente a propriedade mais complicada para descrever. É uma propriedade de uma partícula elementar como eletrões e fotões. Quando eles se movem através de um campo magnético, eles serão desviados como se tivessem as mesmas propriedades de pequenos ímãs. Se pegarmos o mundo clássico, por exemplo, um objeto giratório carregado tem propriedades magnéticas. Partículas elementares como fotões ou eletrões têm propriedades semelhantes. Sabemos que pelas regras da mecânica quântica as partículas elementares não podem girar. Independentemente da incapacidade de girar, os físicos chamaram as propriedades magnéticas das partículas elementares de "spin". Pode ser um pouco enganador, mas ajuda a aprender o facto de que o fotão será desviado pelo campo magnético. O spin do fotão não muda e pode se manifestar em duas orientações possíveis [75].

- LED - Díodos emissores de luz são usados para criar fotões na maioria dos experimentos de ótica quântica. Os LEDs criam uma luz não polarizada (do mundo real). Na tecnologia moderna é possível usar LEDs como fonte de fotões único. Desta forma, uma sequência de fotões é criada, que será então usada no canal quântico para gerar e distribuir as chaves no processo de distribuição de chaves quânticas entre emissor e recetor. Dispositivos de rede ótica normal usam fontes de luz LED que criam

explosões de fotões em vez de fotões individuais. Na criptografia quântica, um único fotão deve ser enviado para ter a chance de polarizá-lo na entrada do canal ótico e verificar a polarização no lado de saída [75].

4.6.2 Transmissão de Dados Usando Fotões

A parte tecnicamente mais desafiadora da transmissão de dados codificada num fotão individual é a técnica para ler o bit codificado de dados de cada fotão. Como será possível ler o bit codificado no fotão quando a própria essência da física quântica está a impossibilitar a medição do estado quântico sem perturbações? Existe uma exceção [75].

Anexando um bit de dados a cada fotão polarizando em cada fotão individual. Os fotões de polarização são feitos filtrando o fotão através do filtro de polarização. O fotão polarizado é enviado através do canal quântico em direção ao recetor no outro lado [75].

O Princípio da Incerteza de Heisenberg entra na experiência com a regra de que o fotão, quando polarizado, não pode ser medido novamente, porque a medição mudará seu estado [75].

Felizmente, há uma exceção no Princípio da Incerteza que permite a medição, mas somente em casos especiais quando a medição das propriedades do spin do fotão é feita com um dispositivo (filtro neste caso) cujo estado quântico é compatível com a partícula medida [75].

Num caso em que o spin vertical dos fotões é medido com filtro diagonal, o fotão será absorvido pelo filtro ou o filtro mudará as propriedades de spin dos fotões. Ao alterar as propriedades, o fotão passará pelo filtro, mas obterá spin diagonal. Em ambos os casos, a informação que foi enviada do remetente é perdida no lado do recetor [75].

A única maneira de ler os fotões atualmente codificados bit/spin é passá-lo através do tipo certo de filtro. Se polarizada com polarização diagonal (X) a única maneira de ler este spin é passar o fotão através do filtro diagonal (X). Se o filtro vertical (+) for usado na tentativa de ler a polarização de fotões, o fotão será absorvido ou mudará a rotação e obterá polarização diferente, como ocorreu no lado da fonte [75].

4.6.3 Criação de Chaves ou Distribuição de Chaves

A técnica de transmissão de dados usando fotões para gerar uma chave segura no nível quântico é geralmente referida como processo de distribuição de chaves quânticas. Às vezes, QKD também é erroneamente referenciado como Criptografia Quântica. QKD é apenas uma parte da Criptografia Quântica [75].

Distribuição usa propriedades dos fotões tal como o spin que é resolvido por protocolos de QKD permitindo a troca de uma chave criptográfica com segurança (leis da física garantidas). Quando finalmente criada, a chave é absolutamente segura e pode ser usada com todos os tipos de algoritmos de criptografia convencionais [75].

4.6.4 Anexando o Bit de Informação no Fotão - Troca de Chave

A fase de troca de chaves, às vezes chamada de *Raw Key Exchange*, que fornece a antecipação da necessidade futura de *Key Sifting*, é uma técnica igual aos protocolos de distribuição de chaves Quantum listados BB84 e E91. Para poder transferir informações numéricas (binárias) através do canal quântico, precisamos de aplicar uma codificação específica a diferentes estados do fotão [75]. Por exemplo, a codificação será aplicada como na tabela seguinte, fazendo com que o spin de fotões diferente carregue um valor binário diferente.

Tabela 4.3 - Estado de polarização dos fotões dependendo do valor do bit e da base

Bits Bases	0	1
+	↑	→
x	↗	↘

Fonte: Tabela retirada do documento da Ref [75].

No processo de distribuição de chaves, o primeiro passo é o remetente aplicar a polarização nos fotões enviados e anotar a polarização aplicada. Para que este seja um exemplo, tomaremos a tabela 4.4 como a lista de fotões enviados com suas informações de polarização listadas [75].

Tabela 4.4 - Tabela da discussão da chave secreta entre Alive e Bob

O bit aleatório da Alice	0	1	1	0	1	0	0	1
A base de envio aleatório da Alice	+	+	×	+	×	×	×	+
Polarização dos fotões que a Alice enviou	↑	→	↘	↑	↘	↗	↗	→
Base de medição aleatória do Bob	+	×	×	×	+	×	+	+
Medição da polarização do fotão do Bob	↑	↗	↘	↗	→	↗	→	→
DISCUSSÃO PÚBLICA DA BASE								
Chave secreta compartilhada	0		1			0		1

Fonte: Tabela retirada do documento da Ref [75].

O remetente enviou uma chave 0101 mas é apenas o início do processo de geração de chave no qual esta chave será transformada do primeiro grupo de bits enviado para a chave real ser gerada e protegida [75].

4.6.5 Ler Bits de Informação no Lado do Recetor

Surge a questão de como podemos usar as propriedades do fotão acima descritas e ainda ser capaz de realmente lê-lo no lado do recetor. Na etapa acima, os fotões com as informações anexadas a eles foram enviados para o lado do recetor [75].

O próximo passo descreverá como a distribuição das chaves quânticas é, e com isso, toda a criptografia quântica, funciona. Durante o envio, é feita uma lista contendo cada fotão enviado ao remetente para o recetor e polarizado com spin específico (codificado um pouco de informação em cada fotão) [75].

No caso ideal, quando o remetente envia um fotão com rotação vertical e o recetor também aplica um filtro vertical no momento da chegada do fotão, ele transferirá com sucesso um dado usando partículas quânticas (fotão). Num caso menos ideal, quando um fotão com spin vertical é medido com filtro diagonal, o resultado será um fotão com spin diagonal ou nenhum fotão. O último acontecerá se o fotão for absorvido pelo filtro. Nesse caso, o bit de dados transferidos será posteriormente descartado na fase de verificação de chave[75].

4.6.6 Verificação de Chave - Processo Key Sifting

A *Key Sifting* ou verificação de chave é uma técnica feita diferentemente com os protocolos de distribuição de chaves Quantum listados BB84 e E91. A verificação da chave entra agora no processo e é geralmente referido como processo de Key Sifting [75].

No protocolo BB84, o recetor comunicará com o remetente e fornecerá a lista de filtros aplicados para cada fotão recebido. O remetente analisará essa lista e responderá com uma lista mais curta. Essa lista é feita deixando de fora as instâncias onde o emissor e o recetor usaram filtros diferentes na transferência de um único fotão [75].

No protocolo E91, o recetor fornecerá ao remetente a lista de resultados que ele produziu de cada fotão recebido, sem enviar a orientação do filtro usada (diferença do BB84). Em seguida, o remetente precisará de usar essa lista mais a sua polarização aplicada durante o envio para deduzir a orientação do filtro usado pelo recetor. Em seguida, o remetente revela ao destinatário para quais transferências ele é capaz de deduzir a polarização. O remetente e o destinatário descartarão todos os outros casos. Em todo este processo, o envio de fotões polarizados é feito através de uma linha especial de fibra ótica [75].

Se pegarmos no BB84 por exemplo, o processo de *Key Sifting* é feito pelo recetor enviando ao remetente apenas a lista de polarização aplicada em cada transferência de fotão. O recetor não envia o *spin* ou o valor que obteve como resultado dessa transferência. Tendo isso em mente, fica claro que o canal de comunicação para a verificação de chaves não deve ser um canal quântico, mas sim um canal de comunicação normal, sem nem mesmo a necessidade de ter a criptografia aplicada. O recetor e o remetente estão trocando os dados que são apenas localmente significativos para o seu processo de deduzir em quais etapas eles conseguiram enviar um fotão polarizado e ler o bit de um fotão com informação [75].

No final do processo do *Key Sifting*, considerando que não houve espionagem, ambos os lados terão exatamente a mesma chave criptográfica. A chave após o processo de *Sifting* será metade do comprimento original da chave bruta quando o BB84 for usado ou um quarto com o E91. Outros bits serão descartados no processo de *Sifting* [75].

4.6.7 Deteção de Intercetação

Se um terceiro mal-intencionado quiser intercetará a comunicação entre os dois lados, a fim de ler a informação codificada, ele terá que aplicar aleatoriamente a polarização nos fotões transmitidos. Se a polarização é feita, este terceiro precisará encaminhar os fotões para o remetente original. Como não é possível adivinhar corretamente toda a polarização, quando o emissor e o recetor validam a polarização, o recetor não poderá descriptografar dados, e a intercetação da comunicação é detetada [75].

Em média, o atacante que esteja a tentar intercetar os fotões usará a polarização incorreta do filtro na metade dos casos. Ao fazer isso, o estado desses fotões será alterado, causando erros na troca bruta de chaves pelo emissor e pelo recetor [75].

É basicamente a mesma coisa que acontece quando o recetor usa filtro errado ao tentar ler a polarização de fotões ou quando o mesmo filtro errado é usado por um intercetador [75].

Em ambos os casos, para provar a integridade da chave, é suficiente que o remetente e o destinatário estejam a verificar os erros na sequência ou na troca da *raw key* [75].

Alguma outra coisa pode causar erros de troca da *raw key*, não apenas espionagem. Problemas de componentes de hardware e imperfeições, causas ambientais para o canal quântico também podem causar perda de fotões ou alteração de polarização. Todos esses erros são categorizados como uma possível deteção de espiões e são filtrados na filtragem de chaves. Para ter certeza de quanta informação o espião poderia ter reunido no processo, a *Key Distillation* é usada [75].

4.6.8 Key Distillation

Quando temos uma *Sifting Key*, para remover erros e informações que um intruso poderia ter obtido, a *Sifting Key* deve ser processada novamente. A chave após a *Key Distillation* será protegida o suficiente para ser usada como chave secreta [75].

Por exemplo, para todos os fotões, para os quais o intercetador usou o filtro de polarização direito e para o qual o recetor também usou o filtro de polarização direito, não temos uma intercetação de comunicação detetada. Aqui a *Key Distillation* entra em jogo [75].

O primeiro de dois passos é corrigir todos os possíveis erros na chave, o que é feito usando um protocolo clássico de correção de erros. Nesta etapa, teremos uma saída de taxa de erro que aconteceu. Esta estimativa da taxa de erro podemos calcular a quantidade de informação que o atacante pode ter sobre a chave [75].

O segundo passo é a amplificação da privacidade, que usará a compressão na tecla para apertar as informações do intercetador. O fator de compressão depende proporcionalmente da taxa de erro [75].

4.7 Ataques

De seguida, irei falar de alguns ataques que podem surgir na era quântica, e como é que são feitos.

4.7.1 Intercetar e Reenviar

O tipo mais simples de ataque possível é o ataque de intercetação-reenvio, onde Eve mede os estados quânticos (fotões) enviados por Alice e depois envia os estados de substituição para Bob, preparados no estado que ele mediu. No protocolo BB84, isso produz erros na partilha de chave da Alice e Bob. Como Eve não tem conhecimento da base, um estado enviado por Alice é codificado, e ele só pode adivinhar em qual base medir, da mesma forma que Bob. Se Eve escolher corretamente, Eve mede o estado correto de polarização dos fotões conforme enviado por Alice e reenvia o estado correto para Bob. No entanto, se Eve escolher incorretamente, o estado que Alice enviou será aleatório, e o estado enviado a Bob não pode ser o mesmo que o estado enviado por Alice. Se Bob medir este estado na mesma base que Alice enviou, ele também recebe um resultado aleatório (como Eve lhe enviou um estado na base oposta) com 50% de chance de um resultado errado (ao invés do resultado correto ele teria sem a presença de Eva). A tabela 4.5 mostra um exemplo desse tipo de ataque.

Tabela 4.5 - Tabela da discussão da chave secreta entre Alive e Bob com Eve.

O bit aleatório de Alice	0	1	1	0	1	0	0	1
A base de envio aleatório de Alice	+	+	×	+	×	×	×	+
Polarização de fotões enviada por Alice	↑	→	↘	↑	↘	↗	↗	→
Base de medição aleatória de Eve	+	×	+	+	×	+	×	+
Medida polarizada de Eve e o seu envio	↑	↗	→	↑	↘	→	↗	→
Base de medição aleatória de Bob	+	×	×	×	+	×	+	+
Medição da Polarização dos fotões do Bob	↑	↗	↗	↘	→	↗	↑	→
DISCUSSÃO PÚBLICA DA BASE								
Chave secreta compartilhada	0		0			0		1
Erros na chave	✓		✗			✓		✓

Fonte: Tabela retirada do documento da Ref [76].

A probabilidade de Eve escolher a base incorreta é de 50% (assumindo que Alice escolhe aleatoriamente), e se Bob mede esse fotão intercetado na base que Alice enviou ele recebe um resultado aleatório, ou seja, um resultado incorreto com probabilidade de 50%. A probabilidade de um fotão intercetado gerar um erro na string de chave é, então, 50% × 50% = 25%. Se Alice e Bob comparam publicamente n dos seus bits de chave (descartando-os como bits chave, já que não são mais secretos) a probabilidade de encontrarem desacordo e identificarem a presença de Eve é $P_d = 1 - \left(\frac{3}{4}\right)^n$. Portanto, para detetar um atacante com probabilidade P_d=0,9999999999, Alice e Bob precisam comparar n = 72 bits-chave [76].

4.7.2 Ataque man-in-the-middle

A distribuição quântica de chaves é vulnerável a um ataque man-in-the-middle quando usado sem autenticação na mesma medida que qualquer protocolo clássico, uma vez que nenhum princípio conhecido de mecânica quântica pode distinguir amigo de inimigo. Como no caso clássico, Alice e Bob não podem autenticar-se um ao outro e estabelecer uma ligação segura sem alguns meios de verificar as identidades uns dos outros (como um segredo compartilhado inicial). Se Alice e Bob tiverem um segredo compartilhado inicial, eles poderão usar um esquema de autenticação incondicionalmente seguro (como Carter-Wegman, [77]) juntamente com a distribuição de chaves quânticas para expandir exponencialmente essa chave, usando uma pequena quantidade da nova chave para autenticar a próxima sessão [78]. Vários métodos para criar este segredo compartilhado inicial foram propostos, por exemplo, usando uma teoria de terceiros [79] ou de caos [80]. No entanto, apenas a família "quase fortemente universal" de funções *hash* pode ser usada para autenticação incondicionalmente segura [81].

4.7.3 Denial of Service

Como atualmente é necessária uma linha dedicada de fibra ótica entre os dois pontos ligados pela distribuição de chaves quânticas, um ataque de negação de serviço pode ser montado simplesmente cortando ou bloqueando a linha. Essa é uma das motivações para o desenvolvimento de redes de distribuição de chaves quânticas, que encaminhariam a comunicação por meio de links alternativos em caso de interrupção.

4.7.4 Ataques de Cavalos de Tróia

Um sistema de distribuição de chaves quânticas pode ser testado por Eve, enviando luz brilhante do canal quântico e analisando as reflexões num ataque de Cavalo de Tróia. Num estudo de pesquisa de 2014, foi mostrado que Eve discerne a escolha da base secreta de Bob com mais de 90% de probabilidade, violando a segurança do sistema [82].

4.7.5 Provas de Segurança

Se Eve presumir que tem recursos ilimitados, por exemplo, poder de computação clássica e quântica, há muito mais ataques possíveis. O BB84 tem se mostrado seguro contra qualquer ataque permitido pela mecânica quântica, tanto para enviar informações usando uma fonte ideal de fotões que apenas emite um único fotão de cada vez, como também usando fontes de fotões práticos que às vezes emitem pulsos multi-fotonicos [83]. Estas provas são incondicionalmente seguras, no sentido de que nenhuma condição é imposta aos recursos disponíveis para o intercetador, no entanto, existem outras condições necessárias:

- Eve não pode aceder fisicamente aos dispositivos de codificação e decodificação de Alice e Bob.
- Os geradores de números aleatórios usados por Alice e Bob devem ser confiáveis e verdadeiramente aleatórios (por exemplo, um gerador de números aleatórios Quantum).
- O canal de comunicação clássico deve ser autenticado usando um esquema de autenticação incondicionalmente seguro.
- A mensagem deve ser criptografada usando um esquema de *One-Time Pad*.

4.7.6 Quantum Hacking

Os ataques de hackers visam vulnerabilidades na operação de um protocolo QKD ou deficiências nos componentes dos dispositivos físicos usados na construção do sistema QKD. Se o equipamento usado na distribuição de chaves quânticas puder ser adulterado, ele poderá gerar chaves que não eram seguras usando um ataque de gerador de números aleatórios. Outra classe comum de ataques é o ataque de Cavalo de Tróia que não requer acesso físico aos *endpoints*: em vez de tentar ler os fotões de Alice e Bob, Eve envia um grande pulso de luz de

volta para Alice entre os fotões transmitidos. O equipamento de Alice reflete um pouco da luz de Eve, revelando o estado da base de Alice (por exemplo, um polarizador). Este ataque pode ser detetado, e usando um detetor clássico para verificar os sinais não legítimos (ou seja, a luz de Eve) entrando no sistema de Alice.

Vários outros ataques, incluindo ataques de estado falso, ataques de remapeamento de fase e ataques de mudança de tempo, já são atualmente conhecidos. O ataque por mudança de tempo foi demonstrado num criptosistema quântico comercial [84]. Esta é a primeira demonstração de hacking quântico contra um sistema de distribuição de chaves quânticas não caseiro. Mais tarde, o ataque de remapeamento de fase também foi demonstrado num sistema de QKD aberto especialmente orientado para a pesquisa (feito e fornecido pela empresa suíça Id Quantique sob seu programa Quantum Hacking) [85].

O primeiro ataque que alegou ser capaz de espionar toda a chave sem deixar vestígios foi demonstrado em 2010 [86]. Foi demonstrado experimentalmente que os detetores de fotões únicos em dois dispositivos comerciais poderiam ser totalmente controlados remotamente usando iluminação brilhante especialmente adaptada. Numa onda de publicações, a colaboração entre a Universidade Norueguesa de Ciência e Tecnologia na Noruega e o Instituto Max Planck para a Ciência da Luz na Alemanha demonstrou vários métodos para espionar com sucesso Sistemas QKD baseados nas fraquezas de fotodiodos Avalanche (APDs) a operar no modo fechado. Isso desencadeou pesquisas sobre novas abordagens para proteger as redes de comunicações [87].

4.7.7 Futuro da Segurança

Os atuais sistemas comerciais são voltados principalmente para governos e corporações com altos requisitos de segurança. A distribuição de chaves por correio é tipicamente usada em tais casos, onde não se acredita que os esquemas tradicionais de distribuição de chaves ofereçam garantias suficientes. Isto tem a vantagem de não ser intrinsecamente limitado à distância e, apesar dos longos tempos de viagem, a taxa de transferência pode ser elevada devido à disponibilidade de dispositivos de armazenamento portáteis de grande capacidade. A principal diferença da distribuição de chaves quânticas é a capacidade de detetar qualquer intercetação da chave, enquanto que, com o correio, a segurança da chave não pode ser provada

ou testada. Os sistemas QKD também têm a vantagem de serem automáticos, com maior confiabilidade e menores custos operacionais do que uma rede de correio humana segura.

O protocolo de três estágios de Kak foi proposto como um método para comunicação segura que é inteiramente quântico, ao contrário da distribuição quântica de chaves, na qual a transformação criptográfica usa algoritmos clássicos [88].

Os fatores que impedem a ampla adoção da distribuição de chaves quânticas fora das áreas de alta segurança incluem o custo do equipamento e a falta de uma ameaça demonstrada aos protocolos de troca de chaves existentes. No entanto, com as redes de fibra ótica já presentes em muitos países, a infraestrutura está em vigor para um uso mais difundido.

Um Grupo de Especificação da Indústria (ISG) do Instituto Europeu de Normas de Telecomunicações (ETSI) foi criado para tratar de questões de padronização em criptografia quântica [89].

4.8 Criptografia Pós-Quântica

A criptografia pós-quântica (às vezes chamada de quantum-proof, quantum-safe ou quantum-resistant) refere-se a algoritmos criptográficos (geralmente algoritmos de chave pública) que são considerados seguros contra um ataque a um computador quântico. A partir de 2018, deixou de ser verdade para os algoritmos de chave pública mais populares, que podem ser eficientemente quebrados por um computador quântico hipotético suficientemente forte. O problema com os algoritmos atualmente populares é que a segurança depende de um dos três problemas matemáticos: o problema da fatorização de números inteiros, o problema do logaritmo discreto ou o problema do logaritmo discreto da curva elíptica. Todos esses problemas podem ser facilmente resolvidos num computador quântico suficientemente poderoso para executar o algoritmo de Shor [90][91]. Embora os computadores quânticos conhecidos publicamente não possuam poder de processamento para quebrar(ainda) qualquer algoritmo criptográfico real [92], muitos criptógrafos estão a criar novos algoritmos para se preparar para um momento em que a computação quântica se torne uma ameaça para a segurança de todos nós. Este tipo de trabalho ganhou mais atenção nas áreas académicas e na indústria através da conferência PQCrypto desde 2006 e, mais recentemente, por vários

workshops sobre Criptografia Segura de Quantum, facultada pelo Instituto Europeu de Padrões de Telecomunicações (ETSI) e o Instituto de Computação Quântica [93][94][95].

Em contraste da ameaça que a computação quântica representa para os atuais algoritmos de chave pública, a maioria dos algoritmos criptográficos e funções *hash* atuais são considerados relativamente seguros contra ataques de computadores quânticos [91][96]. Enquanto o algoritmo do quantum Grover acelera ataques contra cifras simétricas, dobrar o tamanho da chave pode efetivamente bloquear esses ataques [97]. Assim, a criptografia simétrica pós-quântica não precisa de diferir significativamente da criptografia simétrica atual.

4.9 Algoritmos Criptográficos Pós-Quântico

Atualmente, a pesquisa de criptografia pós-quântica é focada principalmente em seis abordagens diferentes:

4.9.1 Criptografia Lattice-based

É o termo genérico para a construções de primitivas criptográficas que envolvem lattices, seja na própria construção ou na prova de segurança. As construções baseadas em lattices são atualmente importantes candidatos à criptografia pós-quântica. Ao contrário de esquemas de chaves públicas mais amplamente utilizados e conhecidos, como os sistemas de criptografia RSA, Diffie-Hellman ou Curva Elíptica, que são facilmente atacados por um computador quântico, algumas construções baseadas em lattices parecem resistentes a ataques de computadores clássicos e quânticos. Além disso, sabe-se que muitas construções baseadas em lattices são seguras sob a suposição de que certos problemas de rede computacional bem estudados não podem ser resolvidos eficientemente [98].

4.9.2 Criptografia Multivariável

Este sistema criptográfico, como o esquema Rainbow (Unbalanced Oil and Vinegar), que é baseado na dificuldade de resolver sistemas de equações multivariadas. Várias tentativas de criar esquemas seguros de criptografia de equações multivariadas falharam. No entanto, esquemas de assinatura multivariada, como o Rainbow, podem fornecer a base para uma assinatura digital de segurança quântica [99].

4.9.3 Criptografia Baseada em Hash

Este sistema criptográfico como as assinaturas Lamport e o esquema de assinatura Merkle e os esquemas XMSS [100] e SPHINCS [101] mais recentes. As assinaturas digitais baseadas em *hash* foram inventadas no final dos anos 70 por Ralph Merkle e vêm sido estudadas desde então como uma alternativa interessante para assinaturas digitais numéricas teóricas como RSA e DSA. A principal desvantagem é que, para qualquer chave pública baseada em *hash*, existe um limite no número de assinaturas que podem ser assinadas usando o conjunto correspondente de chaves privadas. Este facto reduziu o interesse por essas assinaturas até que o interesse foi revivido devido ao desejo da criptografia que era resistente ao ataque de computadores quânticos. O esquema de assinatura baseado em *hash stateful* XMSS é descrito no RFC 8391 [102].

4.9.4 Criptografia Baseada em Código

Este sistema criptográfico depende de códigos de correção de erros, como os algoritmos de criptografia McEliece e Niederreiter e o esquema relacionado Courtois, Finiasz e Sendrier Signature. A assinatura McEliece original usando códigos Goppa aleatórios tem resistido ao escrutínio por mais de 30 anos. No entanto, muitas variantes do esquema McEliece, que procuram introduzir mais estrutura no código usado para reduzir o tamanho das chaves, mostraram-se inseguras [103]. O Grupo de Estudos de Criptografia Pós-Quântica, recomendou o sistema de criptografia de chave pública McEliece como um candidato a proteção de longo prazo contra ataques de computadores quânticos [104].

4.9.5 Criptografia Isogênica da Curva Elíptica Supersingular

Este sistema criptográfico baseia-se nas propriedades das curvas elípticas supersingulares e dos gráficos de isogênica[4] supersingular para criar uma substituição Diffie-Hellman com sigilo antecipado [105]. Este sistema criptográfico usa a matemática bem estudada de curvas elípticas supersingulares para criar uma troca de chaves tipo Diffie-Hellman que pode servir como um substituto resistente à computação quântica direta para os métodos de troca de chaves Diffie-Hellman e curva elíptica Diffie-Hellman que estão em uso

[4] Os grupos isógenos são grupos de até 32 células.

generalizado hoje em dia. Por funcionar como as implementações existentes de Diffie-Hellman, oferece sigilo que é visto como importante para proteger contra o comprometimento de chaves de longo prazo através de falhas [106]. Em 2012, os pesquisadores Sun, Tian e Wang do Laboratório do Estado Chinês para Redes de Serviços Integrados e da Universidade Xidian estenderam o trabalho de De Feo, Jao e Plut para criar assinaturas digitais seguras quânticas baseadas em isogênicos da curva elíptica supersingular [107].

4.9.6 Resistência Quântica Chave Simétrica

Desde que se use tamanhos de chave suficientemente grandes, os sistemas criptográficos de chave simétrica como AES e SNOW 3G já são resistentes ao ataque de um computador quântico [108]. Além disso, os principais sistemas e protocolos de gestão que usam criptografia de chave simétrica em vez de criptografia de chave pública, como *Kerberos* e a Estrutura de Autenticação de Rede Móvel 3GPP, também são inerentemente seguros contra-ataques de um computador quântico. Devido à sua ampla implantação no mundo, alguns pesquisadores recomendam o uso expandido da gestão de chaves simétricas do tipo *Kerberos* como uma maneira eficiente e eficaz de obter criptografia pós-quântica hoje [109].

4.9.7 Comparação de Algoritmos

Tabela 4.6 - Comparação dos Algoritmos

Algoritmo	**Tipo**	**Chave Publica**	**Chave Privada**	**Assinatura**
NTRU Encrypt [110]	Lattice	6130 B	6743 B	
Rainbow [111]	Multivariate	124 KB	95 KB	
SPHINCS [112]	Hash Signature	1 KB	1 KB	41 KB
SPHINCS+ [113]	Hash Signature	32 B	64 B	8 KB
GLP-Variant GLYPH Signature [114][115]	Ring-LWE	2 KB	0.4 KB	1.8 KB
New Hope [116]	Ring-LWE	2 KB	2 KB	
Goppa-based McEliece [104]	Code-based	1 MB	11.5 KB	
Random Linear Code based encryption [117]	RLCE	115 KB	3 KB	
Quasi-cyclic MDPC-based McEliece [118]	Code-based	1232 B	2464 B	
SIDH [119]	Isogeny	751 B	48 B	
SIDH (compressed keys) [120]	Isogeny	564 B	48 B	

Fonte: Tabela retirada das referências, [104][110]-[120].

Uma consideração prática sobre a escolha entre algoritmos criptográficos pós-quânticos é o esforço necessário para enviar chaves públicas pela *Internet*. Deste ponto de vista, os algoritmos Ring-LWE, SPHINCS+ e SIDH fornecem tamanhos de chaves convenientemente abaixo de 1KB.

4.10 Projeto Open Quantum Safe

O projeto *Open Quantum Safe* [121][122] (OQS) foi iniciado no final de 2016 e tem o objetivo de desenvolver e criar protótipos de criptografia resistente à quântica. Ele visa integrar os esquemas pós-quânticos atuais numa biblioteca: *liboqs* [123]. *liboqs* é uma biblioteca C de software livre para algoritmos criptográficos resistente à quântica. O *liboqs* inicialmente concentra-se em algoritmos de troca de chaves. Fornece uma API comum adequada para algoritmos de troca de chave pós-quântica e reunirá várias implementações. Também incluirá uma rotina de testes e benchmarking para comparar o desempenho de implementações pós-quânticas. Além disso, o OQS também fornece integração de *liboqs* ao *OpenSSL* [124].

A partir de abril de 2017, os seguintes algoritmos de troca de chaves começaram a ser suportados: [121]

Tabela 4.7 - Algoritmos suportados para o projeto Open Quantum Safe

Algoritmo	Tipo
BCNS15[125]	Ring learning with errors key exchange
NewHope[126]	Ring learning with errors key exchange
Frodo[127]	Learning with errors
NTRU[128]	Lattice-based cryptography
SIDH[129][130]	Supersingular isogeny key exchange
McBits[131]	Error-correcting codes

Fonte: Tabela retirada da seguinte localização: https://en.wikipedia.org/wiki/Post-quantum_cryptography

4.11 Implementações

Um dos principais desafios da criptografia pós-quântica é a implementação de algoritmos potencialmente quânticos nos sistemas existentes. Há testes feitos, por exemplo, pela Microsoft Research, implementando o PICNIC em uma PKI usando módulos de segurança

de *hardware* [132]. Implementações de teste para o algoritmo NewHope do Google também foram feitas por fornecedores de HSM.

5 Simulação da Quantum Key Distribution

A *Quantum Key Distribution* são duas das principais e realistas áreas de aplicação da computação quântica hoje em dia. O QKD envolve a tarefa de compartilhar uma chave secreta entre as partes em uma comunicação usando qubits e outros recursos da mecânica quântica. Mais comumente, envolve o compartilhamento de uma chave secreta entre duas partes, que por convenção é considerada Alice e Bob (Alice quer compartilhar uma chave com Bob), mas também pode ser estendida a três partes (tripartite) ou esquemas QKD multipartidos.

Os dois recursos mais comuns usados nos algoritmos QKD são a ortogonalidade mútua de diferentes bases de medição (por exemplo, as bases de cálculo $|0\rangle$ e $|1\rangle$ e as bases diagonais $|+\rangle$ e $|-\rangle$) e o entrelaçamento de qubits (por exemplo, o estado Bell ($\frac{|00\rangle + |11\rangle}{\sqrt{2}}$). O famoso protocolo BB84 [133] e o protocolo B92 [134] são baseados em medições de qubits em bases mutuamente ortogonais e não ortogonais, enquanto o protocolo E91 [134] é baseado em entrelaçamento qubit e correlações quânticas não locais.

Nesta dissertação irei apresentar um esquema QKD tripartido, que é chamado por *Complete Network Quantum Key Distribution* (CNQKD), dividido em quatro, três participantes do QKD e uma parte adicional, todos ligados entre si com canais clássicos e quânticos, representando um grafo completo como rede entre os participantes. Esta arquitetura é proposta para fornecer mais robustez ao sistema contra invasores, confundindo qualquer potencial invasor. Usarei as correlações não locais de Bell entre os estados de Bell compartilhados entre diferentes partes (como no protocolo E91) ao longo dos canais quânticos e o princípio de *hashing*, passando apenas valores *hash* através dos canais clássicos para fornecer segurança ao sistema. Será usado o estado máximo de entrelaçamento do estado GHZ(Greenberger–Horne–Zeilinger) $|\mathrm{GHZ}\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}}$ ou o estado W(é um estado quântico entrelaçado de três qubits) $|\mathrm{W}\rangle = \frac{|001\rangle+|010\rangle+|100\rangle}{\sqrt{3}}$ para o QKD tripartido, possivelmente como uma extensão direta das ideias do protocolo E91 para três qubits ou qualquer outro QKD tripartido. Num artigo escrito por Kounteya Sarkar intitulado por "*A robust tripartite quantum key distribution using mutually shared Bell states and classical hash values using a complete-graph network architecture*", onde qualquer QKD ou implementações similares usando uma rede semelhante a um grafo completo entre os participantes e usando as correlações não-locais

entre os estados da Bell, juntamente com o princípio de *hashing*, ainda não tinham sido propostas. Será dado o detalhe da proposta com um exemplo junto com a análise de segurança que realizaram para mostrar como um potencial atacante pode-se confundir. Também se simulou uma experiência quântica da IBM para os canais quânticos e um programa em Python para os canais clássicos, verificando, assim, que a proposta funciona [135].

Desde 2016, a IBM fornece um compositor no site, que é uma plataforma de computação quântica baseada na nuvem. [136] Qualquer pessoa pode criar um circuito quântico nos dispositivos de cinco e dezasseis qubits para uma execução real ou simulação que está disponível com a ajuda do QISKit Terra e usá-lo alterando o back-end para efetuar uma execução ou simulação. O IBM Q Experience é usado para realizar uma série de experiências reais nos chips quânticos. As experiências reais incluem simulação quântica [136][137][138][139][140][141][142][143][144], desenvolvendo algoritmos quânticos [145][146][147][148][149][150][151][152], teste de tarefas teóricas de informação quântica [140][146][154][155][156], criptografia quântica [157][158][159], correção quântica de erros [140][160][161][162][163], aplicações quânticas [141][143][157][163][164][165][166].

5.1 Trabalhos Anteriores e Literatura

Uma série de trabalhos de pesquisa estão continuamente entrando em QKD com muitas referências disponíveis na literatura. Além dos protocolos mencionados na seção anterior [133][134][135], novas propostas e modificações são regularmente adicionadas. Gisin et al. [168] fornece uma boa visão geral da Criptografia Quântica juntamente com a QKD. Já que estamos interessados em QKD tripartido [169][170] nos fornecem dois algoritmos separados de QKD de três partes, onde o último usa estados de GHZ [171] e outro esquema QKD tripartido usando os estados GHZ. Desde que nos concentramos em nossa arquitetura de rede e passagem de *tokens*.

Para tornar um QKD tripartido mais robusto e não necessariamente no próprio processo QKD, os vários esquemas QKD de três partes disponíveis podem ser usados. Não apenas o QKD, os estados do GHZ também foram usados para outros propósitos, como o Compartilhamento Secreto de *Quantum* [172]. A não-localidade quântica fornecida pelo teorema de Bell [173] exibida por estados entrelaçados, como por exemplo, dois estados qubit

Bell ou três estados qubit GHZ que constitui o pano de fundo fundamental para oferecer segurança [174]. É abrangente para todos os aspetos do teorema de Bell, localidade e não-localidade, e das suas propriedades e aplicações. As correlações não locais da Bell são usadas com frequência no QKD, o protocolo E91 a utiliza para identificar potenciais invasores [175][176], são os dois exemplos usando correlações de Bell de estados entrelaçados para executar informações e autenticação mútua em um ambiente quântico.

O princípio do *hashing* é um dos conceitos mais populares e poderosos frequentemente usados em algoritmos criptográficos clássicos e quânticos. O facto mais intrigante do *hashing* é que os valores de *hash* são funções unidirecionais, ou seja, podemos facilmente calcular os valores *hash* de qualquer dado com facilidade, mas extrair os dados originais dos valores de *hash* é quase impossível com um bom algoritmo de *hash*. Os valores de *hash* também são específicos e até mesmo um único bit de diferença nos dados originais pode alterar significativamente o valor de *hash*. Portanto, não é fácil para um invasor alterar os dados originais, mas ter o mesmo valor de *hash*. Capítulo 11 da referência [177] dá uma ideia abrangente sobre funções *hash* criptográficas e do seu uso. MD5 [178] e *Secure Hash Algorithm* (SHA) [179] são os dois algoritmos *hash* mais populares e usados com mais frequência, mas há muitos mais. Não apenas no domínio da computação clássica, mas funções *hash* quânticas também foram propostas e estão sob pesquisa ativa [180][181]. Dão duas dessas propostas de *hashing* quântico. No entanto, serão usadas as funções *hash* clássicas, como será usado valores de *hash* apenas para comunicações ao longo dos canais clássicos de nossa rede (figura seguinte) e não os canais quânticos.

Entre as várias ferramentas disponíveis para simulação e processamento da vida real para algoritmos quânticos, a plataforma IBM Quantum Experience [136] deve ter uma menção especial, uma vez que trouxe uma revolução no campo de testes e simulação de algoritmos quânticos. O IBM Q oferece uma experiência de computação quântica over-the-cloud, permitindo que os utilizadores criem circuitos quânticos usando uma interface gráfica muito interativa e testem esses circuitos, tanto como uma simulação (feita num computador clássico) quanto em processadores quânticos reais. Vários pesquisadores foram beneficiados com essa experiência quântica exclusiva fornecida pela IBM. A Figura 5.1 mostra o local de trabalho para a experiência do IBM Q, onde os utilizadores podem projetar, construir e testar circuitos quânticos.

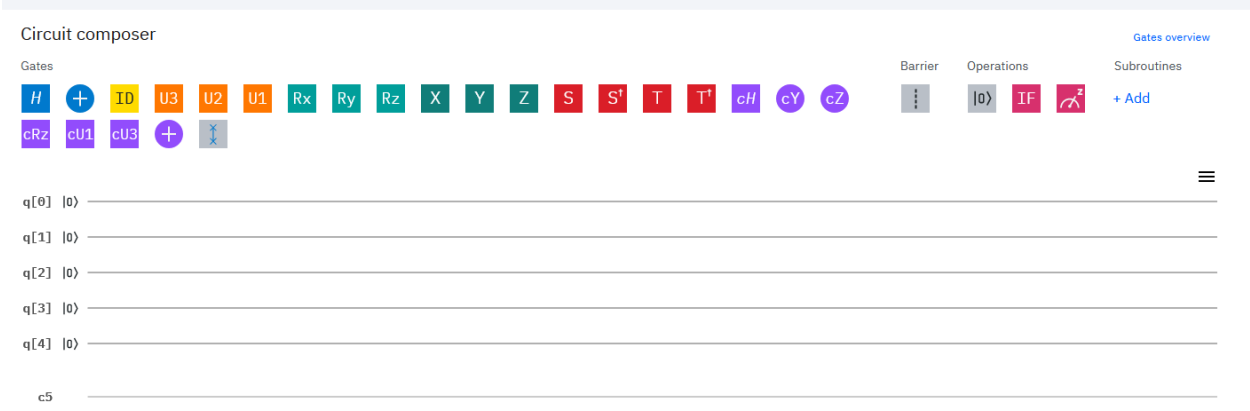

Figura 5.1 - A GUI interativa do IBM Quantum Experience.

Fonte: IBM Quantum Experience [136].

5.2 Proposta de Kounteya Sarkar, Bikash K. Behera , et al

As principais características da proposta são as seguintes:

- Embora seja um QKD tripartido, para tornar o esquema resiliente contra atacantes, usamos quatro partes ligadas numa rede semelhante a um grafo completo (figura seguinte), onde cada uma das partes compartilha um canal quântico e clássico entre si. A proposta em geral pode ser estendida a um maior número de partes e não restrita a quatro partes. Os quatro grupos foram nomeados com as letras "A", "B", "C" e "D". Sem perda de generalidade, vamos supor que "A", "B" e "C" sejam as três partes envolvidas na distribuição das chaves [182].

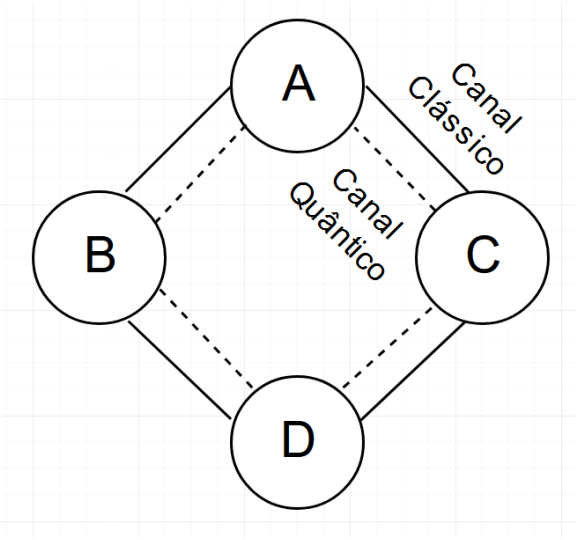

Figura 5.2 - A rede completa de grafo entre os quatro participantes.
Fonte: Da referência [182]

- Todas as partes compartilham no máximo dois qubits entrelaçados no estado de Bell ($\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ ou $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$ ou outro idêntico) entre si, ou seja, A e B compartilham os estados entre si, B e C compartilham, A e D compartilham e assim por diante. Assim, em geral, se tivermos 'n' partidos, então temos $\binom{n}{2}$ pares de partes que compartilham os estados da Bell entre si. Esse compartilhamento mútuo dos estados da Bell é de onde o esquema deriva a sua robustez. Além disso, as três partes envolvidas no processo QKD compartilham entre si, no máximo, três estados quânticos de GHZ (ou estados W) que eles usam para o processo real de distribuição de chaves. O processo pelo qual ocorre a distribuição das chaves está aberto à implementação. Um análogo direto de três qubits do protocolo E91 podem ser usados na implementação. O trabalho proposto vem a visar um aumento na robustez do sistema QKD [182].

- Entre as três partes, A, B e C que realmente participam do esquema QKD, assumimos que enquanto duas partes (digamos A e B) usam a chave compartilhada para se comunicar, a terceira parte (C) pode ser considerada um árbitro entre A e B no caso de qualquer disputa possa surgir no futuro entre as últimas partes em relação à chave. Por exemplo, após a chave ter sido compartilhada, A e B podem discordar sobre a chave compartilhada, para que possam consultar C, que também compartilham a mesma chave para resolver a disputa. C, portanto, atua como um terceiro confiável que pode ser consultado para qualquer arbitragem. Esquemas de terceiros confiáveis são muito

comuns na distribuição de chaves, tanto no reino clássico quanto no quântico. A arquitetura *Kerberos* é um exemplo de esquema confiável de terceiros na criptografia clássica [182].

- Enquanto A, B e C estão envolvidos no QKD real, a quarta parte D também desempenha um papel fundamental na rede, pois embora D não participe no QKD, ele funciona na medição mútua do estado de Bell ao redor a rede discutida a seguir, que fornece robustez ao sistema e confunde qualquer potencial atacante. De facto, sem a participação de todos os quatro participantes, o algoritmo proposto não estaria completo. Um exemplo passo-a-passo do algoritmo é dado na próxima secção, incluindo como as três partes para o QKD real são selecionadas, o candidato excluído torna-se automaticamente na quarta parte do processo [182].

- Como já mencionado, as partes compartilham mutuamente dois estados de qubit Bell $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ entre eles. Em intervalos regulares de tempo, cada um dos nós envia um do qubit entrelaçado de dois qubits para qualquer uma das outras partes através do canal quântico direto que todos os nós têm entre si. Ao receber o qubit, os dois nós (isto é, o emissor e o receptor dos qubits do estado de Bell) executam uma medição da desigualdade de Bell nos qubits. Se a desigualdade satisfizer a condição de Bell (ou a condição CHSH [174] para um limite mais restrito) então pelo teorema de Bell a correlação entre os dois qubits não permanecem mais não-local e os nós estão cientes de que o canal quântico deve ter sido comprometido por um atacante. Essas duas partes tomam nota desse facto, ou seja, o canal quântico compartilhado deixa de ser conhecido como seguro. Se, por outro lado, as desigualdades falharem, então as correlações permanecem não-locais e então o canal quântico prevalece seguro. Este processo é realizado repetidamente por cada um dos nós com cada um dos outros nós em intervalos regulares para determinar a segurança do canal quântico compartilhado. Observe que, como cada nó tem um canal direto com todos os outros nós, esse processo pode ser executado independentemente entre diferentes nós e também entre um nó com dois ou mais nós ao mesmo tempo. Nossa arquitetura como um grafo completo alcança robustez dessa maneira. É importante notar que este envio mútuo de medições de correlação de estado de Bell e não-local entre cada um dos nós continua a acontecer regularmente

através dos canais quânticos e independentemente de quaisquer mensagens serem transmitidas através do canal clássico [182].

- As quatro partes consideradas são conhecidas apenas entre si e não revelam a sua identidade para fora. Assim, todos os quatro nós aparecem iguais a qualquer estranho ou atacante sem distinção. Isso aumenta a confusão do invasor em relação a quem a distribuição das chaves está a acontecer. Mas então, como é que os quatro nós concordam entre si e iniciam e terminam o algoritmo. Isto é conseguido usando *hashing* e enviando o valor de *hash* através do canal clássico. Aqui propomos que cada parte da nossa rede tenha consigo uma tabela que compartilhe exclusivamente com todas as outras partes. A tabela seguinte mostra um exemplo de duas tabelas, a tabela de A e B e a A e C. Para aumentar a segurança, propuseram ainda, como se vê claramente na tabela seguinte, que as tabelas compartilhadas entre diferentes partes são todas diferentes. decidir entre si. A tabela contém algumas mensagens pré-decididas e o algoritmo de *hash* (por exemplo, MD5, SHA, etc.) que eles pretendem usar entre si. Sempre que uma parte, digamos A, deseja iniciar um QKD com B e C, ele refere-se à tabela exclusiva que compartilha com B e C, escolhe a mensagem apropriada, calcula o *hash* da mensagem e envia a mensagem ao respetivo destinatário por meio de um canal clássico. Por causa da maravilhosa propriedade unidirecional da função *hash*, qualquer invasor ou atacante no canal clássico não tem como extrair o significado do *hash*, mesmo com a posse da mensagem *hash* [182].

Tabela 5.1 - Exemplo de duas tabelas que A compartilha cada uma com B e C.

Sample table shared between A and B	
HASH-ALGO	MD5
REQUEST SHARE- KEY	
REQUEST THIRD P- C	
REQUEST THIRD P-D	
REQUEST TERMINATE KEY	
ACKNOWEDGE	
REQUEST ARBITRAR- C	
OK ARBITRAR WITH-C	
.....	
.....	

Sample table shared between A and C	
HASH-ALGO	SHA512
START QKD	
KEEP THIRD PARTY-B	
KEEP THIRD PARTY-D	
DISCARD KEY	
ACK	
BE MY ARBITRAR WITH-B	
OK WITH ARBITRAR-B	
.....	
.....	

Fonte: Da referência [182]

- Quando o destinatário da mensagem *hash* recebe uma mensagem através de um canal clássico, ela sabe quem é o remetente. Isso é obtido pelo facto de cada nó ter uma ligação direta única com todos os outros nós, devido à rede semelhante a um gráfo. O destinatário, em seguida, usa a tabela que compartilha com o remetente e calcula o *hash* das mensagens de acordo com o algoritmo especificado e compara com o hash recebido. Se os *hashes* coincidirem, o destinatário saberá qual é a mensagem e enviará uma confirmação da mesma maneira, caso contrário, se não houver correspondência, o destinatário não fará nada. Desta forma, as duas partes concordam entre si no canal clássico uma nova distribuição de chaves. Além disso as duas partes, usando a mesma técnica de *hashing* e consultando quem está a seu lado, concordam com o terceiro, e ambos comunicam o mesmo ao terceiro sobre a sua decisão pela mesma técnica. O terceiro pode então enviar uma confirmação para ambas as outras partes e o QKD de três partes pode-se começar a dar inicio da troca de mensagens pelo canal quântico. Uma vez que a quarta parte não recebe nenhuma mensagem *hash* sobre os canais clássicos, ela não tem conhecimento de nenhuma comunicação entre os outros três nós e continua enviando, recebendo e medindo seu estado sobre o canal quântico como de costume [182].

- Embora o invasor não tenha como extrair o significado da mensagem *hash*, ele ainda pode misturar o *hash* para confundir as entidades válidas. Para superar isto, foi proposto o seguinte. Primeiro, impõem-se a condição de que sempre que qualquer destinatário receber uma mensagem *hash*, se for capaz de extrair o significado, deverá enviar uma confirmação ao recetor (usando a mesma técnica de *hash* e referindo-se a sua tabela

mutuamente compartilhada) caso não seja possível para extrair o significado considera a mensagem como lixo e não envia uma resposta. O remetente espera por algum tempo e, ao não receber qualquer resposta, entende que algo pode estar errado. Em segundo lugar, a estrutura exata e o conteúdo da tabela que as partes referem para construir / extrair o significado do *hash* e da ação é diferente para cada uma das partes, daí as tabelas que A compartilha com B é diferente do que compartilha com C ou D. As tabelas são necessariamente bastante longas para que o invasor não consiga obter todas as conversas válidas possíveis entre as duas partes (tabela em supra) e manter essas tabelas expansivas em cada nó para cada outro nó na rede seja definitivamente um desafio, especialmente se o número de nós for grande. No entanto, essa é uma sobrecarga necessária que precisamos para aumentar a segurança. Desta forma, mesmo se por algum meio um atacante se apoderar das informações de uma tabela, ela não poderá conhecer o conteúdo das outras tabelas, pois elas são todas diferentes [182]

- Mesmo que o invasor não tenha meios de descodificar a mensagem de *hash*, ela pode, ainda assim, espionar os canais e descobrir as partes envolvidas na comunicação, identificando a origem e os destinos. Para evitar isso, como uma medida de segurança final, propôs-se que, como a partilha é regular dos estados da Bell através dos canais quânticos, todas as partes compartilham valores de *hash* de lixo regularmente para confundir o invasor. Um participante que recebe um *hash* de lixo pode verificar imediatamente a sua autenticidade, verificando a sua tabela e, ao não encontrar qualquer correspondência, irá entendê-la como um lixo. Esse envio e recebimento de *hash* de lixo também ocorre regularmente e independente de outras comunicações. Para qualquer *hash* válido, os remetentes e destinatários poderão decodificar a mensagem, enquanto que, para valores de *hash* de lixo, serão simplesmente ignorados. [182]

- Se por qualquer razão o canal quântico entre um remetente e um recetor foi comprometido, ambos podem detetá-lo medindo as correlações da não-localidade, conforme discutido acima. Nesse cenário, mesmo que um destinatário receba um *hash* válido de um remetente, ele não envia uma confirmação de volta. O remetente também estará ciente do canal quântico comprometido através da medição em seu próprio qubit e também quando não recebe nenhum reconhecimento do destinatário. Eles então cessam imediatamente qualquer operação que estavam a fazer, tal como compartilhar

estados de GHZ para o QKD e tentar novamente mais tarde, quando as condições melhorarem [182]

- Quando o terceiro é selecionado para atuar como o árbitro por duas outras partes, e todas as respetivas mensagens de *hash* e seus reconhecimentos a esse respeito forem transmitidos, ao sentir o canal quântico livre de qualquer intruso pela medição da Bell, o terceiro nó prepara estados GHZ de três qubits, e envia dois qubits de cada estado para cada um dos outros dois nós e mantém o terceiro com ele mesmo. Após todos os qubits de estado de GHZ terem sido transferidos, as três partes podem então concordar mutuamente com uma chave baseada nos seus qubits partilhados dos estados de GHZ por qualquer método mencionado anteriormente ou como uma extensão direta do protocolo E91 para três qubits. Se neste processo, a qualquer momento, qualquer parte detetar um intruso nos seus canais quânticos pela medição da Bell, ele imediatamente interrompe o protocolo [182].

- Finalmente, afirma-se duas suposições importantes para o nosso esquema. Primeiro, assumimos que a comunicação entre dois nós, seja clássica ou quântica, só pode acontecer através do canal direto compartilhado entre os nós, já que temos uma rede completa entre os nós. Por exemplo, se A quer enviar algo para C, ele só pode enviar através do canal direto que tem para C, não pela rota através de B ou D. Em segundo lugar, devemos abordar a questão de como as tabelas sobre as quais trocam informação são criadas em primeiro lugar, especialmente quando todos são diferentes. Para isso, assume-se que, durante a formação da rede, ou quando um novo nó se une à rede, ele deve interagir fisicamente com todos os outros nós de maneira segura e, nesse momento de interação, todos os nós podem decidir sobre sua única tabela, bem como estabelecer o canal clássico e quântico. Sem dúvida, essa condição de interação física no início pode parecer uma desvantagem, mas, uma vez que as tabelas tenham sido compartilhadas e os canais estabelecidos, os nós podem comunicar com segurança [182].

Tendo listado os pontos mais importantes do esquema, será dado um exemplo para se ver como o algoritmo é executado desde o início. Novamente, sem perda de generalidade,

assumindo que A quer iniciar o QKD com B e ambos querem que C atue como terceiro, D não participa diretamente do esquema real de QKD. A figura 5.2 e a tabela 5.2 podem ser observadas para consulta. A tabela seguinte mostra em síntese as entidades que efetivamente são transferidas pelos canais quânticos e clássicos [182]

Tabela 5.2 - Tabela com a comunicação ao longo dos dois tipos de canais

Canal Quântico	Qubits, ambos Qubits no estado de Bell e GHZ.
Canal Clássico	Apenas valores de Hash, e lixo para confundir o atacante.

Fonte: Da referência [182]

5.3 CNQKD: Exemplo

1. A decide que quer partilhar uma chave com B, onde C atua como o árbitro. A verifica a sua tabela que partilha com B, seleciona o item apropriado (por exemplo, "Eu quero uma chave contigo" com a estrutura da tabela 5.1), usando o algoritmo mencionado na tabela 5.2, envia-se o *hash* para B ao longo do canal clássico que é compartilhado com B [182].

2. Como B recebe o *hash*, verifica a sua própria tabela que compartilha com A, calcula os *hashes* dos itens da tabela de acordo com o algoritmo especificado um por um e compara o mesmo com o valor de *hash* que recebeu de A. Se corresponder com "Eu quero uma chave contigo", indo pelo exemplo no ponto anterior, sabe que A quer compartilhar uma chave consigo mesmo. B então envia o *hash* do reconhecimento para A [182].

3. Tendo recebido o reconhecimento de B, A agora deseja comunicar a B a respeito de ter C como o seu terceiro confiável/árbitro. De maneira similar, A agora consulta a sua tabela e envia B a *hash* da mensagem correspondente. B recebe o *hash*, extrai o seu significado e, se estiver disposto a ter C como terceira entidade, envia o seu reconhecimento para A, caso contrário, envia uma mensagem de erro / arrependimento [182].

4. A e B estão de acordo sobre C, então agora ambos A e B enviam o seu pedido (algo como “eu quero que seja o árbitro entre mim e B” da perspetiva de A, e similar da perspetiva de B) para C. Depois de receber as mensagens de A e B, C envia uma confirmação para A e B. Note que C enviará a sua confirmação para A e B somente após receber as mensagens de requisição de ambos, caso contrário, não enviará nada. Como no algoritmo a confirmação é uma obrigação, se A e B, mesmo depois de enviar a solicitação para C não receber uma resposta, eles sabem que algo deve estar errado e perdem o processo atual. Se ambos receberem o reconhecimento de C, então A e B enviarão uma mensagem pronta para receber (claro que não o original, mas o *hash*) entre si e para C, indicando que agora estão prontos para receber os qubits de C [182].

5. C prepara agora os estados de três qubits entrelaçados (por exemplo, estados GHZ) e envia dois dos qubits para A e B e mantém o terceiro consigo mesmo. No entanto, enviar para A e B, C garante que o canal quântico entre ele e A e B não sejam comprometidos pela realização de um teste de desigualdade de Bell nos qubits que ele já partilhou com A e B. Depois de enviar o primeiro par de GHZ qubits, C, em seguida, repete o processo repetidamente, até ter qubits suficientes a partir dos quais a chave secreta pode ser extraída. Como dito antes, o processo exato da distribuição de chaves usando os estados do GHZ foi deixado aberto para implementação. Pode ser uma extensão direta do protocolo E91, como cada uma das três partes A, B e C medem o qubit de estado GHZ que eles possuem em três bases de medição separadas, e depois publicamente comparam e escolhem apenas aqueles qubits para os quais todos os três partes medidas na mesma base, e descartar os outros qubits. Assim, agora A, B e C compartilham uma chave secreta única entre si, e A e B agora podem usar a chave para se comunicarem entre si e consultar C se surgir alguma disputa no futuro em relação à chave [182].

6. Durante todo o tempo, a quarta parte D não desempenhou qualquer papel no QKD. Não obstante, D, juntamente com as outras três partes, verifica regularmente a integridade dos vários canais quânticos da rede, compartilhando e medindo as correlações não-locais dos estados da Bell, como já mencionado [182].

5.4 Análise de Segurança

Tendo dado os detalhes sobre o algoritmo (CNQKD) e um exemplo, vamos agora examinar o fator mais importante do algoritmo, a robustez que ele fornece contra um potencial invasor. Será analisada a segurança de três maneiras, primeiro pela própria natureza da proposta de rede, segundo pelos qubits de estado mútuos de Bell compartilhados pelos nós através dos canais quânticos e finalmente pelo uso de valores de *hash* somente através dos canais clássicos. Mostrando que a proposta é realmente robusta e segura [182].

5.4.1 Segurança Fornecida pela Arquitetura de Rede

Foi proposta uma arquitetura de rede semelhante a um grafo completo (Figura 5.2) para a abordagem. Que segurança esta arquitetura específica transmite ao sistema? Para entender isto, considera-se a Figura 5.3 que mostra uma rede QKD típica entre as duas partes A e B. Esta rede tem uma arquitetura vulnerável, pois há apenas um link direto entre as partes. É fácil para um invasor comprometer a rede, já que tudo o que ela precisa fazer é espionar ou manipular o link direto entre os nós [182].

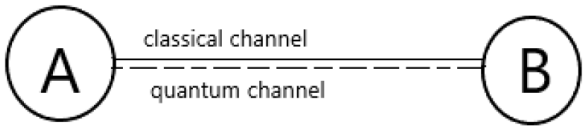

Figura 5.3 - Uma rede típica de canais clássicos e quânticos entre duas partes
Fonte: Figura da referência [182]

Como existe apenas um canal quântico e um canal clássico, toda a comunicação que acontece entre os nós deve acontecer apenas através desses canais. A arquitetura de rede da Figura 5.3 em si não fornece nenhuma segurança, as duas partes precisam confiar apenas no algoritmo que estão a usar para fornecer a segurança. Considerando a rede proposta (Figura 5.2). A própria arquitetura da rede consiste em $\frac{n(n-1)}{2}$ canais (cada um para clássico e quântico) para uma rede com 'n' nós (propriedade de um gráfo completo). Os nós ocultam completamente os seus detalhes ao mundo externo e só são conhecidos por eles mesmos. Além disso, eles enviam continuamente um ao outro qubits de estado de Bell ao longo do canal quântico e

valores de *hash* (*hash* de lixo no caso de não haver comunicação real) de tempos em tempos. Todos estes fazem a um potencial atacante ficar confuso. Para ver isso, considere um invasor a bisbilhotar os canais entre A e B. O atacante deteta alguns qubits em transição através do canal quântico e alguns valores de *hash* através do canal clássico. Mas como A e B enviam continuamente um ao outro qubits e valores de *hash*, o invasor não tem como saber se os qubits são os qubits de GHZ a serem usado no QKD real, ou nos qubits de Bell. O invasor não pode descodificar o significado do valor de *hash* também (propriedade unidirecional), nem tem uma cópia das tabelas (tabela 5.1, portanto, não pode saber se o valor de *hash* é um lixo ou alguma mensagem válida. No máximo, o invasor pode captura e mede os qubits e envia alguns outros qubits e também distorce a mensagem de *hash*. No entanto, A e B saberão imediatamente da presença dos atacantes pelo fracasso da não localidade de Bell quando eles medem os qubits, bem como quando encontram que o *hash* não corresponde a nenhuma mensagem válida. Assim, comparando com a Figura 5.3, onde um atacante tem 100% chance de atacar os canais, nesta proposta (Figura 5.2) o atacante tem $\frac{3}{\frac{n(n-1)}{2}}$ (por causa da QKD tripartida) probabilidade de atacar corretamente os canais requeridos. Se aumentarmos o número de nós "n", o sistema tornar-se-á ainda mais robusto, pois a probabilidade de adivinhar corretamente o canal para atacar diminui rapidamente, referindo-se ao gráfico abaixo. O eixo horizontal mostra o número de nós na rede e o eixo vertical mostra a probabilidade. É de notar que, como este é um QKD tripartido, se tivermos três partes, o atacante tem 100% de chance de atacar corretamente, mas diminui rapidamente com o aumento de nós [182].

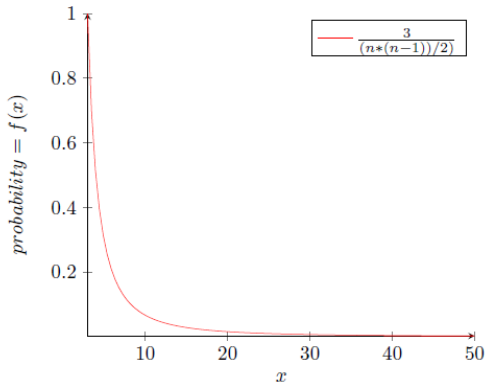

Figura 5.4 - Probabilidade de sofrer um ataque (Y) vs. quantidade de nós (X)

Fonte: Tabela retirada da referência [182]

Outra vantagem da desta arquitetura de rede é que é resiliente até certo ponto, mesmo após ser atacada. Por exemplo, considerando o QKD real que está em processo entre A, B e C, quando um atacante ataca o sistema. Como dito antes, neste caso tem $\frac{3}{6}$ (4 nós) de adivinhar corretamente um canal para atacar. Supondo que o atacante acha o canal entre B e D. Ambos B e D imediatamente percebem que o canal BD está comprometido, mas como o QKD real está a ser processado ao longo dos canais ABC, elas vão continuar a comunicar, pois não são afetadas. Isto é algo que não é possível na arquitetura simples (Figura 5.3) [182].

5.4.2 Segurança ao Longo dos Canais Quânticos

Por segurança ao longo dos canais quânticos, foi usada uma correlação não-local de Bell fornecida pelo qubit entrelaçado no estado de Bell. Como todas as partes na rede trocam continuamente os qubits da Bell e medem a desigualdade de Bell para a não-localidade, os canais quânticos estão sempre sob escrutínio ativo por todas as partes. Qualquer ação do atacante será imediatamente exposta e pode-se tomar as medidas apropriadas para o efeito. A resiliência da rede proposta garante que um QKD ainda possa continuar a funcionar, mesmo que o invasor tenha acedido a alguns canais diferentes daqueles que estão em uso para o QKD real [182].

5.4.3 Segurança ao Longo dos Canais Clássicos

Finalmente, será analisada a segurança dos canais clássicos. Os nós enviam apenas valores de *hash* ao longo dos canais clássicos, tanto lixo quanto mensagens válidas. O invasor pode bisbilhotar os canais clássicos e obter os valores de *hash*, mas não pode extrair o significado dos valores de *hash*. Não é possível diferenciar entre um lixo e um valor de *hash* válido. No máximo, pode distorcer os valores de *hash* e enviar o valor distorcido de volta. No entanto, como qualquer mensagem *hash* válida deve corresponder a uma das mensagens nas tabelas compartilhadas pelos nós e porque é quase impossível ter o mesmo valor de *hash* para duas mensagens diferentes (propriedade do valor de *hash*), se um nó receber um valor distorcido, simplesmente trata a mensagem como lixo e não faz nada. Sem o acesso às tabelas em si (que os nós mantêm em segredo e em particular), o invasor também não pode comprometer os canais clássicos [182].

5.5 Exemplo e Simulação

5.5.1 Simulação de Canal Quântico

De acordo com a rede de gráficos completos, todos os nós estão ligados com um canal clássico, bem como um canal quântico. Através do canal quântico, as partes compartilham apenas qubits entrelaçados entre si, seja qubits da Bell ou qubits do estado da GHZ. Para emular tal comportamento, assume-se que os respetivos nós têm um circuito quântico para gerar um qubit no estado de Bell ou um em estado de GHZ. A Figura 5.5 é um circuito para gerar estados Bell e a Figura 5.6 é o circuito para gerar estados GHZ. Estes circuitos foram simulados no computador IBM Quantum, a plataforma de computação quântica por nuvem fornecida pela IBM [182].

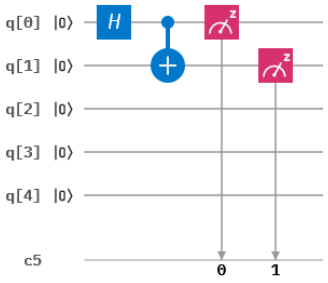

Figura 5.5 - Um circuito para gerar um par Bell.

Fonte: IBM Quantum Experience [136].

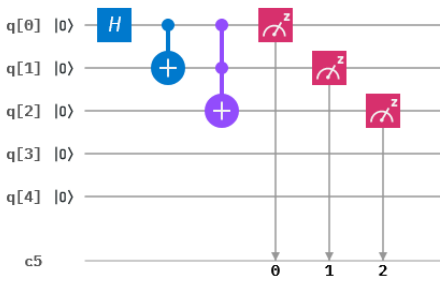

Figura 5.6 - Um circuito para gerar um estado de GHZ.

Fonte: IBM Quantum Experience [136].

Nos dois circuitos mostrados, todo o circuito, como dito antes, é estendido através das partes que comunicam e que são relevantes, cada um dos qubits compartilhados por cada parte são relevantes para esta experiência. Para o circuito do estado de Bell, por exemplo, o remetente tem o *top* qubit na sua posse enquanto o recetor tem o *bottom* na sua posse. Para o circuito do estado GHZ, que é usado para a transferência real da chave, o árbitro pode ser o criador do estado GHZ, que tem o maior qubit em sua posse, enquanto os outros dois nós, entre os quais o QKD real ocorre, são os dois últimos qubits [182].

A fim de mostrar que os dois circuitos acima realmente produzem os resultados necessários, ou seja, o estado de Bell e GHZ, o circuito foi testado na plataforma de experiência quântica da IBM. As Figura 5.7 e 5.4 mostram os resultados dos dois circuitos acima (Figura 5.5 e 5.6). Figura 5.7 mostra o resultado do circuito de estado Bell executado no computador quântico real. Figura 5.8 mostra o resultado do circuito de estado GHZ executado no computador quântico real. Deve-se notar que, na execução real de um circuito quântico, há sempre alguma probabilidade finita de obter resultados diferentes daqueles desejados. Ambos os circuitos foram testados por múltiplos números de vezes e, como vemos, os circuitos realmente produzem os resultados necessários. Para o circuito do estado de Bell, na metade do tempo temos "11" correspondendo a |11⟩ do Bell e a outra metade obtemos "00" correspondendo a |00⟩. Da mesma forma, para o estado de GHZ, onde metade do tempo obtemos |000⟩ e a outra metade do tempo obtemos |111⟩ em medições [182].

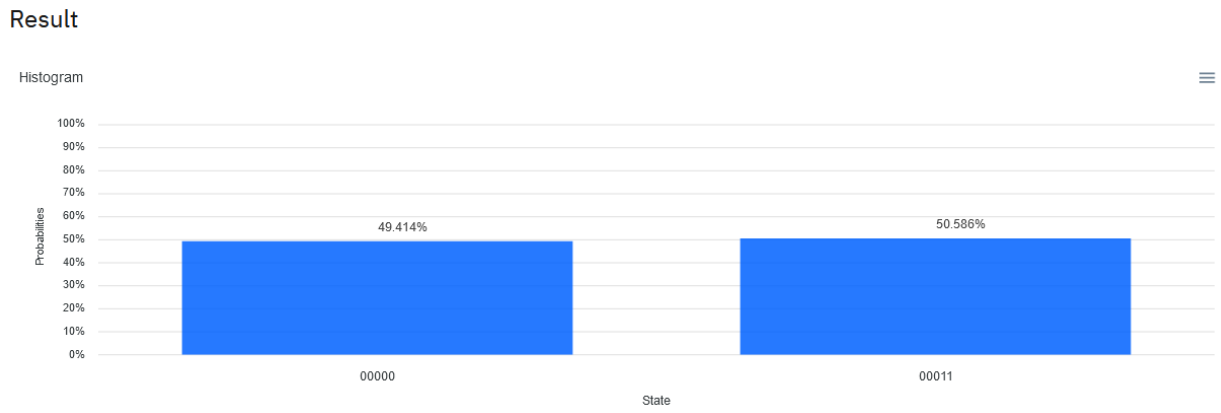

Figura 5.7 - Histograma a revelar o resultado do circuito do estado da Bell

Fonte: IBM Quantum Experience [136].

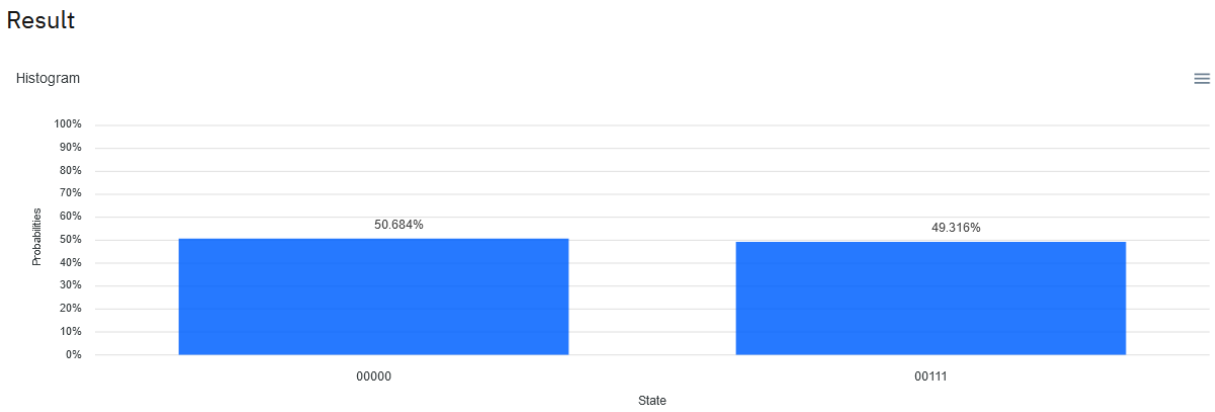

Figura 5.8 - Histograma a revelar o resultado do circuito do estado da GHZ.

Fonte: IBM Quantum Experience [136].

Na arquitetura proposta, existe um canal quântico entre cada um dos participantes. Assumindo que os ditos participantes possuem os respetivos circuitos quânticos compartilhados entre si juntamente com os respetivos qubits. Para ter uma ideia, irei considerar o seguinte exemplo de uma comunicação ao longo do canal quântico entre A e B. Considerando a partilha mútua dos qubits do estado de Bell e dos qubits de estado de GHZ entre A e B [182].

Estado de Bell - Como todos os outros nós da rede, A e B compartilham continuamente entre eles um qubit de cada par de Bell para verificar a integridade do circuito. A e B tem um circuito quântico para gerar o par de Bell (Figura 5.5) que se estende de A a B. A possui o qubit superior, enquanto B tem o qubit inferior em sua posse. Sempre que A quiser enviar um qubit de um par de Bell para B, ele inicializa dois qubits para $|0\rangle$, cria e estende o circuito de Bell para B, faz o circuito atuar nos dois qubits e finalmente envia o qubit inferior entrelaçado para B. A e B então ambos realizam uma medição da desigualdade de Bell nos qubits mantidos por eles para averiguar a integridade do canal quântico [182].

Estado de GHZ - O funcionamento e o uso do estado de GHZ é semelhante ao anterior. Consideremos agora que A, B e C são as três partes no QKD real, e que A e B são as duas partes que compartilham realmente uma chave secreta quântica e que C é o árbitro. Sempre que as três partes concordam em iniciar o processo de distribuição de chaves, o árbitro, neste caso C, cria o circuito de estado GHZ (Figura 5.8) e estende-se entre si e as outras duas partes, A e B. C tem consigo o topo mais qubit enquanto A e B tem os dois qubits inferiores. C inicializa os três qubits no estado $|0\rangle$, aplica o circuito GHZ aos três qubits para preparar o

entrelaçamento e finalmente mantém o qubit superior enquanto envia os outros dois qubits para A e B. Agora A, B e C podem iniciar qualquer entrelaçamento baseado em três partes QKD com os qubits GHZ [182].

6 Conclusões

A Quarta Revolução Industrial já está entre nós e precisamos de uma visão holística para entender os seus processos. A nossa relação com a tecnologia é histórica e pensadores como o filósofo italiano Umberto Galimberti defendem que: sem a tecnologia, não teríamos sobrevivido à magnitude da natureza. Na linha do tempo desta relação, o intervalo entre as inovações disruptivas tem sido cada vez mais curto. As transformações que vivemos são tão velozes que temos a sensação de que não conseguimos acompanhá-la a maior parte das vezes. Tal angústia resulta de um facto: o avanço tecnológico começa a ser incontornável. Chegando a um patamar em que os desenvolvemos tecnologias com características inéditas como a autonomia, a capacidade de processamento de dados inalcançável para os humanos tal como *Big Data*, Inteligência Artificial, *Machine Learning*, *Deep Learning*, Impressoras 3D de materiais bio sintéticos não são mais uma ficção, mas sim uma realidade.

O *Quantum Computing* é um campo emergente de pesquisa na interseção de ciência da computação na 4ª revolução industrial. O *Quantum Computing* pode ser usado para diversas funcionalidades, tais como: aplicações em criptografia, simulação de sistemas mecânicos quânticos complexos, inteligência artificial, previsão do tempo, etc. Os computadores quânticos serão indispensáveis no futuro. Nos últimos anos, houve imenso progresso com experiências de *Quantum Computing* com o IBM Quantum Experience (IBM QE), onde os computadores quânticos reais estão ao alcance de qualquer pessoa. Apresentei na minha dissertação somente os conceitos básicos do *Quantum Computing* para o uso do IBM QE com alguns circuitos a serem testados tais como: circuito do estado GHZ e o circuito de estado de Bell.

Os atuais sistemas comerciais são voltados principalmente para governos e corporações com altos requisitos de segurança. A distribuição de chaves criptográficas por correio é tipicamente usada em tais casos, onde não se acredita que os esquemas tradicionais de distribuição de chaves ofereçam garantias suficientes. Isto tem a vantagem de não ser intrinsecamente limitado à distância e, apesar dos longos tempos de viagem, a taxa de transferência pode ser elevada devido à disponibilidade de dispositivos de armazenamento portáteis de grande capacidade. A principal diferença da distribuição de chaves quânticas é a capacidade de detetar qualquer intercetação da chave, enquanto que, com o correio, a segurança

da chave não pode ser provada ou testada. Os sistemas QKD também têm a vantagem de serem automáticos, com maior confiabilidade e menores custos operacionais do que uma rede de correio humana segura. Os protocolos de segurança usados no QKD são os protocolos BB84 e E91 (protocolos de computação clássica).

A possibilidade de trocar mensagens secretas é de extrema importância para a nossa sociedade. Desde coisas simples como o envio de e-mails que não podem ser lidos por um terceiro até à transmissão de informações altamente sensíveis entre governos que precisam de ser seguranças na sua transmissão. Por décadas a criptografia desempenha um papel fundamental para garantir a privacidade, a estabilidade económica e as relações estáveis entre os países do mundo. Como sabemos, os sistemas criptográficos clássicos são vulneráveis a vários tipos de ataques de terceiros. O problema é que a chave secreta precisa de ser transmitida por canais inseguros ou (em um sistema de criptografia público-privado) a segurança depende das suposições matemáticas que contem propriedades específicas que são difíceis de calcular. Além disso, os algoritmos de *Quantum Computing* podem reduzir significativamente o tempo necessário para encontrar as soluções para esses problemas (encontrar fatores primos de grandes números ou calcular um logaritmo discreto).

A necessidade de superar estes problemas colocados pelos sistemas criptográficos assimétricos clássicos levou ao desenvolvimento de um campo chamado pós-criptografia quântica. Contendo problemas que se acredita que sejam mais difíceis do que fatorizar grandes números que são usados para preparar uma chave pública e privada. Esses métodos ainda não são praticamente utilizados devido a problemas de desempenho e resultados pouco claros sobre a sua segurança. Embora ainda não existam algoritmos clássicos ou quânticos para resolver esses problemas, é apenas suposto que eles sejam difíceis de resolver. Na teoria da complexidade (quântica) ou novos tipos de cálculos podem apenas mudar o problema para o futuro.

A única criptografia incondicionalmente segura requer uma chave aleatória com o mesmo tamanho da mensagem. A questão é: como é que a chave pode ser distribuída com segurança? A distribuição quântica de chaves fornece uma solução para essa questão, explorando as propriedades da mecânica quântica.

7 Trabalho futuro

Na realização deste trabalho, deixou-se um pouco de lado o projeto MICIUS que existe atualmente, pois só houve uma chamada de vídeo conferencia em 2017 com a duração pouco mais de uma hora, e nunca mais houve qualquer tipo de dados reais a passar, só a realização do teorema de Bell, para validar se havia entrelaçamento ou não.

O entrelaçamento ainda está a "anos luz" de ser encontrada uma forma de obter o valor sem que o entrelaçamento seja quebrado.

A mecânica quântica, continua com variáveis ocultas que ainda ninguém as conhece/não foram descobertas.

A comunicação quântica ainda é algo que não se consegue controlar de todo e por isso ainda é "impossível" haver uma manipulação total da mecânica quântica.

O algoritmo real a ser utilizado pelo QKD tripartido não é discutido nesta dissertação, pois há muitos algoritmos disponíveis para o QKD, em vez disso, focou-se mais na arquitetura semelhante a um grafo completo, que fornece a robustez ao sistema. Na arquitetura, existem canais clássicos e quânticos entre cada um dos nós. Para fornecer a segurança ao longo dos dois canais, foi proposto que os nós compartilhassem uns com os outros qubits de estado Bell regularmente e meçam as condições de não-localização de Bell para verificar qualquer infiltrador ao longo dos canais quânticos e somente valores de *hash* ao longo dos canais clássicos. Os valores de *hash* não são aleatórios, mas são escolhidos apenas a partir de um conjunto de mensagens válidas com base em uma única tabela compartilhada entre duas partes na arquitetura, listando todas as comunicações válidas que podem ser exigidas por qualquer nó.

Bibliografia

[1] SCHWAB, Klaus - The Fourth Industrial Revolution. 1ª ed. Suiça: **Crown Publishing Group**, 2017. ISSN 978-1524758868, p. 11-40.

[2] MARR, Bernard - **Why Everyone Must Get Ready For The 4th Industrial Revolution**. [Consult. 26 Jan. 2019] Disponivel em WWW:<URL:https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/#5af877b44f90>.

[3] LUGER, George F - Inteligência Artificial. Estruturas e Estratégias para a Solução de Problemas Complexos. 4ª ed. Brasil: **Booskman**, 2004. ISSN 85-363-0396-4, p. 23-774.

[4] RICH, Elaine; KNIGHT, Kevin - Inteligência Artificial. 2ª ed. Brasil: **McGraw-Hill**, 1994. ISSN 85-346-0122-4, p. 3-722.

[5] VASCONCELOS, V.V.;JUNIOR, Martins - P.P. Protótipo de Sistema Especialista em Direito Ambiental para Auxílio à decisão em Situações de Desmatamento Rural. 1ª ed. Rio Claro: **SP**, 2004. ISSN: 1980-654X, p. 53-58.

[6] REDAÇÃO VOZ DA INDUSTRIA - **Como é a Aplicação da Inteligencia Artificial na Industria**. [Consult. 03 Fev. 2019] Disponivel em WWW:<URL:https://avozdaindustria.com.br/como-e-a-aplicacao-da-inteligencia-artificial-na-industria/>.

[7] MANCINI, Mónica - **IoT-*Internet* of Things. Conceitos, Aplicações e Projetos**. [Consult. 09 Fev. 2019] Disponivel em WWW:<URL:https://www.youtube.com/watch?v=zXqDS1LKFEk>.

[8] MARMÉ, Paulo - **O que é a Internet das Coisas (IoT – *Internet* of Things)?** [Consult. 09 Fev. 2019] Disponivel em WWW:<URL:https://www.wattson.pt/2018/03/09/o-que-e-a-*Internet*-das-coisas-iot-*Internet*-of-things/>.

[9] CRUZ, Daniel - **A Quarta Revolução Industrial e a *Internet* das Coisas**. [Consult. 03 Fev. 2019] Disponivel em WWW:<URL:https://www.itchannel.pt/news/opiniao/a-quarta-revolucao-industrial-e-a-*Internet*-das-coisas>.

[10] CHEN, Min; MAO, Shiwen; LIU, Yunhao - Mobile Networks and Applications. 1ª ed. New York: **Chlamtac**, 2014. ISSN 1383-469X, p. 171–209

[11] TEMPONI, Luiz; SALLES, Victor - **Big Data: tudo que você sempre quis saber sobre o tema**. [Consult. 09 Fev. 2019] Disponivel em WWW:<URL:http://www.bigdatabusiness.com.br/tudo-sobre-big-data/>.

[12] NASCIMENTO, Rodrigo - **Afinal, o que é Big Data?** [Consult. 09 Fev. 2019] Disponivel em WWW:<URL:http://marketingpordados.com/analise-de-dados/o-que-e-big-data-%F0%9F%A4%96/>.

[13] GE, Mouzhi; BANGUI, Hind; BUHNOVA, Barbora - Big Data for *Internet* of Things: A SurveySystems. 1ª ed. Holanda: **Elsevir**, 2018. ISSN 0167-739X, p. 601–614

[14] KOIKE, Tiago - **O Big Data na Indústria 4.0: Qual a sua importância?** [Consult. 03 Fev. 2019] Disponivel em WWW:<URL:https://www.pollux.com.br/blog/big-data-na-industria-4-0-qual-sua-importancia/>.

[15] MARQUES DA SILVA, Mário; GUERREIRO, João, PIRES, Mónica - **On the Contribution of 5G Communications to Industry 4.0, Proceedings of 2100 Projects Association Joint Conferences 6** (2018). p. 2-4

[16] GONÇALVES,Paulo Cesar - Protótipo de um robô móvel de baixo custo para uso educacional. Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computaçãoda - **Universidade Estadual de Maringá**, Maringá. p. 2-5

[17] ALMEIDA, Nuno; LIMA, Pedro - **Contributos para um Livro Branco da Robótica em Portugal. Sociedade Portuguesa de Robótica**. [Consult. 10 Fev. 2019].

Disponivel em WWW:<URL:http://www.spr.ua.pt/site/images/stories/RnM/spr-rnm-dez2011.pdf>.

[18] GIANTOMASO, Isabela - **Tecnologia do MIT permite corrigir erros de robôs com a mente**. [Consult. 10 Fev. 2019]. Disponivel em WWW:<URL:https://www.techtudo.com.br/noticias/noticia/2017/03/tecnologia-do-mit-permite-corrigir-erros-de-robos-com-mente-entenda.html >.

[19] ARMERDING, Taylor - **Robôs trazem uma série de recursos, mas eles não vêm com muita segurança**. [Consult. 10 Fev. 2019]. Disponivel em WWW:<URL:https://itmidia.com/robos-trazem-uma-serie-de-recursos-mas-eles-nao-vem-com-muita-seguranca/ >.

[20] MELO, Raquel - **Quarta Revolução Industrial: que futuro teremos?** [Consult. 10 Fev. 2019]. Disponivel em WWW:<URL:https://futuroexponencial.com/quarta-revolucao-industrial-futuro >.

[21] GERNOT Alber; THOMAS Beth; MICHAL Horodecki, et al - Quantum Information - **Springer Tracts in Modern Physics book series**. Springer, 2001. ISBN 978-3-540-44678-1. Vol. 173.

[22] FEYNMAN, Richard P. - **There's Plenty of Room at the Bottom. Engineering and Science**. (2012), pp. 22-36. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://media.wiley.com/product_data/excerpt/53/07803108/0780310853.pdf >. ISSN 0013-7812

[23] FEYNMAN, Richard P. - **QED: The Strange Theory of Light and Matter**. Princeton University Press, 2006. ISBN 978-0-691-12575-6.

[24] WILLIAMS, Colin P. - **Explorations in Quantum Computing**. 2nd edition, Springer, 2011. ISBN 978-1-84628-887-6. p. 8-9

[25] PAM, Dirac - A new notation for quantum mechanics. **Mathematical Proceedings of the Cambridge Philosophical Society**. 35, 2008. ISSN 0305-0041

[26] BENNETT C.H.;BERNSTEIN E.; **BRASSARD G.; VAZIRANI U.. - The strengths and weaknesses of quantum computation**. SIAM Journal on Computing. 1997. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/abs/quant-ph/9701001>

[27] BERNSTEIN D.J. - Grover vs. McEliece. In: Sendrier N. (eds) Post-Quantum Cryptography. **Lecture Notes in Computer Science**. Vol 6061, 2010. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/book/10.1007/978-3-642-12929-2#editorsandaffiliations > ISBN 978-3-642-12928-5

[28] BECKMAN, David; CHARI, Amalavoyal N.; DEVABHAKTUNI, Srikrishna; PRESKILL, John. - Efficient Networks for Quantum Fatoring. **Physical Review A**. Vol. 54, 1996. p. 1034-1063. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/abs/quant-ph/9602016 >

[29] VANDERSYPEN, lieven M. K.; STEFFEN, Matthias; BREYTA, Gregory; YANNONI, Costantino S.; SHERWOOD, Mark H. & CHUANG, Isaac L. - Experimental realization of Shor's quantum fatoring algorithm using nuclear magnetic resonance. **Nature**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nature.com/articles/414883a >

[30] LU, Chao-Yang; BROWNE, Daniel E.; YANG, Tao & PAN, jian-Wei. - Demonstration of a Compiled Version of Shor's Quantum Fatoring Algorithm Using Photonic Qubits. **Physical Review Letters**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.99.250504>

[31] MARTÍN-LÓPEZ, Enrique; LAING, Anthony; LAWSON, Thomas; ALVAREZ, Roberto; ZHOU, Xiao-Qi; O'BRIEN, Jeremy L. - Experimental realization of Shor's quantum fatoring algorithm using qubit recycling. **Nature Photonics**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nature.com/articles/nphoton.2012.259>

[32] NANYANG, Xu; Jing Zhu; DAWEI, Lu; XIANYI, Zhou; XINHUA, Peng; JIANGFENG, Du. - Quantum Fatorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System. **Physical Review Letters**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/abs/1111.3726v1 >

[33] NIKESH S. Dattani; NATHANIEL, Bryans. - **Quantum fatorization of 56153 with only 4 qubits**. (2014) [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.arxiv-vanity.com/papers/1411.6758/ >

[34] CHANG, Kenneth. - Scientists Teleport Not Kirk, but an Atom. **New York Times**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nytimes.com/2004/06/17/us/scientists-teleport-not-kirk-but-an-atom.html >

[35] RIEBE, M.; HÄFFNER, H.; ROOS, C. F.; HÄNSEL, W.; BENHELM, J.; LANCASTER, G. P. T.; KÖRBER, T. W.; BECHER, C.; SCHMIDT-KALER, F.; JAMES, D. F. V.; BLATT, R. - Deterministic quantum teleportation with atoms. **Nature**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nature.com/articles/nature02570 >

[36] BARRETT, M. D.; CHIAVERINI, J.; SCHAETZ, T.; BRITTON, J.; ITANO, W. M.; JOST, J. D.; KNILL, E.; LANGER, C.; LEIBFRIED, D.; OZERI, R.; WINELAND, D. J. - Deterministic quantum teleportation of atomic qubits. **Nature**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nature.com/articles/nature02608 >

[37] KLUGER, Jeffrey. - A 'Teleportation' to Outer Space. **Revista Time**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://time.com/4856222/a-teleportation-to-outer-space/ >

[38] THOMPSON, Avery. - How Quantum Teleportation Actually Works. **Popular Mechanics**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.popularmechanics.com/science/a25699/how-quantum-teleportation-works/ > ~

[39] CORNWALL, Remi. - The Misuse of the No-Communication Theorem by Ghirardi - In The Analysis of a Non-Local Communication SystemThat Effectively Swaps Distant Joint Entanglement to Local Path Entanglement of an Interferometer. **Preprints**. (2019). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.preprints.org/manuscript/201901.0090/v1 >

[40] FAYE, Jan. - Copenhagen Interpretation of Quantum Mechanics. **Stanford Encyclopedia of Philosophy**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://plato.stanford.edu/entries/qm-copenhagen/ >

[41] PERES, Asher. - Popper's experiment and the Copenhagen interpretation. **Cornell University**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/9910078.pdf >

[42] SEN, D. - The uncertainty relations in quantum mechanics. **Current Science Association**. Vol. 7, nº 2 (2014). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.currentscience.ac.in/Volumes/107/02/0203.pdf >. ISSN 0011-3891

[43] MICHAEL, A. Nielsen and ISAAC, L. - Quantum Computation and Quantum Information - 10th Anniversary Edition, **Cambridge University Press**, 2010, [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf >. ISBN 978-1-107-00217-3.

[44] HANSON, Ronald. - Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. **Nature**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nature.com/articles/srep30289.pdf >.

[45] NORSEN, Travis. - Against 'Realism'. **Foundations of Physics**, Vol. 37, nº. 3, p. (2007). p. 311-340. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/0607057.pdf >.

[46] ABRAMSKY, Samson; BRANDENBURGER, Adam. - The sheaf-theoretic structure of non-locality and contextuality. **New Journal of Physics**. Vol. 13, (2011). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://iopscience.iop.org/article/10.1088/1367-2630/13/11/113036/pdf >.

[47] BEN-DOV, Yoav. - Local realism and the crucial experiment. **Local realism and the crucial experiment**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://bendov.info/eng/crucial.htm >.

[48] PESSOA JR, Osvaldo. - Conceitos de Física Quântica. São Paulo: **Livraria da Física Editora**. Vol. 2. ISBN 9798588325592.

[49] FALK, Dan. - New Support for Alternative Quantum View. **Quantum Magazine**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.quantamagazine.org/pilot-wave-theory-gains-experimental-support-20160516/ >.

[50] BOHM, David. - A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. Palmer **Physica Laboratory**. Vol. 85, nº 2. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://journals.aps.org/pr/abstract/10.1103/PhysRev.85.166 >.

[51] GREINER, Walter - Quantum Mechanics: An Introduction. **Springer**. 2001. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://books.google.pt/books?id=7qCMUfwoQcAC&pg=PA29&dq=wave-particle+all-particles&redir_esc=y&hl=pt-PT#v=onepage&q=wave-particle%20all-particles&f=false >.

[52] KUMAR, Manjit. - Quantum: Einstein, Bohr, and the Great Debate about the Nature of Reality (Reprint ed.). **W. W. Norton & Company**, 2011. ISBN 978-0-393-33988-8.

[53] BOHR, N. - The Quantum Postulate and the Recent Development of Atomic Theory. **Nature**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nature.com/articles/121580a0.pdf >.

[54] CAMILLERI, K. - Heisenberg and the Interpretation of Quantum Mechanics: the Physicist as Philosopher. **Cambridge University Press**, Cambridge UK, 2009. ISBN 978-0-521-88484-6.

[55] PREPARATA, G. - An Introduction to a Realistic Quantum Physics. **World Scientific**, River Edge NJ, 2002. ISBN 978-981-238-176-7.

[56] BENNETT, Charles H.; et al. - Experimental quantum cryptography. **Journal of Cryptology**. 5:1, p. 3–28. (1992). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://doi.org/10.1007/BF00191318 >.

[57] WIESNER, Stephen. - Conjugate coding. **ACM SIGACT News**. 15:1, p.78-88. (1983). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://dl.acm.org/citation.cfm?id=1008920 >.

[58] BENNETT, Charles H.; BRASSARD, Giles. - Quantum cryptography: Public key distribution and coin tossing. **Theoretical Computer Science**. 560:1, p. 7-11. (2014). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://doi.org/10.1016/j.tcs.2014.05.025 >.

[59] EKERT, Artur K. - Quantum cryptography based on Bell's theorem. **American Physical Society**. 67:6, (1991). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.67.661 >.

[60] KAK, Subhash. - A three-stage quantum cryptography protocol. **Foundations of Physics Letters**. 19:3, p. 293–296. (2016). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/0503027.pdf >.

[61] CHEN, Y.; et al. - Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks. International Conference on Computing, **Electronics and Electrical Technologies**. (2012). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.98 >.

[62] KAK, SUBHASH. - A three-stage quantum cryptography protocol. **Foundations of Physics Letters**. 19:3, p. 293-296. (2006). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/article/10.1007%2Fs10702-006-0520-9 >.

[63] CARDINAL, David. - **Quantum Cryptography Demystified: How It Works in Plain Language**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.extremetech.com/extreme/287094-quantum-cryptography >.

[64] GUANCO, Frank. - What is Quantum Key Distribution? **Cloud Security Alliance**. (2015). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf >.

[65] BENNETT, C. H.; BRASSARD, G.. - Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. **Theoretical Computer Science**. 175:8, (1984). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://core.ac.uk/download/pdf/82447194.pdf >.

[66] TOMAMICHEL, Marco; LEVERRIER, Anthony. - A largely self-contained and complete security proof for quantum key distribution. **Centre for Quantum Software and Information**. 1:14. (2017). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1506.08458.pdf >.

[67] PORTMANN, Christopher; RENNER, Renato. - Cryptographic security of quantum key distribution. **Institute for Theoretical Physics**. (2014). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1409.3525.pdf >.

[68] CHAU, H. F. - Practical Scheme To Share A Secret Key Through An Up To 27.6% Bit Error Rate Quantum Channel. Department of Physics. **University of Hong Kong**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/0205060.pdf >.

[69] BENNETT, C. H.; BESSETTE, F.; BRASSARD, G.; SALVAIL, L.; SMOLIN, J. - Experimental Quantum Cryptography. **Journal of Cryptology**. 5:1, (1992), pp. 3-28. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/article/10.1007/BF00191318 >.

[70] BRASSARD, Gilles.; SALVAIL, Louis - Secret key reconciliation by public discussion. Eurocrypt. **Lecture Notes in Computer Science**. 93:1 (1993). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/chapter/10.1007/3-540-48285-7_35 >.

[71] NGUYEN, Kim-Chi; VAN ASSCHE, Gilles; CERF, Nicolas J. - Side-Information Coding with Turbo Codes and its Application to Quantum Key Distribution. **Cryptol**. Vol.5 (1992), p. 3-28. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://adsabs.harvard.edu/abs/2004cs.....6001N>.

[72] ELKOUSS, D.; MARTINEZ-MATEO, J.; MARTIN, V.. - Quantum Information & Computation. **DBLP**. 15:1 (2011), p. 37-49. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://dblp.org/db/journals/qic/qic15>.

[73] 3. NGUYEN, Kim-Chi; VAN ASSCHE, Gilles; CERF, Nicolas J. - High Performance Error Correction for Quantum Key Distribution using Polar Codes. **Quantum Information and Computation**. 14:3, (2013). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1204.5882.pdf >.

[74] DEUTSCH, A.; EKERT, R.; JOZSA, C.; MACCHIAVELLO, S.; POPESCU, A.; SANPERA. Quantum privacy amplification and the security of quantum cryptography over noisy channels. **Clarendon Lab, University of Oxford**. Vol. 77, p. 2818-2821, (1996). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/9604039.pdf >.

[75] SHIELDS, A. J.; DYNES, J. F.; YUAN, Z. L.; LUCAMARINI, M. - Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. **Nature**. Vol.

557, (2018). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nature.com/articles/s41586-018-0066-6 >. ISSN 1476-4687.

[76] CURTY, Marcos; LÜTKENHAUS, Norbert. - Intercept-resend attacks in the Bennett-Brassard 1984 quantum key distribution protocol with weak coherent pulses. **Phys. Rev. A**. 71:1, (2005). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/0411041.pdf >.

[77] WEGMAN, M. N.; CARTER, J. L. - New hash functions and their use in authentication and set equality. **Journal of Computer and System Sciences**. Vol. 22, (1981). pp 265-279, [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/chapter/10.1007/3-540-49264-X_24 >.

[78] NGUYEN, Kim-Chi; GILLES VAN, Assche; CERF, Nicolas J. - Using quantum key distribution for cryptographic purposes: A survey. **Theoretical Computer Science**. 560:1, (2014), p. 62-81. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.sciencedirect.com/science/article/pii/S0304397514006963 >.

[79] ZHANG, Z.; LIU, J.; WANG, D.; SHI, S.. - Quantum direct communication with authentication. **Phys. Rev. A**. 75:2, (2007). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/0512051.pdf >.

[80] D. HUANG, Z.; CHEN, Y.; LEE M.. - Quantum Secure Direct Communication Based on Chaos with Authentication. **Journal of the Physical Society of Japan**. 76:12, (2007). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://journals.jps.jp/doi/abs/10.1143/JPSJ.76.124001 >.

[81] LARSSON, Jan-Åke. Unconditionally secure authentication**. Security Aspects of the Authentication Used in Quantum Cryptography**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://www.lysator.liu.se/~jc/mthesis/5_Unconditionally_secure_au.html >.

[82] JAIN, Nitin; ANISIMOVA, Elena; KHAN, Imran; MAKAROV, Vadim; MARQUARDT, Christoph; LEUCHS, Gerd. - Trojan-horse attacks threaten the security of

practical quantum cryptography. **New Journal of Physics**. (2014). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://iopscience.iop.org/article/10.1088/1367-2630/16/12/123030/meta >.

[83] SHOR, Peter W.; PRESKILL, John. - Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. **Phys. Rev. Lett**. 85:2, (2000). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.85.441 >.

[84] ZHAO, Yi; FRED FUNG, Chi-Hang; QI, Bing; CHEN, Christine; LO, Hoi-Kwong. - Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. **Phys. Rev. A**. 78:4, (2008). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.78.042333 >.

[85] XU, Feihu; Lo QI, Bing; LO, Hoi-Kwong. - Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. **New Journal of Physics**. Vol. 12, (2010). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://iopscience.iop.org/article/10.1088/1367-2630/12/11/113026 >.

[86] DONG, Zhao-Yue; YU, Ning-Na; WEI, Zheng-Jun; WANG, Jin-Dong. - An attack aimed at active phase compensation in one-way phase-encoded QKD systems. **Eur. Phys. J. D..** 68:230, (2014). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/article/10.1140/epjd/e2014-40693-6#citeas >.

[87] HUGHES, Richard; NORDHOLT, Jane (16 September 2011). - Refining Quantum Cryptography. **Science Magazine**. Vol. 333, (2011). P. 1584-1586. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://science.sciencemag.org/content/333/6049/1584 >.

[88] THAPLIYAL, K.; PATHAK, A. - Kak's three-stage protocol of secure quantum communication revisited. **Quantum Information Processing**. Vol. 17:229, 2018. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1803.02157.pdf >.

[89] ETSI. - **Quantum Key Distribution (QKD).** [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.etsi.org/technologies/quantum-key-distribution?jjj=1564008364037 >.

[90] BERNSTEIN, Daniel J. - Introduction to post-quantum cryptography. **Springer Berlin Heidelberg**. 2009. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL:https://link.springer.com/book/10.1007/978-3-540-88702-7#editorsandaffiliations >. ISBN: 978-3-540-88701-0

[91] SHOR, Peter W. - Polynomial-Time Algorithms for Prime Fatorization and Discrete Logarithms on a Quantum Computer. **SIAM Journal on Computing**. 26:5, (1996). p. 1484–1509. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/9508027.pdf >.

[92] GERSHON, Eric. - New qubit control bodes well for future of quantum computing. **Yale University**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://phys.org/news/2013-01-qubit-bodes-future-quantum.html >.

[93] HEGER, Monica. - **Cryptographers Take On Quantum Computers**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://spectrum.ieee.org/computing/software/cryptographers-take-on-quantum-computers >.

[94] DING, Jintai. - **Q&A With Post-Quantum Computing Cryptography**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://spectrum.ieee.org/computing/networks/qa-with-postquantum-computing-cryptography-researcher-jintai-ding >.

[95] ETSI. - **Quantum Computing and the risk to security and privacy**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.etsi.org/technologies/quantum-safe-cryptography >.

[96] BERNSTEIN, Daniel J.. - Cost analysis of hash collisions:Will quantum computersmake SHARCS obsolete. **National Science Foundation**. (2009). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://cr.yp.to/hash/collisioncost-20090823.pdf >.

[97] BERNSTEIN, Daniel J.. - Grover vs. McEliece. **National Science Foundation**. (2009). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://cr.yp.to/codes/grovercode-20100303.pdf >.

[98] SPRINGER, Cham. - Lattice Cryptography for the *Internet*. In: Mosca M. (eds) Post-Quantum Cryptography. **PQCrypto 2014**, 2014. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/chapter/10.1007/978-3-319-11659-4_12 >. ISBN: 978-3-319-11658-7

[99] DING, Jintai. - Rainbow, a New Multivariable Polynomial Signature Scheme. In: Ioannidis J., Keromytis A., Yung M. (eds) Applied Cryptography and Network Security. **Lecture Notes in Computer Science**. vol 3531, (2005). [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/chapter/10.1007/11496137_12 >. ISBN 978-3-540-31542-1.

[100] BUCHMANN, J.; DAHMEN, E.; HÜLSING A.. - XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. **PQCrypto 2011**. 2011. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/chapter/10.1007/978-3-642-25405-5_8 >. ISBN: 978-3-642-25404-8

[101] BERNSTEIN, Daniel J.; HOPWOOD, Daira; et al. - SPHINCS: practical stateless hash-based signatures. **Lecture Notes in Computer Science**. vol 9056. 2015. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/chapter/10.1007/978-3-662-46800-5_15 >. ISBN 9783662467992.

[102] HUELSING, A.; BUTIN, D.; GAZDAG, S.; RIJNEVELD, J.; MOHAISEN, A.. - **XMSS: eXtended Merkle Signature Scheme**. RFC 8391. 2018. ISSN: 2070-1721

[103] OVERBECK, Raphael; BERNSTEIN, Daniel. - Code-based cryptography. Post-Quantum Cryptography. **Springer**, Berlin, Heidelberg, 2009. ISBN 978-3-540-88701-0. p. 95–145.

[104] AUGOT, Daniel. - Initial recommendations of long-term secure post-quantumsystems. Post-Quantum Cryptography for Long-Term Security. **PQCRYPTO 2015**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: http://pqcrypto.eu.org/docs/initial-recommendations.pdf >.

[105] DE FEO, Luca; JAO; PLUT. - Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. **Springer**, Berlin, Heidelberg, 2011. ISBN 978-3-642-25404-8.

[106] HIGGINS, Peter. - **Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection >.

[107] SUN, Xi; TIAN; Wang. - Browse Conference Publications > Intelligent Networking and Co … Help Working with Abstracts Toward Quantum-Resistant Strong Designated Verifier Signature from Isogenies. **Intelligent Networking and Collaborative Systems (INCoS)**. 2012. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://ieeexplore.ieee.org/document/6337933 >. ISBN 978-1-4673-2281-2

[108] PERLNER, Ray. - **Quantum Resistant Public Key Cryptography: A Survey**. 2009. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.nist.gov/publications/quantum-resistant-public-key-cryptography-survey?pub_id=901595 >.

[109] CAMPAGNA, Matt; HARDJONO; Pintsov; Romansky; YU. - Kerberos Revisited Quantum-Safe Authentication. **ETSI Quantum-Safe-Crypto Workshop**. 2013. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL:

https://docbox.etsi.org/Workshop/2013/201309_CRYPTO/S03_INDUSTRY_SESSION/PITNEYBOWES_PINTSOV.pdf >.

[110] HIRSCHHORN, Philip S.; HOFFSTEIN, Jeffrey; HOWGRAVE-GRAHAM, Nick; WHYTE, William. - Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches In: Abdalla M., Pointcheval D., Fouque PA., Vergnaud D. (eds) Applied Cryptography and Network Security. **Springer**, Berlin, Heidelberg, 2016. ISBN 978-3-642-01956-2.

[111] PETZOLDT, A.; BULYGIN, S.; BUCHMANN, J. - Selecting Parameters for the Rainbow Signature Scheme. In: Sendrier N. (eds) Post-Quantum Cryptography. **PQCrypto**, 2010., vol 6061.. ISBN 978-3-642-12928-5. Springer, Berlin, Heidelberg. 6061.

[112] BERNSTEIN, Daniel J.; HOPWOOD, Daira; HÜLSING, Andreas; LANGE, Tanja; NIEDERHAGEN, Ruben; PAPACHRISTODOULOU, Louiza; SCHNEIDER, Michael; SCHWABE, Peter; WILCOX-O'HEARN, Zooko; OSWALD, Elisabeth; FISCHLIN, Marc. - SPHINCS: practical stateless hash-based signatures. Lecture Notes in Computer Science. **Springer Berlin Heidelberg**, 2015. ISBN 9783662467992. p. 368–397.

[113] BERNSTEIN, Daniel J.; DOBRAUNIG, Christoph; et al. - **SPHINCS + Submission to the NIST post-quantum project**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://pdfs.semanticscholar.org/d87c/9542622bf5345da856959a0ae959d55ed6b6.pdf?_ga=2.40781922.1168185878.1564089278-1547105999.1563920860 >.

[114] GÜNEYSU, T.; LYUBASHEVSKY, V.; PÖPPELMANN, T.. - Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems. **Computer Science**, 2012. ISBN 978-3-642-33026-1. vol 7428.

[115] Chopra, Arjun. - GLYPH: A New Insantiation of the GLP Digital Signature Scheme. **IACR Cryptology ePrint Archive 2017**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.semanticscholar.org/paper/GLYPH%3A-A-New-Insantiation-of-the-GLP-Digital-Scheme-Chopra/3e019c349161bb6a258f97c59b992b7c7cb796a4 >.

[116] ALKIM, Erdem; DUCAS, Léo; PÖPPELMANN, Thomas; SCHWABE, Peter. - Post-quantum key exchange - a new hope. **Cryptology ePrint Archive 2015**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.semanticscholar.org/paper/GLYPH%3A-A-New-Insantiation-of-the-GLP-Digital-Scheme-Chopra/3e019c349161bb6a258f97c59b992b7c7cb796a4 >.

[117] Wang, Yongge. - **Revised Quantum Resistant Public Key Encryption Scheme RLCEand IND-CCA2 Security for McEliece Schemes**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://pdfs.semanticscholar.org/1ffb/51b130157b073cce4aee2d6bd287d8f7fcb3.pdf>.

[118] MISOCZKI, R.; TILLICH, J. P.; SENDRIER, N.; BARRETO, P. - MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. **2013 IEEE International Symposium on Information Theory**. 2013. ISBN 978-1-4799-0446-4. p. 2069–2073.

[119] COSTELLO, C.; LONGA, P.; NAEHRIG, M.. - Efficient Algorithms for Supersingular Isogeny Diffie-Hellman. Robshaw M., Katz J. (eds) Advances in Cryptology : **CRYPTO 2016**. ISBN 978-3-662-53017-7

[120] COSTELLO C.; JAO, D.; LONGA, P.; NAEHRIG, M.; RENES, J.; URBANIK, D. - Efficient Compression of SIDH Public Keys. Coron JS., Nielsen J. (eds) Advances in Cryptology. **EUROCRYPT, 2017**. ISBN 978-3-319-56619-1

[121] **Open Quantum Safe**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://openquantumsafe.org/ >.

[122] STEBILA, Douglas; MOSCA, Michele. - Post-Quantum Key Exchange for the *Internet* and the Open Quantum Safe Project. **Springer**. 2017. Vol. 10532, p. 1-24. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://eprint.iacr.org/2016/1017.pdf >.

[123] Open Quantum Safe. - **C library for quantum-resistant cryptographic algorithms**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://github.com/open-quantum-safe/liboqs >.

[124] Open Quantum Safe. - **openssl: Fork of OpenSSL that includes quantum-resistant algorithms and ciphersuites based on liboqs**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://github.com/open-quantum-safe/openssl >.

[125] Open Quantum Safe. - **liboqs nist-branch algorithm datasheet: kem_newhopenist**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://github.com/open-quantum-safe/liboqs/blob/7cc365a363a05cdb233b9d72d0164c123d7b0b65/docs/algorithms/kem_newhopenist.md >.

[126] LAMACCHIA, Brian; COSTELLO, Craig; et al. - **Craig Costello Lattice Cryptography Library**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.microsoft.com/en-us/research/project/lattice-cryptography-library/ >.

[127] BOS, Joppe; COSTELLO, Craig; et al. - **Take off the ring! Practical, Quantum-Secure Key Exchange from LWE**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://eprint.iacr.org/2016/659 >.

[128] NTRUOpenSourceProject. - **libntruencrypt**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://github.com/NTRUOpenSourceProject/NTRUEncrypt >.

[129] BOS, Joppe; COSTELLO, Craig; et al. - **SIDH Library**. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://www.microsoft.com/en-us/research/project/sidh-library/ >.

[130] COSTELLO C.; JAO, D.; et al. - **Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies**. [Consult. 28 Jul. 2019]. Disponível na

Internet:<URL: https://web.archive.org/web/20140503190338/http://eprint.iacr.org/2011/506>.

[131] BERNSTEIN, Daniel J.; CHOU, Tung; SCHWABE, Peter. - **McBits: fast constant-time code-based cryptography** [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://eprint.iacr.org/2016/659 >.

[132] CHASE, Melissa; DERLER, David; et al. - The Picnic Signature Scheme. Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. **ACM CCS.** 2017. [Consult. 28 Jul. 2019]. Disponível na *Internet*:<URL: https://github.com/Microsoft/Picnic/blob/master/spec/design-v1.0.pdf >.

[133] BENNETT, Charles H., BRASSARD, G.. - Quantum cryptography: Public key distribution and coin tossing. **Theoretical Computer Science**. Vol. 560, nº 1 (2014), p. 7-11. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://core.ac.uk/download/pdf/82447194.pdf >.

[134] BENNETT, Charles H. - Quantum cryptography using any two nonorthogonal states. **American Physical Society**. 68:21, 3121-3124 (1992). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.68.3121 >.

[135] ARTUR, Ekert. - Quantum cryptography based on Bells theorem. **American Physical Society**. 67:6, 661-663 (1991). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: http://cqi.inf.usi.ch/qic/91_Ekert.pdf>.

[136] IBM. **IBM Q Experience Composer**. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://quantum-computing.ibm.com/composer >.

[137] KUNTAL HALDER, Narendra N. HEGADE, Bikash K. BEHERA, Prasanta K. Panigrahi. - Digital Quantum Simulation of Laser-Pulse Induced Tunneling Mechanism in Chemical Isomerization Reaction. **Indian Institute of Science Education and Research**

Kolka. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1808.00021.pdf >.

[138] MALIK, Gaurav; SINGH, Rahul; BEHERA, Bikash; PANIGRAHI, Prasanta. - First Experimental Demonstration of Multi-particle Quan-tum Tunneling in IBM Quantum Computer. **Indian Institute of Science Education and Research Kolkata**. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://www.researchgate.net/publication/330216616_First_Experimental_Demonstration_of_Multi-particle_Quan-tum_Tunneling_in_IBM_Quantum_Computer/link/5c348f99a6fdccd6b59b2be8/download >.

[139] DAATTAVYA, Aggarwal; SHIVAM, Raj; BIKASH, K. Behera; PRASANTA, K. Panigrahi. - Application of quantum scrambling in Rydberg atom on IBM quantum computer. **Indian Institute of Science Education and Research Kolkata**. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1806.00781.pdf >.

[140] DAATTAVYA, Aggarwal; SHIVAM, Raj; BIKASH, K. Behera; PRASANTA, K. Panigrahi. - Experimental demonstration of non-local controlled-unitary quantum gates using a five-qubit quantum computer. **Quantum inf. process.** 17:274 (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1709.05697.pdf >.

[141] SCHULD, Maria; FINGERHUTH, Mark; PETRUCCIONE, Francesco. Implementing a distance-based classifier with a quantum interference circuit. **Europhys**. 119:6 (2017). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1703.10793.pdf >.

[142] TANNU, Swamit S.; QURESHI, Moinuddin K.. - A Case for Variability-Aware Policies for NISQ-Era Quantum Computers. **Emerging Technologies**. (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/ftp/arxiv/papers/1805/1805.10224.pdf >.

[143] WOOTTON, James R. - **Benchmarking of quantum processors with random circuits. University of Basel**. (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1806.02736v1.pdf >.

[144] MANABPUTRA; BEHERA, Bikash K.; PANIGRAHI, Prasanta K. - A Simulational Model for Witnessing Quantum Effects of Gravity Using IBM Quantum Computer. **Indian Institute of Science Education and Research Kolka**. (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1806.10229.pdf >.

[145] VIYUELA, O. et al., Observation of topological Uhlmann phases with superconducting qubits. **Department of Physics, Harvard University**. 4:10 (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1607.08778.pdf >.

[146] GARCÍA-MARTÍN, Diego; SIERRA, Germán. - Five Experimental Tests on the 5-Qubit IBM Quantum Computer. **Journal of Applied Mathematics and Physics**. 6:7, p. 1460-1475 (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1712.05642.pdf >.

[147] JHA, Rounak; DAS, Debaiudh; DASH, Avinash; JAYARAMAN, Sandhya; BEHERA, Bikash K.; PANIGRAHI, Prasanta K.. - A Novel Quantum N-Queens Solver Algorithm and its Simulation and Application to Satellite Communication Using IBM Quantum Experience. **Indian Institute of Science Education and Research Kolka**. (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1806.10221.pdf>.

[148] Sisodia, M.; SHUKLA, A.; THAPLIYAL, K.. - Design and experimental realization of an optimal scheme for teleportaion of an n-qubit quantum state. **Quantum Inf. Process**. 16:292 (2017). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1704.05294.pdf >.

[149] BEHERA, Bikash K.; PANIGRAHI, Prasanta K; MANABPUTRA. - Generalization and Demonstration of an Entanglement Based Deutsch-Jozsa Like Algorithm Using a 5-Qubit Quantum Computer. **Quantum Inf. Process**. 17:160 (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1708.06375.pdf >.

[150] DEFFNER, Sebastian. - Demonstration of entanglement assisted invariance on IBM's Quantum Experience. **Heliyon 3**. (2017). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1609.07459.pdf >.

[151] YALCINKAYA, I.; GEDIK, Z. - Optimization and experimental realization of the quantum permutation algorithm. **Phys. Rev. A**. 96. (2017). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1708.07900.pdf >.

[152] SRINIVASAN, Karthik; SATYAJIT, Saipriya; BEHERA, Bikash K.; PANIGRAHI, Prasanta K.. - Efficient quantum algorithm for solving travelling sales man problem: An IBM quantum experience. **Indian Institute of Science Educationand Research Kolkat**. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1805.10928.pdf >.

[153] BEHERA, Bikash K.; PANIGRAHI, Prasanta K; DASH, Avinash; SARMAH, Deepankar. - Exact search algorithm to fatorize large biprimes and a triprime on IBM quantum computer. **Indian Institute of Science Educationand Research Kolkat**. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1805.10478.pdf >.

[154] HUFFMAN, Emilie; MIZEL, Ari. - Violation of noninvasive macrorealism by a superconducting qubit: Implementation of a Leggett-Garg test that addresses the clumsiness loophole. **Phys. Rev. A**. 95:3, (2017). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://journals.aps.org/pra/pdf/10.1103/PhysRevA.95.032131 >.

[155] ALSINA, Daniel; LATORRE, José Ignacio. - Experimental test of Mermin inequalities on a five-qubit quantum computer. **Phys. Rev. A**. 94:1 (2016). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.94.012314 >.

[156] KALRA, Amolak Ratan; GUPTA, Navya; BEHERA, Bikash K.; PRAKASH, Shiroman; PANIGRAHI, Prasanta. K. - Demonstration of the No-Hiding Theorem on the 5 Qubit IBM Quantum Computer in a Category Theoretic Framework. **Quantum Inf.**

Process. 18:170, (2019). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1707.09462.pdf >.

[157] Behera, Bikash K.; BANERJEE, Anindita; PANIGRAHI, Prasanta K.. - Experimental realization of quantum cheque using a five-qubit quantum computer. **Quantum Inf. Process**. 16:312, (2017). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1707.00182.pdf >.

[158] PLESA, M.-I.; MIHAI, T. - A New Quantum Encryption Scheme. **Advanced Journal of Graduate Research**. Vol. 4, p. 59-67. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://doi.org/10.21467/ajgr.4.1.59-67 >.

[159] MAJUMDER, Ayan; MOHAPATRA, Santanu; KUMAR, Anil. - Experimental Realization of Secure Multiparty Quantum Summation Using Five-Qubit IBM Quantum Computer on Cloud. **Scientific Reports**. 6:19655, (2017). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1707.07460.pdf >.

[160] GHOSH, D.; AGARWAL, P.; PANDEY, P.; BEHERA, B. K.; PANIGRAHI, P. K.. - Error Correction in IBM Quantum Computer and Explicit Generalization. **Quantum Inf. Process**. 17:153, (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1707.07460.pdf >.

[161] ROFFE, Joschka; HEADLEY, David; CHANCELLOR, Nicholas; HORSMAN, Dominic; KENDON, Viv. - Protecting quantum memories using coherent parity check codes. Quantum Sci. **Technol**. Vol. 3, (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1709.01866.pdf >.

[162] PANDEY, P.; BEHERA, B. K.; PANIGRAHI, P. K.; et al. - Nondestructive discrimination of a new family of highly entangled states in IBM quantum computer. **Quantum Inf. Process**. 17:212, (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/article/10.1007/s11128-018-1976-9 >.

[163] HARPER, Robin; FLAMMIA, Steven T.. Fault-Tolerant Logical Gates in the IBM Quantum Experience. **Phys. Rev. Lett**. 122:080504, (2019). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/abs/1806.02359 >.

[164] DASH, Avinash; ROUT, Sumit; BEHERA, Bikash K.; PANIGRAHI, Prasanta K.. - Quantum Locker Using a Novel Verification Algorithm and Its Experimental Realization in IBM Quantum Computer. **Quantum Inf Process**. 18:108, (2019). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1710.05196.pdf >.

[165] ALVAREZ-RODRIGUEZ, U.; SANZ, M.; LAMATA, L.; SOLANO, E.. - Quantum Artificial Life in an IBM Quantum Computer. **Scientific Reports**. 8:14793, (2018). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1711.09442.pdf >.

[166] BEHERA, B.K.; SETH, S.; DAS, A; et al. - Demonstration of entanglement purification and swapping protocol to design quantum repeater in IBM quantum computer. **Quantum Inf Process**. 18:108, (2019). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://link.springer.com/article/10.1007/s11128-019-2229-2 >.

[167] BEHERA, Bikash K.; REZA, Tasnum; GUPTA, Angad; PANIGRAHI, Prasanta K.. - **Designing Quantum Router in IBM Quantum Computer**. (2018) [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1803.06530.pdf >.

[168] GISIN, N.; RIBORDY, G.; TITTEL, W.; ZBINDEN, H.. - Quantum cryptography. **Rev. Mod. Phys**. 74:145, (2002). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/quant-ph/0101098.pdf >.

[169] ALSHOWKAN, M.; ELLEITHY, K.; ODEH, A.; ABDELFATTAH, E.. - **A New Algorithm for Three-Party Quantum Key Distribution. Third International Conference on Innovative Computing Technology**. 2013. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://ieeexplore.ieee.org/document/6653692/citations?tabFilter=papers >. ISBN: 978-1-4799-0048-0.

[170] KHYM, G. L.; Chung, W. Y.; Kim, J. I.; et al. - Quantum Key Distribution among Three Parties Using GHZ States. **Journal- Korean Physical Society**. 44:6, (2004). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://www.researchgate.net/publication/290098760_Quantum_key_distribution_among_three_parties_using_GHZ_states >. ISBN: 978-1-4799-0048-0.

[171] GUO, Y.; SHI, R.; ZENG, G.. - Secure networking quantum key distribution schemes with GreenbergerHorneZeilinger states. **Physica Scripta**. 81:4, (2010). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://www.researchgate.net/publication/231066588_Secure_networking_quantum_key_distribution_schemes_with_Greenberger-Horne-Zeilinger_states >.

[172] HILLERY, M.; BUZEK, V.; BERTHIAUME A.. - Quantum secret sharing. **Phys. Rev. A**, 59:3. (1999), p. 1829-1834. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/abs/quant-ph/9806063 >.

[173] JOHN STEWART, Bell. - On the Einstein Podolsky Rosen paradox. **John S. Bell on the foundations of quantum mechanics**. (1964), p.7-12. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://cds.cern.ch/record/111654?ln=pt >.

[174] Brunner, N.; Cavalcanti, D.; Pironio, S.; Scarani, V.; Wehner, S.. - Bell nonlocality. **Rev. Mod. Phys**. 86:2, (2014). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/abs/1303.2849 >.

[175] LI, X.; BARNUM, H.; Quantum Authentication Using Entangled States. **International Journal of Foundations of Computer Science**. 15:04, pp. 609-617. (2004). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://www.worldscientific.com/doi/abs/10.1142/S0129054104002649 >.

[176] ALSHOWKAN, Muneer; ELLEITHY, Khaled. - Quantum mutual authentication scheme based on Bell state measurement. USA : **Farmingdale**, 2016. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://ieeexplore.ieee.org/document/7494095 >. ISBN: 978-1-4673-8490-2.

[177] Stallings, W. - Cryptography and Network Security: Principles and Practice. 5th ed. Boston: **Pearson Education**. 2011. ISBN-13: 978-0-13-187316-2. p. 327-356.

[178] RIVEST, R.. The MD5 Message-Digest Algorithm. **MIT Laboratory for Computer Science**. (1992). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://www.ietf.org/rfc/rfc1321.txt >.

[179] EASTLAKE, D.. - US Secure Hash Algorithms (SHA and HMAC-SHA). **Motorola Labs**. (2006). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://www.ietf.org/rfc/rfc1321.txt >.

[180] YANG, Yu-Guang; XU, Peng; YANG, Rui; et al. - Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. **Scientific Reports**. 6:19788, (2016). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4731770/ >.

[181] ABLAYEV, Farid; VASILIEV, Alexander. - Quantum Hashing. **Kazan Federal University**. (2013). [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://arxiv.org/pdf/1310.4922.pdf >.

[182] SARKAR, Kounteya; BEHERA, Bikash K.; PANIGRAHI, Prasanta K.. - A robust tripartite quantum key distribution using mutually shared Bell states and classical hash values using a complete-graph network architecture. **Bikash K. Behera's Lab**. [Consult. 28 Jun. 2019]. Disponível na *Internet*:<URL: https://www.researchgate.net/publication/333148981_A_robust_tripartite_quantum_key_distribution_using_mutually_shared_Bell_states_and_classical_hash_values_using_a_complete-graph_network_architecture >.