ANDERSON GOMES DE OLIVEIRA

CRIPTOGRAFIA USANDO PROTOCOLOS QUÂNTICOS

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Pós-graduação Lato Sensu Administração de Redes Linux para obtenção do título de especialista.

Orientador
Prof. MSc. Joaquim Quinteiro Uchôa

LAVRAS
MINAS GERAIS – BRASIL
2004

ANDERSON GOMES DE OLIVEIRA

CRIPTOGRAFIA USANDO PROTOCOLOS QUÂNTICOS

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Pós-graduação Lato Sensu Administração de Redes Linux para obtenção do título de especialista.

Aprovada em 18 de setembro de 2004

_____

Prof. DSc. José Monserrat Neto

_____

Prof. MSc. Rudini Menezes Sampaio

_____

Prof. MSc. Joaquim Quinteiro Uchôa

(Orientador)

LAVRAS

MINAS GERAIS – BRASIL

Dedicatória

Este trabalho é dedicado a vários mestres que, na escola ou na vida cotidiana, foram, ao mesmo tempo, exemplos e guias nos caminhos que trilhei.

Aos meus pais, **José e Adélia**, meus mestres no caminho da vida;

Aos professores **Gabriel e Paulo Fernando**, meus mestres no caminho da Eletrônica;

Aos professores **Amábile, Armando, Paulo Henrique e Meneguzzi**, meus mestres no caminho da Física;

Aos *sensei* **Nilton Vieira e José Martins**, meus mestres no caminho do Budô;

Aos professores **Cleto e Joaquim**, meus mestres no caminho da Informática.

Cada um destes mestres, assim como tantos outros, não citados, contribuíram, cada qual a seu modo, para a minha formação humana, acadêmica e profissional.

As boas qualidades que porventura forem notadas nesse trabalho foram, em grande parte, mérito dos ensinamentos deles.

Os aspectos negativos são devidos às minhas próprias deficiências.

Resumo

Sistemas criptográficos baseados na codificação de informação em estados quânticos para distribuição de chaves criptográficas vêm sendo propostos como uma alternativa à criptografia clássica. Tais sistemas, por se basearem na inviolabilidade da leis da Física, apresentam o potencial, ao menos teórico, de garantia de segurança total. Neste trabalho serão apresentados os principais conceitos teóricos e resultados experimentais da Teoria Quântica necessários para a compreensão do funcionamento dos dois principais protocolos de criptografia quântica e uma discussão sobre o modo de funcionamento desses protocolos, destacando suas principais características, pontos fortes e vulnerabilidades.

Sumário

Capítulo 1 - Introducão

Os sistemas criptográficos clássicos (i.e. não-quânticos), apesar das inovações mais recentes, que possibilitam níveis de segurança muito altos, padecem de três problemas que podem aparecer isoladamente ou em conjunto dependendo do protocolo específico. O primeiro deles é conhecido como problema de distribuição de chaves e que foi resolvido, ao menos em parte, pelo uso de sistemas baseados em chave pública.

O segundo é que o nível de segurança que os sistemas clássicos mais eficientes podem oferecer baseia-se, em geral, na dificuldade, do ponto de vista computacional, de se decifrar as mensagens criptografadas usando estes sistemas e não em questões de princípio que garantam, do ponto de vista teórico, a sua inviolabilidade. Assim, citando por exemplo o sistema clássico RSA, a segurança fornecida baseia-se especificamente na dificuldade de se fatorar números naturais muito grandes em tempo razoável e não em algum princípio fundamental que garanta, com absoluta certeza, a impossibilidade de violação.

O terceiro problema refere-se à impossibilidade de se obter um canal totalmente seguro que não possa, em princípio, ser espionado passivamente, conforme demonstrado por Shannon na sua Teoria Matemática da Comunicação (SHANNON, 1948). Assim, em princípio, qualquer canal de transmissão de informações clássico pode ser espionado, tendo seus dados copiados/lidos sem que os correspondentes autorizados saibam que foram espionados.

Portanto, embora os sistemas clássicos tenham atingido um alto grau de refinamento e possam, considerando a tecnologia atual, fornecer níveis de segurança arbitrariamente grandes, os princípios matemáticos usados na formulação dos diversos protocolos criptográficos clássicos disponíveis não garantem, de modo geral, que eles continuarão viáveis em vista de novas tecnologias de análise criptológica, seja em termos de hardware mais avançado

(especialmente com o possível desenvolvimento de computadores quânticos de uso geral) ou de técnicas matemáticas inovadoras.

Este trabalho tem por principal objetivo apresentar a leitores com formação na área de informática, uma introdução ao uso de protocolos quânticos para a implementação de sistemas criptográficos extremamente seguros.

Atualmente, a maior parte do material sobre o assunto disponível na internet apresenta-se na forma de textos de divulgação científica ou de artigos técnicos sobre pontos específicos relacionados ao assunto. Dentre os primeiros, com algumas exceções, o que se encontra são textos superficiais, sem muito rigor científico. Já no caso dos artigos técnicos, o que se observa são artigos bastante técnicos, para a leitura dos quais um conhecimento adequado dos fundamentos da Teoria Quântica é um pré-requisito.

Esse é um campo de pesquisas que usa extensamente conceitos, ferramentas e resultados experimentais da Teoria Quântica. Uma apresentação destes protocolos para um público cuja formação acadêmica ou profissional não aborda, em princípio, conhecimentos avançados de física teórica ou experimental deve, necessariamente, incluir uma discussão sobre as principais características relevantes da Teoria Quântica. Além disso, tanbém é importante a apresentação dos principais resultados experimentais cuja interpretação pode contribuir para o entendimento dos princípios de funcionamento dos protocolos.

Assim, este trabalho foi estruturado de forma a discutir inicialmente os principais conceitos de física e criptografia relevantes e, só então, passar à descrição do funcionamento dos protocolos. Com isso, objetiva-se fornecer uma progressão estruturada na construção do conhecimento sobre o assunto para um público com conhecimentos técnicos na área de informática, especialmente administração e segurança de redes, mas não adequadamente familiarizado com os princípios da Teoria Quântica.

No Capítulo 2 serão apresentados vários conceitos básicos de

criptografia, uma definição do sistema criptográfico de Vernam, uma discussão sobre problemas nos sistemas clássicos e as motivações para o uso de sistemas criptográficos quânticos.

No Capítulo 3 serão apresentados conceitos básicos de Teoria Quântica, incluindo definições teóricas e discussão qualitativa sobre os resultados experimentais mais importantes para o entendimento de protocolos criptográficos quânticos. Considerando as características do público-alvo, os conceitos de Teoria Quântica serão apresentados usando uma abordagem baseada na mecânica ondulatória de Schröedinger que, complementada por discussões sobre questões experimentais e discussão de princípios gerais, pode ser tornada bem mais intuitiva para o leitor não familiarizado.

No Capítulo 4 será apresentado o protocolo BB84, o primeiro protocolo funcional a codificar a informação nos estados quânticos das partículas que transportam a informação, seguindo-se uma discussão sobre vulnerabilidades no protocolo, mecanismos de correção de erros e amplificação de privacidade.

O Capítulo 5 apresentará uma alternativa ao protocolo BB84, conhecida como protocolo de Ekert, que faz uso de correlações fortes entre as funções de onda das partículas envolvidas na comunicação. Como este protocolo depende diretamente dos resultados do experimento EPR aplicado a fótons, o Capítulo contém uma discussão sobre fótons geminados dentro do contexto EPR, uma apresentação do Teorema de Bell e uma explicação do funcionamento do protocolo de Ekert, que segue a mesma linha de apresentação usada no Capítulo 3 para o protocolo BB84.

Finalmente, o Capítulo 6 apresenta uma discussão sobre as linhas de pesquisa atuais e perspectivas em criptografia quântica.

Capítulo 2 – Conceitos básicos de criptografia

Este Capítulo apresenta alguns conceitos gerais de criptografia. Serão apresentados ainda, o problema da distribuição de chaves, as motivações para o uso de sistemas de criptografia quântica, assim como um breve histórico sobre o desenvolvimento inicial destes sistemas.

2.1) Definições iniciais

As definições apresentadas nesta seção serão apenas aquelas necessárias para as discussões subseqüentes sobre sistemas criptográficos clássicos e quânticos.

Embora todos os conceitos discutidos possam ser definidos de forma mais genérica e rigorosa, o autor optou por apresentar apenas definições simplificadas de cada termo ou conceito, rigorosas o bastante apenas para evitar ambigüidades no resto do texto. Para definições mais rigorosas desses ou de qualquer outro conceito ligado a criptografia em geral, recomenda-se a leitura de (SCHNEIER, 1996) e, no caso específico da aplicação destes conceitos à criptografia quântica, a leitura de (VOLOVICH, 2001) e (MAGNIEZ, 1993).

Criptografia: arte ou ciência de desenvolver códigos e cifras de modo a enviar mensagens em forma reconhecível e interpretável apenas para o destinatário e incompreensível para qualquer possível interceptador.

Criptoanálise: arte ou ciência de quebrar ou violar códigos e cifras;

Alfabeto: um conjunto de letras ou, de modo geral, de caracteres;

Texto simples (plaintext): mensagem original que se deseja enviar;

Texto cifrado ou encriptado: mensagem na forma disfarçada e ilegível

para receptores não-autorizados;

Unidade de mensagem: subconjuntos tanto do texto simples quanto do texto cifrado/encriptado;

Função de cifragem: seja o conjunto de todas as possíveis unidades de mensagem em texto simples. Define-se como função de cifragem, uma função f que, aplicada a qualquer elemento do conjunto *S* de todas as possíveis unidades de mensagem em texto simples, leve a algum elemento do conjunto *C* de todas as possíveis unidades de mensagens cifradas;

Transformação de decifração: o mapeamento (ou, basicamente, a função inversa da função de cifragem) que, aplicado a um texto cifrado, recupera o texto simples original;

Sistemas criptográficos: Um sistema criptográfico é definido como o conjunto de funções de cifragem e decifração, a especificação dos parâmetros permitidos para estas funções, as regras para o uso da função de cifragem, criação e distribuição de chaves, definição do alfabeto, dos conjuntos *S* e *C*, das unidades de mensagem e de todos os outros itens necessários para garantir que as mensagens cifradas só sejam legíveis para o destinatário visado pelo emissor da mensagem;

Chave criptográfica: Em um dado sistema criptográfico, a função de cifragem é definida de forma genérica de modo que uma escolha de parâmetro adequada (dentre os parâmetros compatíveis com a especificação do sistema) determina, dentre todas as funções possíveis, qual função específica será usada em um caso particular.

Para especificar exatamente qual o elemento do conjunto *C* de todas as possíveis unidades de mensagens cifradas será obtido pela aplicação da função de cifragem a um elemento qualquer do conjunto *S* de todas as possíveis unidades de mensagem em texto simples, existe um parâmetro de controle que deve ser especificado e que, definindo exatamente a função, selecionará

exatamente qual o resultado obtido pela aplicação dessa função de cifragem particular a uma certa unidade de mensagem. A esse parâmetro de controle se dá o nome de chave.

Da mesma maneira, a transformação de decifração é definida de modo genérico quando da especificação do sistema e a escolha da chave adequada é que fará com que seja feito o mapeamento correto entre mensagem cifrada e texto descriptografado.

Dependendo da especificação do sistema criptográfico, pode ser usada a mesma chave na cifragem e na decifração (sistemas criptográficos simétricos) ou podem ser usadas chaves diferentes para criptografar e descriptografar (sistemas criptográficos assimétricos).

2.2) Sistemas criptográficos clássicos

Em um sistema criptográfico clássico, as chaves usadas na cifragem e decifração das mensagens são distribuídas aos participantes autorizados da comunicação utilizando-se canais clássicos (não-quânticos) ou combinadas previamente entre eles.

2.2.1) Criptografia de chave privada

Um sistema no qual qualquer receptor que possua a chave de criptografia pode decifrar a mensagem é chamado de sistema criptográfico de chave privada.

Em tais sistemas, a chave usada na transformação de decifração é a mesma usada na função de cifragem (ou pode ser obtida trivialmente a partir da mesma).

Um exemplo simples desse tipo de sistema é a clássica Chave de César.

Neste sistema, a encriptação da mensagem consiste em substituir cada

letra da mensagem original (texto simples) pela letra que fica *n* posições à frente considerando o alfabeto latino. O número *n* é a chave do sistema e deve ser mantido em segredo por ambas as partes, podendo ser previamente combinado ou tendo que ser transferido em algum momento antes, durante ou depois da transmissão da mensagem cifrada, usando ou não o mesmo canal de comunicação.

Deve-se salientar que, de um modo geral, os sistemas criptográficos de chave privada, como a Cifra de César ou o Código de Vernam, discutido na seção 2.2.1.1, apresentam o incoveniente de necessitarem de algum mecanismo confiável para distribuir as chaves criptográficas entre os participantes.

Esse incoveniente acaba por se tornar uma deficiência séria, pois, caso haja alguma falha de segurança no armazenamento ou na transmissão das chaves, qualquer segurança que poderia ser fornecida pelo uso de criptografia torna-se completamente comprometida. Qualquer espião que possua a chave poderá facilmente ler as mensagens trocadas entre os participantes autorizados em uma determinada troca de mensagens.

Outro exemplo sistema que usa chave privada é o Sistema de Vernam (MAGNIEZ, 1993), também conhecido como *One-time Pad*. Por sua relevância no uso em criptografia quântica, será apresentado com mais detalhes.

2.2.1.1) Sistema *One-time Pad* ou código de Vernam

É um sistema de codificação onde se usa uma chave tão longa (mesma quantidade de caracteres) quanto o texto a ser transmitido.

A chave e o texto plano são adicionados ciclicamente, termo a termo.

Essa adição cíclica é o equivalente da operação binária "**ou exclusivo".**

Dentre todos os métodos clássicos, é o único para o qual se pode demonstrar inviolabilidade absoluta desde que cada chave seja usada apenas

uma única vez.

O sistema, na sua versão binária, pode ser definido formalmente assim (MAGNIEZ, 1993):

1) Codificação (*A* envia uma mensagem para *B*)

Seja *T*, a mensagem binária a ser codificada:

$T = t_1 t_2 t_3 ... t_n$

Onde os termos t_i representam os bits individuais da *string T*.

Seja *K*, a chave binária de codificação:

$K = k_1 k_2 k_3 ... k_n$

A mensagem codificada *C* a ser enviada é dada por:

$C = c_1 c_2 c_3 ... c_n$

Onde, para todo *i*, tem-se:

$c_i = t_i \oplus k_i$

2) Decodificação (*B* recupera o texto plano a partir da mensagem recebida).

A mensagem recebida por *B* é *C*:

$C = c_1 c_2 c_3 ... c_n$

B usa a chave *K*, igual `a chave usada por *A* e obtém a mensagem *T*:

$T = t_1 t_2 t_3 ... t_n$ onde:

$t_i = c_i \oplus k_i$

Apesar da promessa de segurança total, três características desse método não o tornam muito prático do ponto de vista de clássico:

1) Asserção inicial forte (única utilização de cada chave);

2) São necessárias chaves muito grandes para transmitir mensagens muito grandes;

3) O problema de distribuição de chaves ou, alternativamente, o problema de armazenar as chaves com segurança.

No entanto, caso se consiga um meio de se transmitir longas chaves com segurança garantida, será possível obter um sistema completamente seguro combinando o uso de chaves assim obtidas com o sistema de Vernam. Conforme será apresentado no capítulo 3, é justamente isso que os protocolos quânticos se propõem a fazer

2.2.2) Problema de distribuição das chaves

Para trocar mensagens cifradas, emissor e destinatário devem combinar previamente entre si, de algum modo, a chave que será utilizada.

Uma vez que o destinatário precisa conhecer a chave para decifrar a mensagem, ambos devem combinar previamente a chave e, de algum modo, armazená-la em local seguro, ou deverão usar algum canal extremamente seguro para transferí-la.

Do ponto de vista da física clássica (que governa os canais usados na criptografia clássica), nada impede que um terceiro não-autorizado possa monitorar o canal de transmissão e "escutar" a mensagem sem ser percebido pelos correspondentes autorizados. Assim, se esse terceiro conseguir interceptar a chave quando de sua distribuição, ele poderá decifrar qualquer mensagem trocada sem que os correspondentes legítimos sequer percebam a quebra de privacidade.

Para resolver o problema da distribuição de chaves em sistemas criptográficos de chave privada, ainda dentro do escopo da criptografia clássica, foram propostos os sistemas de criptografia de chave pública.

2.2.3) Criptografia de chave pública

Nesses sistemas, para cada usuário autorizado, são geradas duas chaves, a chave privada e a chave pública. A função de cifragem é definida de tal forma que o emissor *A*, que deseja enviar uma mensagem para *B*, usa a chave pública de *B* para criptografar a mensagem original e, uma vez criptografada, a mensagem só pode ser descriptografada usando a chave privada de *B*.

Para garantir a segurança de um sistema de criptografia de chave

pública, deve-se escolher funções e chaves de modo que, mesmo possuindo a chave de criptografia, não se possa, usando qualquer poder computacional clássico disponível, ainda que durante intervalos de tempo enormes, quebrar o código, isto é, descriptografar o texto sem um conhecimento prévio da chave de decifração.

Um exemplo desse tipo de criptografia é o sistema RSA, que se baseia no fato de que, para fatorar grandes inteiros de N dígitos, o número de passos necessários cresce mais rapidamente que qualquer polinomial em N.

No entanto, isso se baseia mais em conhecimento empírico que em certeza matemática, uma vez que não há prova rigorosa de que seja realmente assim.

No sistema RSA, dois correspondentes A e B podem gerar, cada um, as suas respectivas chaves privada e pública, anunciar a sua chave pública e trocar mensagens cifradas usando cada qual, como parâmetro da função de cifragem, a chave pública do outro.

A segurança é garantida usando-se números inteiros muito grandes, que sejam produtos de 2 números primos grandes (usados para gerar as chaves), e mantendo ocultas as respectivas chaves privadas. Mantidas essas restrições, as mensagens enviadas só poderão ser decifradas pelo dono da chave privada correspondente à chave pública usada na codificação.

Para detalhes matemáticos e explicações completas do procedimento de criação de chaves e das funções de cifragem e de decifração, como já mencionado, recomenda-se a leitura de (SCHNEIER, 1996), (VOLOVICH, 2001) e (MAGNIEZ, 1993).

Os sistemas de criptografia por chave pública resolveram, na prática, o problema da distribuição de chaves, embora não de forma definitiva, uma vez que não há prova rigorosa de que o sistema não possa ser quebrado.

Recentemente, Manindra Agrawal e colaboradores (AGRAWAL, 2002),

criaram um algoritmo capaz de dizer, com certeza absoluta, se um determinado número é primo ou não e que pode ser executado em tempo que cresce polinomialmente com o tamanho do número (e não exponencialmente como outros esquemas anteriormente propostos).

Embora tal resultado não comprometa diretamente a segurança do método RSA, ele ilustra bem como progressos inesperados na Teoria dos Números, especialmente a pesquisa sobre números primos, podem ameaçar a segurança desse sistema. Um resultado como esse pode permitir o refinamento de métodos para fatoração de grandes inteiros, o que pode resultar em ataques mais eficientes ao sistema RSA que o simples uso de força bruta computacional.

Além disso, restam ainda o problema de armazenamento seguro das chaves e, especialmente, o da detecção de intrusos no canal de transmissão, pois os mesmos, em qualquer sistema clássico, ainda podem interceptar as mensagens sem ser detectados e armazená-las indefinidamente. Mesmo que tais sistemas não possam ser quebrados atualmente, nada impede que mensagens interceptadas possam ser lidas no futuro, usando métodos ainda não descobertos.

2.2.4) Motivação para o uso de criptografia quântica

A motivação original para a utilização de elementos da teoria quântica em criptografia foi a de fornecer um nível total de segurança em uma comunicação criptografada, mesmo supondo um espião com poder computacional ilimitado.

Tal nível de segurança exigiria uma solução definitiva tanto para a questão de distribuição das chaves (ou do armazenamento seguro das mesmas), quanto para a determinação de espionagem passiva, ou seja, a captura dos dados em trânsito sem que os correspondentes se apercebam do ocorrido.

Afinal, além da possibilidade de leitura imediata dos dados, deve-se levar em conta a possibilidade de certos dados muito importantes serem copiados e armazenados para leitura posterior quando houver soluções disponíveis para decodificação.

A criptografia quântica surge como alternativa. Através da codificação de informação em estados quânticos de partículas elementares, as leis e princípios da física são usadas como garantia de segurança do sistema.

2.2.5) Histórico da criptografia quântica

A história da criptografia quântica pode ser traçada a partir de um evento determinante que, na época, passou praticamente despercebido.

Em 1969, Stephen J. Wiesner, escreveu o artigo "Conjugate Coding" onde fazia duas propostas inéditas de aplicação da Teoria Quântica:

1) A produção de notas de dinheiro (dinheiro quântico) totalmente imunes à falsificação;

2) Um método para combinação de duas mensagens em uma única transmissão quântica de modo que o receptor pudesse escolher uma delas, mas não as duas. A leitura de uma, automaticamente destruindo a outra.

O artigo (WIESNER, 1983), apesar de inovador, pois lançou as bases do ramo de criptografia quântica, foi recusado para publicação e permaneceu inédito até 1983.

A idéia original de Wiesner para o dinheiro quântico era possível em princípio, mas não na prática, devido à dificuldade de se armazenar fótons e manter os seus estados inalterados e não-medidos por longos períodos de tempo.

Charles Bennet e Gilles Brassard (que conheciam Wiesner e tomaram conhecimento de suas idéias em contatos pessoais) retomaram a idéia de Wiesner e modificaram o seu esquema original, de modo a usar fótons para transmitir informação codificada ao invés de apenas armazená-la.

Por volta de 1982, ambos começaram a publicar uma série de trabalhos conjuntos, em que começaram a formular os primeiros protocolos de criptografia quântica. Tais protocolos eram possíveis em princípio mas não implementáveis na prática.

Em 1984, os trabalhos culminaram no estabelecimento do primeiro protocolo realmente funcional, chamado de BB84, de acordo com as iniciais dos autores e do ano de criação.

Devido às dificuldades técnicas envolvidas, a primeira implementação real de protocolo só começou a ser construída em 1989, com uma reunião de uma equipe maior, formada por Bennet, Brassard, John Smolin (que projetou e preparou a aparelhagem experimental), François Bessette e Louis Salvail (responsáveis pelo software de controle). Esse grupo publicou, em 1991, um artigo conjunto entitulado "Experimental Quantum Criptography" (BENNET, 1991), que, pela primeira vez, demonstrou a viabilidade prática da criptografia quântica que, até o momento, parecia apenas um assunto puramente especulativo.

Também em 1991, com base em sugestões teóricas de David Deutsch, Artur Ekert idealizou um outro protocolo, baseado em estados quânticos fortemente correlacionados, conhecido como Protocolo de Ekert (EKERT, 1991).

Estes dois protocolos formaram a base e o modelo para a maioria dos trabalhos posteriores sobre a utilização de canais quânticos para a distribuição de chaves criptográficas.

Capítulo 3 - Fundamentos da Teoria Quântica

Na literatura sobre criptografia quântica disponível, os conceitos da Teoria Quântica são apresentados dentro do formalismo proposto por Dirac. Embora tal formalismo seja o mais indicado para apresentações axiomáticas e se constitua em uma ferramenta poderosa para enunciação de princípios e demonstrações de teoremas, esse trabalho foi escrito para leitores não familiarizados com o formalismo da teoria e, portanto, optou-se pela abordagem ondulatória, mais intuitiva para os mesmos.

Nas próximas seções, relativas a fundamentos da teoria quântica, o autor optou por apresentar os conceitos seguindo a abordagem da mecânica ondulatória baseada na equação de onda de Schröedinger e interpretação probabilística de Born.

Para apresentações mais rigorosas, baseadas no formalismo de Dirac e na mecânica matricial de Heisenberg recomenda-se, como introdução, a leitura de (DIRAC, 1958).

3.1) Atributos estáticos e dinâmicos

Do ponto de vista da teoria quântica, os atributos que uma partícula podem ter são divididos em estáticos e dinâmicos.

Os atributos estáticos são aqueles inerentes às partículas, possuindo o mesmo valor para todas as partículas do mesmo tipo e sendo invariáveis com o tempo para um mesmo tipo de partícula.

São atributos estáticos, por exemplo de um elétron, a massa, a carga e a magnitude do momento angular (*spin*).

Os atributos dinâmicos ou contextuais são aqueles que não são constantes para uma determinada partícula. Nesse grupo se enquadram a

posição, a quantidade de movimento (*momentum*), energia, direção de rotação, etc, que podem apresentar valores diferentes de acordo com o contexto da medição.

Na física clássica, nada impede que um determinado atributo dinâmico seja medido com precisão absoluta, exceto questões relacionadas à precisão da aparelhagem usada e da engenhosidade do experimentador .

Na física quântica, os atributos dinâmicos são representados por ondas. De um modo totalmente distinto da física clássica, quando se trata de partículas elementares e/ou de eventos que envolvam trocas de energia muito pequenas, há uma limitação fundamental na natureza quanto ao nível de certeza com que se pode conhecer estes atributos.

A Teoria Quântica representa estes atributos através de ondas de probabilidade e, no que se refere a interações entre partículas subatômicas, tudo o que se pode saber sobre os atributos dinâmicos de uma partícula antes da efetiva medição de um determinado atributo é a probabilidade de que ele possua um determinado valor.

A representação usada na teoria quântica consiste em, conhecidas as condições iniciais e de contorno nas quais será realizada uma determinada medida, obter uma função de onda (função ψ), que representa o comportamento da partícula naquelas condições.

3.2) Ondas e superposição

Uma onda é caracterizada por alguma grandeza física cujo valor varia tanto no espaço quanto no tempo. Os parâmetros importantes para caracterizar uma certa onda são:

1) Amplitude : mede o desvio da variável fisica representada em

relação ao estado de repouso;

2) Intensidade : que indica a quantidade de energia transportada pela onda e que é proporcional ao quadrado da amplitude.

No caso de ondas oscilatórias (que possuem ciclos bem definidos no espaço e no tempo e representam flutuações periódicas), são importantes também:

1) Período: o intervalo de tempo gasto na repetição de um ciclo completo;

2) Comprimento de onda: que diz o quanto uma onda oscilatória avança no espaço durante um ciclo completo;

3) Fase: que indica o quanto, em um determinado momento ou em um determindo ponto, o valor da grandeza física avançou em relação ao estado de repouso.

Ondas se propagam. Se uma partícula carregada está em repouso num determinado ponto do espaço, ela gera um campo elétrico estático (cuja amplitude e direção permanecem constantes ao longo do tempo para cada ponto) em todo o espaço ao seu redor. No caso de um campo elétrico, cada ponto no espaço ao redor possuirá um valor diferente de intensidade do campo elétrico (que depende da distância do ponto à posição da partícula) e uma direção diferente do vetor campo elétrico (nesse caso, será sempre radial em relação à posição da partícula geradora do campo).

Caso a partícula se mova para uma nova posição, o campo não se ajusta

instantaneamente para novos valores em todo o espaço ao mesmo tempo. Ao invés disso, propaga-se uma perturbação no campo cujos valores vão se ajustando para o novo valor (que depende da posição final da partícula) com o campo nos pontos mais próximos à partícula variando primeiro e os pontos mais distantes variando depois à medida em que a perturbação se propaga.

Caso a partícula se mova periodicamente, oscilando entre duas posições diferentes, a perturbação no campo se propagará seguindo o mesmo padrão oscilatório. Como os pontos mais próximos à partícula oscilante serão atingidos pela perturbação primeiro, esses pontos estarão com a fase adiantada em relação a pontos mais distantes.

A essa perturbação se propagando dá-se o nome de onda.

Quando duas ondas se encontram, ou seja, quando duas perturbações de origens diferentes atingem o mesmo ponto no espaço, a amplitude da oscilação resultante naquele ponto em cada momento será a soma das oscilações que cada onda causaria individualmente. Isso se chama **Princípio da Superposição**.

Como as duas ondas, em geral não estarão em fase naquele ponto (uma pode estar no seu valor máximo, enquanto que a outra pode estar com apenas 10% do valor máximo) ou então estar no seu valor mínimo, o valor da oscilação resultante em cada ponto dependerá das freqüências de oscilação das fontes geradoras das ondas, da amplitude de oscilação de cada uma e da fase relativa.

Assim, se duas ondas de mesma amplitude se encontram em um certo ponto e ambas com a mesma fase, a oscilação resultante será duas vezes maior naquele ponto. Por outro lado, se uma delas estiver no seu valor máximo enquanto que a outra estiver no seu valor mínimo, não ocorrerá, naquele ponto, oscilação nenhuma.

3.3) Teorema de Fourier

De modo geral, qualquer onda complexa pode ser decomposta em ondas mais simples (com diferentes amplitudes, fases, períodos e comprimentos de onda), de tal modo que o efeito da soma de todas essas ondas mais simples, superpostas, resultaria em uma onda indistinguível da onda original.

O matemático francês Fourier, demonstrou que qualquer onda poderia ser decomposta em ondas senoidais com amplitudes, freqüências e fases devidamente ajustadas de tal modo que a soma resultante de todas essas ondas recomporia a onda original.

Para entender como isso funciona, pode-se considerar o caso do som produzido por dois instrumentos musicais diferentes, por exemplo, um violino e um saxofone.

Embora ambos possam emitir a mesma nota (uma perturbação que se propaga no espaço à mesma freqüência ou que oscila com o mesmo período), as formas das ondas (os padrões de oscilação) emitidas por esses instrumentos são bastante diferentes e essa diferença é percebida como um timbre diferente, característico de cada instrumento.

A aplicação do teorema de Fourier a cada uma dessas ondas produziria como resultado dois conjuntos de ondas senoidais diferentes. Somando as ondas senoidais do conjunto de ondas do violino se obtem uma onda indistinguível da onda original e o mesmo ocorrerá para as ondas componentes da onda produzida pelo saxofone.

Do ponto de vista auditivo, não é possível distinguir a nota emitida por um violino real da nota resultante de vários osciladores que produzissem exatamente as ondas sonoras senoidais nas quais foi decomposta a onda de violino, já que o princípio da superposição e o teorema de Fourier garantem que a soma dessas ondas senoidais será, para todos os efeitos, equivalente à onda

emitida pelo violino.

3.4) Análise espectral

O teorema de Fourier garante que sempre se pode dividir uma certa onda em um conjunto de ondas senoidais que, se sobrepostas, resconstuiriam perfeitamente a onda original. No entanto, não há nada especial com as ondas senoidais e uma generalização do teorema de Fourier garante que se pode escolher uma certa forma de onda como base (digamos ondas triangulares) e, do mesmo modo, se pode decompor qualquer onda nessas ondas de base (no caso em um conjunto de ondas triangulares).

Um exemplo prático de decomposição de ondas em suas componentes é a experiência de Isaac Newton com a divisão da luz branca nas cores do arco-íris usando um prisma. A onda de luz branca é, na verdade, composta de várias ondas de cores (freqüências) diferentes que, quando sobrepostas se combinam para formar a luz branca.

A generalização do teorema de Fourier permite que se escolha uma família de formas de onda qualquer (ondas triangulares, dente-de-serra, impulsos, etc.) e que se possa decompor qualquer onda dada em um conjunto de ondas da família escolhida.

Um exemplo seria escolher, como família de ondas base, justamente as ondas que têm a mesma forma de onda produzidas por um violino. Se uma determinada onda sonora for decomposta em ondas de violino seria, em princípio, possível reproduzir exatamente o mesmo som usando toda uma orquestra de violinos, cada um deles tocando a nota representada por uma das componentes na amplitude e feqüência corretas conforme obtidas pela aplicação do teorema.

3.5) Famílias de ondas conjugadas

Seguindo o exemplo acima, se o som original for produzido por um violino, decompor essa onda em ondas de violino resultaria em um conjunto de ondas de violino formado por uma única onda (no caso, a própria onda original já que a mesma foi produzida por um violino) e, para reproduzí-la, a orquestra de violinos precisaria de apenas um violino tocando para produzir exatamente a mesma nota.

Por outro lado, pode-se escolher qualquer família de ondas (um formato de onda arbitrário qualquer) para realizar a decomposição de uma certa onda. Se for escolhida a mesma família de ondas da qual faz parte a onda original, o conjunto resultante será mínimo (formado por apenas uma onda).

Pode-se, no entanto, imaginar uma família de ondas que decomporia a onda original no maior conjunto de componentes individuais possível (talvez infinitas ondas).

Assim, cada possível forma de onda possui relação especial com duas famílias de ondas. Uma é a família da qual a própria onda faz parte (chamada de família afim) e a outra é a família que decompõe a onda original no maior número de ondas componentes possível (chamada de família conjugada). De modo geral, pode-se considerar que a família afim de uma certa forma de onda é aquela composta de todas as ondas possíveis que são as mais parecidas com a onda original, enquanto que a família conjugada é aquela composta das ondas que menos se parecem com a onda original.

Assim, cada família de onda possui uma família conjugada ou seja, um conjunto formado pelas ondas cuja forma menos se parece com as ondas daquela família.

Se uma certa onda A for decomposta em ondas da família X será obtido um conjunto de ondas do tipo X composto por N_x ondas. Se a mesma onda A for

decomposta em ondas da família *Y*, conjugada da família *X*, será decomposta em um conjunto de ondas do tipo *Y* formado por N_y ondas.

Se as ondas da família *X* forem distingüidas umas das outras por um parâmetro *p* que pode ser , por exemplo, a freqüência de cada uma das ondas, pode ser estabelecido um valor *DX*, proporcional à diferença entre o maior e o menor valor de *p* dentro do conjunto de ondas componentes.

Assim, $\Delta X = 0$ se N_x for igual a 1, correspondendo à decomposição da onda original em apenas um componente (o que indica que a onda pertence exatamente à família *X*) e também ocorrerá que *DX* crescerá se o número de ondas componentes for muito grande e tenderá ao infinito para o caso de serem necessárias infinitas ondas da família *X* para recompor a onda original.

De modo análogo, pode-se definir *DY*.

Matematicamente se demonstra que, sendo *X* e *Y* famílias conjugadas, o produto de *DX* (variância de *X*) por *DY* (variância de *Y*) será sempre maior que a unidade. Simbolicamente:

$$\Delta X \times \Delta Y > 1$$

O que pode ser interpretado como uma indicação de que se uma onda qualquer for decomposta usando duas famílias de ondas conjugadas entre si, não será possível dividir a mesma onda em apenas um componente de cada família.

Assim, se *DX* for igual a 0, isso quer dizer que a onda *A* pertence à família *X* e que, se for decomposta em ondas da família *Y*, a quantidade de ondas *Y* necessárias para recompor a onda *A* original será uma série infinita.

A desigualdade acima (uma propriedade da teoria das ondas) leva diretamente ao Princípio da Incerteza de Heisenberg.

3.6) Medidas quânticas

Na teoria quântica, para se representar uma entidade em uma determinada situação, através das informações sobre condições iniciais e de contorno de cada situação, associa-se a cada entidade uma função de onda (função ψ) que passa a representar aquela entidade.

As ondas quânticas não representam diretamente nenhuma grandeza específica como as ondas da física clássica. A relação entre a onda ψ e a partícula é que o quadrado da amplitude da função de onda em um determinado ponto fornece a probabilidade de a partícula ser encontrada naquele ponto.

Fazendo uma analogia com a decomposição da luz branca por meio de um prisma transparente, pode-se considerar o procedimento matemático de decomposição de uma onda A (ou ψ) qualquer em uma determinada família de formas ondulatórias X como sendo o equivalente a forçar a passagem da onda A por um prisma especial (um analisador de sinal adequado) capaz de dividir a onda nos seus componentes na forma ondulatória desejada.

Um prisma desse tipo corresponde a um operador matemático com propriedades especiais que, uma vez aplicado à função de onda, a decompõe em ondas da família correspondente àquele operador.

Na teoria quântica, a cada atributo dinâmico está associado um operador matemático especial com determinadas propriedades específicas, de forma que a sua aplicação em uma certa onda ψ a decompõe em várias ondas associadas aos vários valores que aquele atributo pode assumir.

A associação se dá do seguinte modo: cada uma das ondas resultantes possuirá algum parâmetro que a distinguirá das outras ondas da mesma família. O parâmetro em questão pode ser a freqüência, o comprimento de onda ou qualquer outro, dependendo do atributo que se queira medir e existirá uma

relação bem determinada entre o valor desse parâmetro e a magnitude da quantidade física que se deseja medir.

O quadrado da amplitude de cada uma das ondas obtidas, através da aplicação do operador, dá a probabilidade de que aquele atributo dinâmico assuma o valor correspondente ao parâmetro distintivo daquela onda particular quando for efetuada uma medida.

Assim, se o interesse for medir um determinado atributo *w* de uma partícula em uma determinada situação experimental, constrói-se a função de onda para a partícula levando-se em conta as condições de realização do experimento e os parâmetros relativos às grandezas físicas envolvidas.

Obtida a função ψ, aplica-se o operador correspondente à grandeza *w* àquela função.

Será obtido um conjunto de ondas da família associada àquele operador e cada onda possuirá um parâmetro que a diferenciará das outras do mesmo conjunto.

Esse atributo pode ser, por exemplo, a freqüência de oscilação de cada uma das ondas. Haverá uma relação bem determinada entre o valor desse parâmetro e o valor da grandeza w que se quer medir. A relação pode ser tão simples quanto:

$$w = 2\pi \times h \times f$$

Onde *f* é a freqüência da onda e *h* é uma constante.

Como cada onda obtida na decomposição apresentará um valor de freqüência diferente, as diversas freqüências f_1, f_2, f_3 ... determinarão os valores que a grandeza w pode assumir, a quantidade de ondas obtidas na decomposição dirá quantos valores possíveis a grandeza poderá assumir e o quadrado da amplitude de cada onda indicará a probabilidade do valor assumido ser aquele

representado por ela.

Desse modo, se forem obtidas 2 ondas, s_1 e s_2, com freqüências f_1 e f_2 respectivamente, a partícula analisada poderá possuir dois valores possíveis de w (w_1 e w_2), um deles proporcional a f_1 e o outro proporcional a f_2. A probabilidade de que o valor medido seja w_1 será dado pelo quadrado da amplitude de s_1 e a probabilidade de que o valor medido seja w_2 será o quadrado da amplitude de s_2.

Se o quadrado da amplitude de s_2 for 0,8 (80%) e o de s_1 for 0,2 (20%), isso quer dizer que, se os experimento em questão for realizado com um grande número de partículas, 80% delas possuirá o valor w_2 e 20% delas possuirá o valor w_1.

Sendo a mecânica quântica uma teoria probabilística, isso é tudo que poderemos saber sobre as partículas nesse exeprimento. Não será possível dizer exatamente qual o valor exato da grandeza w para cada partícula individual. Tudo que a teoria nos informa é a probabilidade associada a cada valor possível de w.

Na Teoria Quântica, as partículas simplesmente **não possuem** nenhum valor bem definido de seus atributos antes que seja realizada uma medida.

Antes de se realizar uma medida, ou ocorrer uma interação qualquer, tudo o que se pode saber sobre os atributos de uma partícula resume-se ao conhecimento de sua função de onda.

As partículas só passam a possuir valores definidos após a realização de uma medida.

Realizar uma medida significa que, dentre os valores possíveis do atributo que se quer medir, um deles será selecionado e se tornará real. Devido a essa característica da teoria, a realização de uma medida é chamada de **colapso da função de onda** (de todas as possibilidades representadas pala onda original, no ato da medida, apenas uma componente é selecionada)**.**

3.7) Princípio da Incerteza de Heisenberg (PIH)

Do mesmo modo que as ondas comuns, as ondas de probabilidade quânticas podem ser decompostas em famílias de ondas diferentes dependendo dos operadores escolhidos. Cada operador válido têm, associado a si, um determindo atributo. Assim, temos um operador para a energia, outro para o momento linear ou simplesmente *momentum* (massa x velocidade), um para posição, etc.

Se um certo operador *R* decompõe as ondas em uma determinada família F_1, haverá um operador *Q* (chamado de conjugado de *R*) que decomporá uma onda ψ na família de ondas F_2, conjugada a F_1. Os dois operadores *R* e *Q* são ditos conjugados entre si.

Sejam dois parâmetros *x* e *y*, que distinguem as ondas das famílias F_1 e F_2, respectivamente.

Se o operador *R* dividir a onda ψ em n ondas da família F_1, *Q* dividi-la em *m* ondas da família F_2 e houver duas grandezas físicas observáveis *X* e *Y* tais que $X_i=X_i(x_i)$ e $Y_j=Y_j(y_j)$, onde x_i e y_j representam todos os valores possíveis para *x* e *y*, então, a aplicação do Teorema de Fourier generalizado levará à seguinte desigualdade:

$$\Delta X \times \Delta Y > h/4\pi$$

Onde h é uma constante da natureza, chamada de Constante de Planck.

A desigualdade acima é chamada de Princípio da Incerteza de Heisenberg (PIH) e determina que, se forem realizadas medidas de dois atributos conjugados quaisquer, não se poderá ter certeza absoluta sobre ambos ao mesmo tempo.

Por exemplo, na formulação original de Heisenberg, as grandezas físicas são r, a posição da partícula, e p, o momentum da partícula.

Em um exemplo simples, se a partícula se move ao longo do eixo y, então Δy representa o comprimento do intervalo para o qual a onda ψ possui amplitude diferente de zero (domínio de ψ).

A aplicação do operador momentum em ψ, divide-a em várias ondas com número de onda k_1, k_2,....Como p=hk (fórmula de Compton), os momenta possíveis para a partícula são, hk_1, hk_2, ...

A relação de incerteza para posição e momentum fica:

$$\Delta y \times \Delta p = h/4\pi$$

O PIH estabele uma restrição absoluta nas possibilidades de medidas de atributos conjugados.

Ao se fazer uma medida exata de um certo atributo dinâmico como, por exemplo, a posição, torna-se impossível estimar o valor do momento linear já que ambos são atributos conjugados, segundo a teoria.

3.8) Fótons

Na física clássica, a luz é considerada como sendo uma vibração dos campos elétrico e magnético e que se propaga no espaço na forma de uma onda, com a velocidade da luz. Quanto maior a freqüência da vibração, maior a freqüência da luz.

A teoria quântica considera a luz como sendo constituída por partículas, chamadas de fótons às quais se pode, para todos os fins, associar uma onda ψ.

Os fótons são caracterizados pelos seguintes atributos: massa igual a

zero, velocidade sempre igual à da luz *c*, energia proporcional à sua freqüência (cor da luz) e polarização, que indica a direção de vibração do campo eletromagnético.

3.9) Polarização

A polarização é um atributo que está relacionado com uma direção no espaço.

A direção de polarização indica a direção de oscilação do campo elétrico, ou seja, a direção em que vibra a onda que compõe o feixe de luz.

Ao escolher uma determinada direção para medir o atributo polarização de um fóton, a teoria quântica diz que apenas dois resultados são possíveis (o que implica que a aplicação do operador polarização à onda ψ): ou o fóton está completamente polarizado naquela direção ou está polarizado em ângulo reto com ela.

Isso implica que, se for colocado um filtro de polarização com eixo óptico orientado de um ângulo θ no caminho de um fóton, ou o fóton estará polarizado naquela direção e passará pelo filtro, ou estará polarizado na direção perpendicular e será barrado e o mesmo valerá para qualquer ângulo escolhido para orientar o filtro.

3.9.1) Fontes de fótons

Na natureza existem certos materiais transparentes (geralmente cristais) que, se forem colocados no caminho de um feixe de luz, apresentam a propriedade de deixar passar somente fótons polarizados em uma única direção, designada como eixo óptico do cristal. Materiais com essa propriedade também podem ser produzidos artificialmente, como ocorre, por exemplo, no caso de

filmes *Polaroid*, usados em óculos de sol ou películas automotivas para reduzir a luminosidade.

Ao se colocar um material desse tipo (designados como filtros de polarização) no caminho de um pulso de luz não polarizado (cujos fótons constituintes estejam polarizados em direções completamente aleatórias), apenas fótons cuja direção de polarização seja a mesma do eixo óptico atravessarão o material.

Assim, montando-se um desses filtros no caminho de um pulso de luz, de tal forma que possa ser girado livremente (mantendo-se o seu eixo óptico perpendicular à direção de propagação do pulso), pode-se obter um "canhão de fótons" (figura 3.1), um dispositivo capaz de emitir pulsos de luz completamente polarizados em uma direção escolhida (girando-se o filtro no ângulo correspondente à direção desejada).

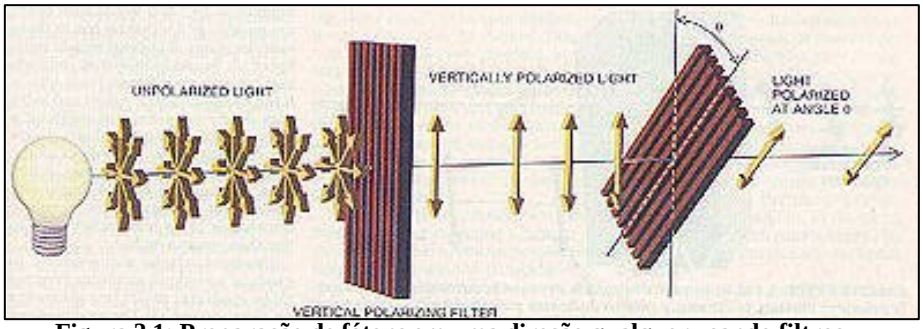

Figura 3.1: Preparação de fótons em uma direção qualquer usando filtros.

Fonte: (BENNET, 1992).

3.9.2) Medidas de polarização

Existe na natureza um material cristalino transparente chamado **calcita** que tem a seguinte propriedade: ele divide um feixe de luz em dois de acordo

com a polarização dos fótons componentes (HERBERT, 1985). Um cristal de calcita possui uma direção especial chamada de eixo óptico. Se um fóton incidente estiver polarizado na mesma direção que o eixo óptico do cristal ele será desviado em uma direção (que, nesse texto, será convencionada como sendo a esquerda) e, se estiver polarizado na direção perpendicular ao eixo, ele será desviado em outra direção (nesse texto, por convenção, a direita).

Na figura 3.2 está representado um cristal de calcita, juntamente com os detectores. A figura foi retirada de (HERBERT, 1985) e usa uma convenção ligeiramente diferente da adotada aqui, com os detectores sendo posicionados acima e abaixo do cristal e não à esquerda e direita, conforme convencionado nesse texto.

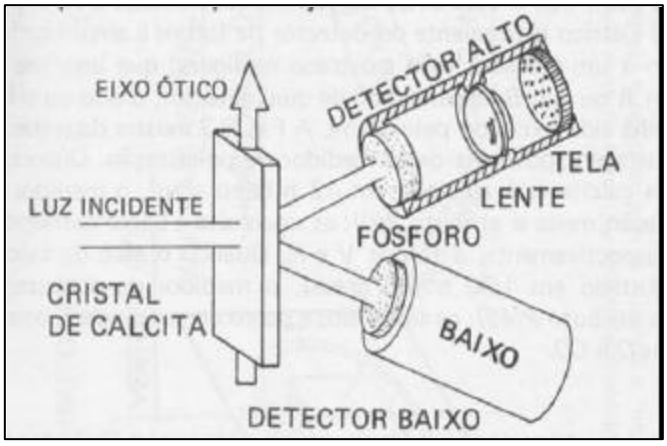

Figura 3.2: Esquema de um medidor de polarização.
Fonte: (HERBERT, 1985).

Como a teoria quântica diz que, escolhida uma direção de medida, um fóton estará polarizado ou naquela direção ou então na direção perpendicular, o cristal de calcita separa os fótons incidentes de acordo com a polarização.

E assim, qualquer que seja a direção escolhida para apontar o eixo óptico do cristal (qualquer que seja a direção de medida), cada fóton que atingi-lo será desviado para a esquerda ou para a direita.

3.9.3) Bases de medida para polarização

Ao escolher como posicionar o seu medidor de polarização, o experimentador estará definindo dois vetores unitários $\boldsymbol{e_1}$ e $\boldsymbol{e_2}$, ortogonais entre si, com um deles definindo o eixo *y* (paralelo ao eixo óptico do cristal) e o outro definindo o eixo *x* (ortogonal ao eixo óptico) e ambos em um plano perpendicular à direção de propagação do fóton. Isso se chama definir uma base para a medida

Os dois vetores definem um sistema de coordenadas para a realização de medidas de polarização, se for convencionado que o vetor $\boldsymbol{e_1}$ define a direção vertical $\boldsymbol{e_2}$ define a direção horizontal, diz-se que o medidor está posicionado no modo Vertical-Horizontal (V-H).

Ao se realizar uma medida com o medidor orientado no modo V-H, será medida a polarização de um fóton de tal forma que ele passará pelo medidor e será desviado para a esquerda (indicando que está polarizado segundo a direção vertical) ou então será desviado para a direita (indicando que está polarizado segundo a direção horizontal).

Também podem ser definidos dois vetores $\boldsymbol{h_1}$ e $\boldsymbol{h_2}$, ortogonais entre si, tais que estes estejam no mesmo plano que $\boldsymbol{e_1}$ e $\boldsymbol{e_2}$ e que o ângulo (medido na direção contrária à dos ponteiros do relógio) entre $\boldsymbol{e_2}$ e $\boldsymbol{h_1}$ seja de 45 graus e o ângulo entre $\boldsymbol{e_2}$ e $\boldsymbol{h_2}$ seja de 135 graus ($\boldsymbol{h_1}$ e $\boldsymbol{h_2}$ definirão um sistema de coordenadas cujos eixos estarão definindo as diagonais no plano em que será medida a polarização). Um medidor assim polarizado será designado como Diagonal-Contradiagonal (D-CD). O posicionamento relativo das duas bases (V-

H e D-CD) está indicado na figura 3.3.

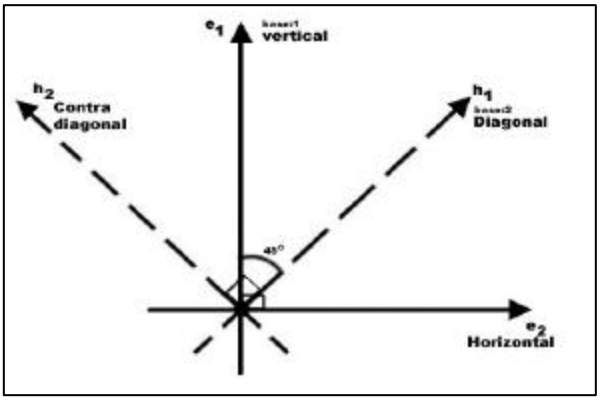

Figura 3.3: Bases conjugadas (V-H e D-CD) para medida de polarização.

Nesse caso, a teoria quântica diz que os atributos definidos por estes dois sistemas de coordenadas (V-H e D-CD) são conjugados entre si.

3.10) Uso de probabilidades na Física Clássica

No contexto da física clássica o uso de probabilidade é feito quando não se conhece todos os detalhes relevantes para descrever uma interação.

Assim, é muito comum o uso de estatística quando se trata de problemas envolvendo muitas partículas (fluidos, gases e plasmas) nos quais, devido à quantidade elevada de elementos em interação, não é possível se computar exatamente a posição exata e o momento de cada partícula envolvida.

Outra aplicação do uso de estatística é o caso em que se analisa o movimento de corpos (e não partículas ideais) em condições reais nas quais os

eventos envolvem interações entre os corpos em estudo e o meio ambiente (sistemas abertos com atrito, deformação, dissipação de energia, etc.).

Em ambos os casos, o uso de estatística se dá devido a questões práticas e não de princípio.

Quando se trata de tantas partículas ou de sistemas em interação com o ambiente como no caso do estudo de gases, não é possível, na prática, computar as posições e momentos iniciais de cada partícula e, nem isso é necessário, uma vez que o conhecimento dos valores médios das variáveis relevantes permite, através do uso de estatística, determinar a evolução do sistema como um todo. Do mesmo modo, quando se trata de sistemas em interação com o ambiente, o uso de valores médios e de aproximações permite que se possa estudar o comportamento do sistema, mesmo sem um conhecimento exato de todas as variáveis envolvidas.

No caso clássico, considera-se que cada uma das variáveis envolvidas possua valores bem definidos. Embora não se conheça o valor exato de cada variável e sejam usadas várias aproximações, trata-se apenas de uma questão prática e não de princípio. Mesmo que o observador não conheça todos os valores, ele poderia, em princípio, realizar todas as medidas exatas, caso possuísse aparelhagem de precisão adequada e tempo o bastante para realizar todas as medidas.

Sendo a física clássica determinística, o conhecimento dos valores exatos de cada variável local relevante permitiria que um observador calculasse com precisão absoluta (caso possuísse poder computacional o bastante) todo o comportamento do sistema em análise.

Para a física clássica, apenas as variáveis locais (aquelas cujos valores são considerados intrínsecos aos objetos envolvidos na interação ou ao ambiente imediatamente próximo) são consideradas relevantes para o estudo de um certo evento.

O não-conhecimento dos valores exatos de todas as variáveis que governam o comportamento de um sistema é conhecido como ignorância clássica.

No entanto, em se tratando de interações elementares, no limite de trocas de energia muito pequenas entre partículas elementares, a física clássica falha, levando a resultados em conflito com a observação e é necessário usar a Teoria Quântica.

3.11) Uso de probabilidades na Teoria Quântica.

O uso de estatística na Teoria Quântica é uma questão de princípio. Nos fenômenos em que é necessário o uso de Teoria Quântica, não se pode conhecer os valores exatos de todas a variáveis necessárias, pelo fato de que essas variáveis simplesmente **não têm valor definido** antes da ocorrência de uma interação ou da realização de uma medida (que é um caso especial de interação entre as partículas e os instrumentos de medida).

No caso de eventos quânticos, não é possível se conhecer os valores das variáveis antes de um certo evento, pois, em princípio, considera-se que estes valores simplesmente não existam de maneira independente e objetiva antes que ocorra alguma interação. Para a Teoria Quântica, antes de uma observação, tudo o que existe são as probabilidades para os valores das variáveis. O status tão privilegiado das probabilidades faz com que o desconhecimento dos valores exatos de cada variável seja de um tipo especial, denominado de "ignorância quântica".

No caso da ignorância clássica, não se conhece os valores de cada variável (não há como se medir cada valor individual por uma questão operacional), mas considera-se que estes valores existam independente de serem observados ou não. Cada variável, para cada partícula, tem um valor definido a

qualquer momento.

Já no caso da ignorância quântica, não se conhece os valores de cada variável porque não há nada para se conhecer. Os valores simplesmente não existem antes da realização de uma medida.

3.12) Correlacionamento de fases e estados geminados

Em certas situações experimentais, duas ou mais partículas podem emergir de uma interação de tal modo que as suas funções de onda fiquem de tal forma embaralhadas devido à mútua interferência (princípio da superposição), que seja mais adequado descrever o sistema como um todo através de uma única função de onda ao invés de uma função de onda para cada partícula.

Esse embaralhamento de fases pode ser interpretado como uma correlação forte entre os estados das partículas envolvidas.

Após o evento, as funções de onda (que determinam o comportamento dos atributos dinâmicos das partículas) interferem de tal maneira que o comportamento subseqüente das partículas fica, para todos os efeitos, completamente entrelaçado, passando a haver uma interdependência nos seus comportamentos em qualquer situação de medida.

Partículas nessa situação são ditas correlacionadas e, uma vez que os estados possíveis de cada partícula são interdependentes, os estados (e os correspondentes valores dos atributos dinâmicos) são ditos geminados.

3.13) O experimento EPR e a validade da Teoria Quântica.

Em um artigo publicado em conjunto com Boris Podolsky e Nathan Rosen em 1935 (EINSTEIN, 1935), Albert Einstein descreveu um experimento mental analisando o comportamento de partículas correlacionadas (em estado

geminado), conhecido como experimento EPR, de acordo com as iniciais dos autores, em que visava demonstrar que o papel especial da probabilidade na mecânica quântica seria uma questão de inadequação da teoria e que qualquer evento poderia ser entendido em termos de variáveis locais.

Para os autores, o uso de probabilidades na mecânica quântica não se devia a questões de princípio. O argumento por trás do experimento EPR, levado às últimas conseqüências, demonstraria que a teoria quântica é fundamentalmente incompleta, não considerando todas as variáveis relevantes.

O uso de probabilidades nos eventos quânticos seria apenas uma conseqüência da falta de conhecimento do observador sobre todas as variáveis realmente importantes para a análise dos eventos.

O argumento original dos autores foi formulado de modo bastante genérico e pode ser melhor compreendido em termos de um exemplo prático.

3.13.1) O argumento EPR para partículas com massa

O primeiro exemplo consiste em uma partícula com *spin* total igual a zero e que decai em duas partículas.

Trata-se de um evento quântico típico, no qual uma partícula espontaneamente se decompõe em duas outras, que passam a ter suas funções de onda correlacionadas.

Tais eventos são completamente probabilísticos e, dado um conjunto de partículas do mesmo tipo, não se pode dizer, a partir da teoria, qual delas vai decair nem quando.

Tudo o que a teoria permite dizer é que, dado um certo tempo, uma fração das partículas terá decaído de uma certa maneira e não de uma outra possível.

Qualquer modalidade de decaimento, que respeite certas leis básicas, pode ocorrer com uma determinada probabilidade dada pela teoria. Desde que algumas leis de conservação sejam respeitadas, a partícula original pode decair de várias maneiras diferentes.

3.13.2) Leis de Conservação

Algumas leis de conservação são, por exemplo, a lei de conservação da energia, a lei da conservação da carga elétrica, a lei da conservação do momento linear e a lei da conservação do momento angular.

Assim, por exemplo, seja uma partícula neutra (carga elétrica igual a zero) inicialmente em repouso e com *spin* (momento angular) igual a zero e que decai em duas partículas menores, um elétron (carga –e) e um anti-elétron (carga +e). As leis de conservação exigem que haja:

a) Conservação da carga:

Se a carga inicial era igual a zero, a soma das cargas das duas partículas resultantes deve permanecer igual a zero. Realmente, as duas partículas consideradas têm cargas que se anulam quando somadas;

b) Conservação da energia total:

Como a energia deve ser conservada, a energia total do sistema antes e depois do decaimento deve ser a mesma. Se a partícula original possuía massa *M* e estava em repouso (não possuía energia cinética) a energia total do sistema antes do decaimento é:

$$E_0 = M \times c^2$$

Onde, *c* é a velocidade da luz no vácuo.

As massas das duas partículas devem ser tais que, quando convertidas em energia e somadas obtenha-se:

$$E = m_1 \times c^2 + k_1 + m_2 \times c^2 + k_2$$

Sendo k_1 e k_2 as energias cinéticas das partículas após o decaimento.

Pela lei da conservação da energia deve ser:

$$E = E_0$$

c) Conservação do momento linear (*momentum*):

O *momentum* deve ser conservado. Como as partículas resultantes do decaimento têm a mesma massa e a partícula original estava em repouso (tinha momento inicial igual a zero), para que o *momentum* (que é um vetor) se conserve, deve ser:

$$\mathbf{p}_1 = m\mathbf{v}\,\hat{\imath} \text{ e } \mathbf{p}_2 = -\,m\mathbf{v}\,\hat{\imath}$$

Onde $\hat{\imath}$ representa um vetor unitário, definindo uma direção no espaço, de forma que a soma dos vetores $\mathbf{p}_1$ e $\mathbf{p}_2$ seja igual a zero.

d) Conservação do momento angular (*spin*):

Supondo partículas girando em torno de um mesmo eixo, convenciona-se que o vetor momento angular apontará no sentido positivo se a partícula gira

no sentido anti-horário e apontará no sentido negativo se a partícula gira no sentido horário.

Uma vez que a partícula original possuía *spin* (momento angular) nulo, a soma dos *spin*s das partículas resultantes também deve ser nula (soma vetorial, pois o momento angular é um vetor).

Para um elétron e um anti-elétron, o módulo do *spin* é um atributo estático, mas a direção do *spin* é um atributo dinâmico.

Em se tratando de um atributo dinâmico, o que a teoria quântica diz é que, uma vez escolhido um eixo para realizar a medição, o *spin* do elétron (e do anti-elétron) terá a direção do eixo e apontará na direção positiva ou negativa com uma probabilidade de 50% para cada uma delas.

3.13.3) O experimento EPR

Trata-se de uma típica medida quântica. Antes da medida, a partícula não possui um *spin* com direção ou sentido definidos. Tudo que se pode dizer é que, se for realizada uma medida escolhendo-se um determinado eixo, o momento angular (*spin*) estará na direção do eixo escolhido com iguais probabilidades de apontar no sentido negativo ou positivo.

O argumento EPR pode ser apreciado através de considerações sobre o *spin* das partículas resultantes do decaimento. Esse é justamente o tipo de evento no qual as partículas ficam em estados geminados, ou com as suas funções de onda correlacionadas.

Sabe-se que após o decaimento, as partículas resultantes devem possuir *spin* total nulo. Como o *spin* de ambas tem o mesmo módulo, eles devem apontar em sentidos opostos para qualquer eixo escolhido, pois a soma (vetorial) dos *spin*s individuais deve ser nula. Diz-se que estas partículas estão em um estado geminado.

Ora, a teoria diz que direção e sentido do *spin* de uma partícula individual, sendo atributos dinâmicos, não existem, de modo objetivo, antes que seja realizada uma medida e que tudo que se pode conhecer sobre o sentido do *spin* de um elétron é que, uma vez fixado um eixo para medição, ele apontará no sentido positivo ou no sentido negativo com 50% de chance para cada possibilidade.

Como as duas partículas estão em estado geminado, o que a teoria quântica diz é que, devido ao correlacionamento de fases, os atributos dinâmicos de cada partícula estão geminados.

A indeterminação quântica continua valendo, não se conhece o valor do *spin* de nenhuma das duas partículas antes da realização de uma medida efetiva.

No entanto, caso o *spin* de uma das partículas seja medido em uma determinada direção (por exemplo, na vertical), e se encontre que ele aponta no sentido positivo (para cima) então, quando for realizada uma medida subseqüente da outra partícula, se for escolhida a mesma direção, o *spin* necessariamente apontará para baixo.

Se uma partícula decai como no exemplo acima, as partículas resultantes se movem em sentidos opostos (conservação do momento linear) e, embora não seja possível dizer, sem realizar a medida, se o *spin* de uma delas aponta no sentido positivo ou negativo, sabe-se que eles devem apontar em sentidos opostos para qualquer eixo escolhido.

Na situação em que a partícula *A* se move para a direita e a partícula *B* se move para a esquerda, um observador pode realizar a medida do sentido do *spin* de *A* fixando seu aparelho de medida M_1 a uma distância d_1 (à direita do local do decaimento e fixado na direção vertical).

Um outro observador pode realizar uma medida do *spin* de *B*, fixando seu aparelho M_2 a uma distância d_2 ($d_2 > d_1$), à esquerda do local de decaimento e também posicionado na vertical.

3.13.4) O paradoxo EPR

O paradoxo EPR aparece no momento da realização da medida de *A*. Caso seja realizada uma medida na direção vertical, e seja verificado que o *spin* de *A* aponta para cima, o *spin* da partícula B que ainda não foi medido (pois $d_2 > d_1$) passará a ter um valor definido na direção vertical mesmo sem ter sido medido, pois, pela conservação do momento angular, ele necessariamente deverá apontar para baixo se medido na direção vertical.

Para toda as outras direções possíveis, a indeterminação quântica continuaria mantida. Caso fosse realizada uma medida da partícula *B* em um ângulo qualquer, diferente da vertical, não se poderia dizer qual seria o resultado obtido pelo medidor, exceto com uma probabilidade de 50%.

3.13.5) A conclusão de Einstein

Einstein fez, basicamente 3 suposições:

1) Supôs que os observadores, com seus aparelhos de medida M_1 e M_2 estivessem tão longe que não pudessem trocar informação entre si em tempo hábil a não ser se comunicando por alguma via mais rápida do que a luz;

2) A decisão de um deles de posicionar o respectivo aparelho de medida fosse completamente independente da decisão do outro;

3) A medida realizada no aparelho M_1 não poderia interferir na decisão do posicionamento do medidor M_2.

As suposições acima são compatíveis com a Teoria da Relatividade e são chamadas, em conjunto, de **pressuposição de localidade**.

Aceitando a pressuposição de localidade acima, Einstein concluiu que a partícula B deveria, necessariamente, possuir algum mecanismo interno (algum atributo estático) que, embora desconhecido (ignorância clássica), definisse todos os possíveis resultados antes da realização da medida por M_2.

Partindo dessa conclusão, os autores afirmam que a descrição que a Teoria Quântica fornece da realidade não pode estar completa, pois deixaria de levar em conta alguns mecanismos internos e substituiria essa falta de conhecimento pelo uso de probabilidades.

Para Einstein, o uso de probabilidades na teoria seria apenas uma questão de ignorância clássica, os valores dos atributos dinâmicos estariam previamente determinados antes da medida ser realizada e seriam apenas desconhecidos (no sentido clássico) e não indeterminados por uma questão de princípio, como afirma a teoria quântica.

É importante notar que o desacordo de Einstein não se referia à concordância da teoria com os resultados experimentais e sim à capacidade da teoria de fornecer uma descrição completa da realidade.

Na concepção de Einstein, uma teoria física deveria explicar não apenas o resultado de medidas, mas também deveria descrever o mecanismo que controla a ocorrência dos eventos e explicar o que ocorre entre as medidas. Para ele, a teoria forneceria resultados corretos e, no entanto, seria incompleta por não fornecer uma descrição dos eventos antes da medição.

3.14) Teoria Quântica e criptografia

O Princípio da Incerteza de Heisenberg se constitui no principal elemento da Teoria Quântica utilizado em protocolos de criptografia. Além dele, conforme será visto nos Capítulos 4 e 5, um conhecimento sobre os fótons e seu atributo polarização é absolutamente essencial para o entendimento desses protocolos.

Embora o experimento EPR tenha sido proposto com o objetivo de investigar os fundamentos da Teoria Quântica e, aparentemente, tenha mais conseqüências filosóficas do que práticas, o uso de fótons EPR e da correlação forte do atributo polarização será fundamental para o funcionamento do Protocolo de Ekert, apresentado no Capítulo 5.

Capítulo 4 – O protocolo BB84 de criptografia quântica

Os protocolos de criptografia baseados em propriedades quânticas procuram resolver o problema de distribuição de chaves garantindo um canal perfeitamente seguro.

A parte quântica propriamente dita de um protocolo quântico qualquer ocorre na primeira fase de distribuição das chaves. O restante do procedimento pode ser realizado classicamente, usando um canal clássico comum.

Baseando-se no PIH, procura-se obter uma forma de transferir a informação sobre as chaves de tal modo que, mesmo que um eventual espião tenha acesso ao canal de comunicação, ele não possa obter uma cópia do que é transmitido sem, ao mesmo tempo, denunciar a sua presença e/ou a violação.

Nos protocolos de criptografia convencionais, pode-se usar a teoria da comunicação de Shannon (VOLOVICH, 2001) e (BENNET, 1991) para demonstrar que um canal qualquer sempre pode ser monitorado passivamente e se pode fazer cópias da informação transmitida sem alterá-la.

Por outro lado, se a informação for codificada através de entidades quânticas elementares, tais como fótons, pode-se conseguir um canal de comunicação tal que, em princípio, as transmissões não possam ser lidas ou copiadas por um observador não autorizado.

Para isso, tais protocolos baseiam-se no uso de atributos conjugados e isso garante, pelo PIH, que a mensuração de um dos atributos torna os valores do seu atributo conjugado completamente aleatórios.

Para qualquer par de atributos conjugados escolhidos, a teoria quântica garante que, se for efetuada uma medida de um deles o outro será tornado aleatório. Isso é usado nos protocolos quânticos especificamente para a distribuição de chaves para que, se a informação for lida no caminho entre o emissor e o destinatário, a mensagem recebida pelo destinatário seja alterada

aleatoriamente de tal modo que o destinatário e o emissor possam perceber, com segurança, que houve alguma leitura não autorizada, possam descartar a mensagem como corrompida e reiniciar o protocolo desde o início até que seja possível estabelecer chaves reconhecidamente seguras.

Para o estabelecimento de um protocolo quântico, as informações são codificadas na polarização de fótons e usa-se o Princípio da Incerteza de Heisenberg (PIH) para garantir a segurança.

Assim, inicialmente será apresentada uma reformulação do PIH em termos de fótons e medidas de polarização e, em seguida, uma descrição do primeiro protocolo quântico implementado na prática (BB84) com uma descrição dos seu funcionamento.

4.1) O PIH aplicado a medidas de polarização

No caso de fótons, em termos de medidas de polarização e medidores, o PIH pode ser enunciado assim:

1) Se o fóton passar por um medidor de polarização, constituído de um cristal bi-refringente como a calcita, ele será desviado para a esquerda ou para a direita;

2) Se já estava polarizado na direção do eixo óptico do medidor ou na direção perpendicular, continuará polarizado como antes;

3) As bases de medida Vertical-Horizontal (*V-H*) e Diagonal-Contradiagonal (*D-CD*), são bases conjugadas;

4) Se o fóton já estava polarizado na direção diagonal ou contra-diagonal relativamente ao eixo óptico, é desviado aleatoriamente para a esquerda (e passa a estar polarizado na direção do eixo) ou para a direita (e passa a estar polarizado na direção perpendicular ao eixo).

5) **Toda a informação sobre a polarização anterior é perdida irreversivelmente.**

Esquematicamente, os resultados possíveis para medidas nas bases *V-H* e *D-CD*, estão sumarizados na tabela 4.1.

Fóton antes	Detector	Fóton depois	Desvio
V	V-H	V	Esq.
V	D-CD	D ou CD	Esq. ou Dir.
H	V-H	H	Dir.
H	D-CD	D ou CD	Esq. ou Dir.
D	V-H	V ou H	Esq. ou Dir.
D	D-CD	D	Esq.
CD	V-H	V ou H	Esq. ou Dir.
CD	D-CD	CD	Dir.

Tabela 4.1: Medidas nas bases *V-H* e *D-CD*, de acordo com o PIH.

4.2) Protocolo BB84

Sejam um emissor A, um destinatário B e um espião E, posicionados conforme a figura 4.1.

Para as transmissões no canal quântico, serão utilizados fótons (ou seja, sinais luminosos) e os atributos conjugados escolhidos serão a polarização medida na base V-H e a polarização medida na base D-CD.

Na prática, *A* disporá de um dispositivo capaz de emitir fótons polarizados em uma das 4 direções definidas como V, H, D e CD. *B* disporá de medidor de polarização (um cristal de calcita) cujo eixo poderá ser alinhado no

modo V-H ou D-CD.

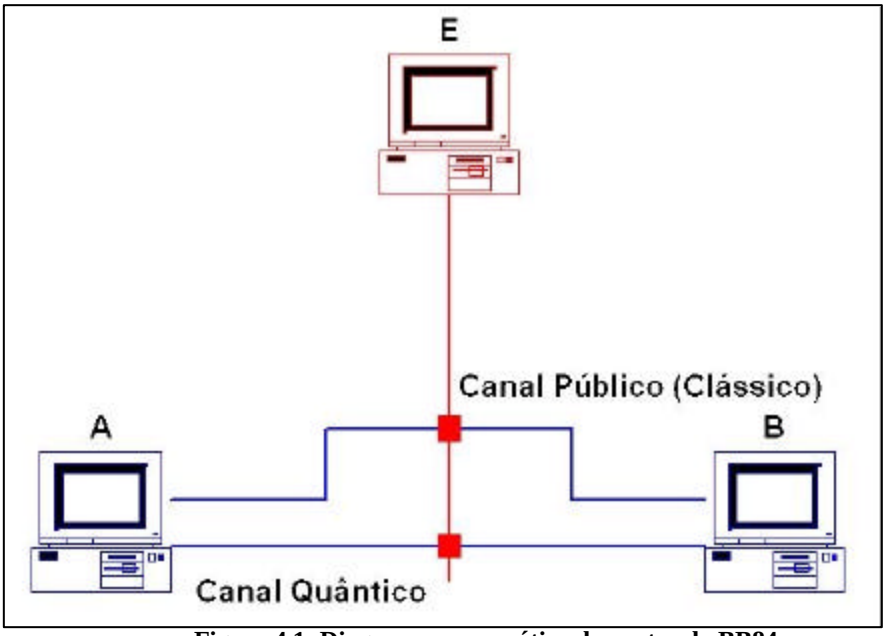

Figura 4.1: Diagrama esquemático do protocolo BB84.

Conforme discutido anteriormente, se o medidor estiver alinhado no modo V-H, um fóton incidente preparado por *A*, com polarização na direção vertical, será certamente desviado para a esquerda e um fóton incidente polarizado na direção horizontal será desviado certamente para a direita.

Fótons polarizados nas direções diagonal e contra-diagonal, serão desviados aleatoriamente para a direita ou para a esquerda.

Do mesmo modo, se o eixo do cristal estiver orientado no modo D-CD, fótons que tenham sido emitidos com polarização vertical ou horizontal serão desviados aleatoriamente para a direita ou para a esquerda.

O objetivo da parte quântica do protocolo BB84 é o estabelecimento de

uma chave criptográfica primária entre *A* e *B*. A seqüência de procedimentos para isso pode ser descrita assim:

Passo 1) A envia uma seqüência aleatória de fótons polarizados em uma das 4 direções (V ,H, D, CD);

Passo 2) B mede os fótons que chegam usando uma seqüência aleatória de orientações, ou alinhando o seu cristal na direção vertical, o que corresponde a usar base V-H, ou alinhando o seu cristal na direção diagonal, o que corresponde a usar a base D-CD a cada medida.

Passo 3) B anota os resultados de suas medidas, indicando, em cada uma, a direção de orientação do seu cristal e se o fóton incidente foi desviado para a direita ou para a esquerda;

Passo 4) B transmite para A apenas a seqüência de orientações que usou, mas não os resultados das medidas, usando um canal comum;

Passo 5) A informa a B quais as orientações estavam corretas, isto é, as que coincidem com as direções de polarização enviadas.

Passo 6) A e B consideram que fótons desviados para esquerda correspondem ao bit 1 e fótons desviados para direita correspondem ao bit 0;

Passo 7) A *string* assim obtida será usada como chave criptográfica em um sistema criptográfico clássico simétrico.

4.3) Um exemplo

Considerando uma transmissão de apenas 10 fótons, os resultados possíveis são sumarizados na tabela 4.2.

Número do fóton	Direção do Fóton emitido por A	Orientação do cristal de B	Direção de desvio	Bits
01	V ($\mathbf{e}_1$)	V-H	Esquerda	1
02	D ($\mathbf{h}_1$)	D-CD	Esquerda	1
03	CD ($\mathbf{h}_2$)	D-CD	Direita	0
04	H ($\mathbf{e}_2$)	V-H	Direita	0
05	H ($\mathbf{e}_2$)	V-H	Direita	0
06	CD ($\mathbf{h}_2$)	V-H	Esquerda	?
07	D ($\mathbf{h}_1$)	V-H	Direita	?
08	H ($\mathbf{e}_2$)	D-CD	Esquerda	?
09	V ($\mathbf{e}_1$)	V-H	Esquerda	1
10	CD ($\mathbf{h}_2$)	D-CD	Direita	0

Tabela 4.2: Um exemplo de transmissão quântica para 10 fótons

Seguindo os passos do protocolo, de acordo com a tabela acima, *A* enviou 10 fótons.

Após medir os 10 fótons, *B* informa a *A* que orientou o seu cristal de acordo com as seguintes direções: V-H, D-CD, D-CD, V-H, V-H, V-H, V-H, D-CD, V-H, D-CD.

A informa a *B* que as orientações corretas foram as seguintes: 01 02 03 04 05 09 10.

Note-se que as medidas 06, 07 e 08 produzirão resultados aleatórios e serão descartadas.

B então usa como chave a *string*: 1100010.

A, sabendo a orientação exata dos fótons que enviou na seqüência original, saberá também que a chave é: 1100010.

Note-se que para cada escolha de direção de B, ele tem 50% de chance de escolher corretamente. Isso limita a eficiência desse canal quântico ideal a 50% em média.

4.4) Segurança no BB84

O que garante a segurança do protocolo BB84?

Seja um espião *E*, que pode monitorar o canal de comunicação por onde passam os fótons.

Se *E* ler os fótons que vêm de *A* e depois retransmiti-los para *B*, a não ser que *E* escolha exatamente as direções corretas de polarização que *A* usou, os fótons que *E* enviar para *B* terão sua polarização modificada de acordo com as medidas efetuadas por *E*.

Podem acontecer as situações descritas na tabela 4.3.

Situação	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
A envia	V	V	H	H	D	D	CD	CD
E mede	V-H	D-CD	V-H	D-CD	V-H	D-CD	V-H	D-CD
Desvio	Esq.	?	Dir.	?	?	Esq.	?	Dir.
E reenvia	V	D,V	H	D,V	V,H	D	V,H	CD

Tabela 4.3: Possibilidades de interceptação e reenvio no BB84

Assim, se houver um espião entre *A* e *B* e considerando um grande

número de fótons enviados, pelo menos 50% (metade do total) dos fótons chegará a *B* com polarização diferente da enviada por *A* (pois serão preparados incorretamente por *E*).

Como *B* também poderá errar na sua escolha com uma probabilidade de 50% na ausência de interceptação, a probabilidade combinada de que *B* consiga um resultado correto na ocorrência de interceptação cai em 25%.

Como passo final do protocolo, *A* e *B* podem tomar, por exemplo, os 1.000 primeiros bits (uma amostra razoável) da *string* resultante e compará-los publicamente.

Se houver uma discrepância entre estes bits da ordem de 25% (note-se que deveria ser apenas 0% sem espionagem), então ambos podem concluir que o canal foi violado e a transmissão espionada.

Assim, devido às propriedades quânticas relacionadas com o PIH, se um espião *E* monitorar o canal de transmissão, ele provocará uma alteração nos dados que poderá ser percebida pelos usuários legítimos do canal como um acréscimo de 25% de erros na taxa esperada.

Outro fato relacionado com as propriedades quânticas é que o espião não pode simplesmente fazer uma cópia da mensagem para analisar depois e simplesmente deixar os fótons passarem sem alterá-los.

O teorema da não-clonagem, demonstrado por Wooters e Zurek (VOLOVICH, 2001), garante que não é possível fazer uma cópia perfeita da mensagem de *A* sem alterá-la.

4.5) Correção de erros no protocolo BB84

A transferência de dados entre dois correspondentes *A* e *B* utilizando o protocolo quântico descrito no Capítulo anterior produz, ao final do processo, duas *string*s *S[A]* e *S[B]* que, na ausência de interceptação e de ruído no canal

(introduzido devido a imperfeições físicas, por exemplo), seriam completamente idênticas termo a termo:

$$S[A] = S[B]$$

Entretanto, em qualquer um desses casos, têm-se:

$$S[B] = S[A] \oplus d$$

Onde *d* é uma *string* arbitrária, do mesmo tamanho que *S[A]* e a operação, representada por $\oplus$, trata-se da operação lógica OU EXCLUSIVO entre os bits de *S[A]* e *d*. Desse modo, cada bit igual a 1 em d indica que o bit efetivamente recebido por *B* foi interceptado, alterado devido a algum ruído no canal ou lido incorretamente devido a alguma falha na aparelhagem de medida.

Para efetuar a correção (com grande probabilidade) de todos os erros em *S[B]*, usando um canal público para efetuar a comparação e, no processo, deixar vazar o mínimo de informação para um eventual espião *E*, *A* e *B* devem utilizar um algoritmo clássico (i. e. não-quântico) uma vez que o canal quântico, supondo-o mais caro, lento e sensível a ruído, seria inconveniente tanto devido ao custo quanto ao tempo gasto.

Esse processo de encontrar e corrigir as discrepâncias entre a chave enviada por *A* e a *string* recebida por *B* chama-se de **Reconciliação** na literatura corrente.

Uma vez que o algoritmo de reconciliação tenha sido aplicado, as *string*s resultantes passarão por um procedimento que as tornará menores ao mesmo tempo em que eliminará (com grande probabilidade) qualquer informação que porventura tenha vazado para um suposto espião durante o processo de reconciliação. Esse segundo procedimento é conhecido como **Amplificação de**

Privacidade.

Um procedimento para a realização da reconciliação é esboçado em (BENNET, 1991) e detalhado mais formalmente em (BRASSARD, 1994) e também em (CACHIN, 1995).

Posteriormente, vários esquemas de otimização foram propostos, por exemplo, em (NAKASSIS, 1998) e (BRASSARD, 1994).

A explicação que segue, baseia-se na proposta apresentada em (BENNET, 1991) que, embora menos elaborada, permite apreciar o tipo de operação necessária para a execução dos processos de reconciliação e amplificação de privacidade.

4.5.1) Reconciliação da chave através de discussão pública

Considerando as *string*s obtidas por *A* e *B* após a transmissão quântica, há a possibilidade de que elas ainda difiram entre si em algumas posições, tanto devido à interceptação, quanto devido a várias fontes de ruído possíveis no canal como, por exemplo, impurezas no meio de transmissão, ruído térmico na aparelhagem, baixa confiabilidade dos instrumentos de medida, limitações de precisão na detecção e medida dos fótons, etc.

Para efeitos de reconciliação, qualquer diferença entre as *string*s *S[A]* e *S[B]* será tratada do mesmo modo uma vez que, para os interlocutores *A* e *B*, erros causados por qualquer desses motivos são, em geral, indistinguíveis.

4.5.1.1) Procedimentos para reconciliação

0) *A* e *B* possuem dois parâmetros previamente definidos, o primeiro deles é o número *k* e o segundo é o número *i*.

1) Para iniciar o procedimento de reconciliação, *A* selecionará um bloco de *k* bits de *S[A]*, começando da posição *i* e o enviará, através de um canal público, para B (note-se que o valor de *k* ou é pré-definido ou, de um modo mais geral, define-se previamente que *k* será uma porcentagem do tamanho de *S[A]* após a transmissão quântica);

2) *B*, comparará o bloco recebido com um bloco de tamanho *k* e iniciando da posição *i*, extraído de sua própria *string S[B]* e calculará o valor de *p*, assim definido:

p = (quantidade de bits 1 em d) / (quantidade de bits de d)

Assim, o número *p*, representa a porcentagem de erros na amostra *k*.

3) *A* e *B* descartam os blocos usados na amostra. Assim, a *string*s *S[A]* e *S[B]* ficam reduzidas de *k* bits.

S'[A] e *S'[B]* são as novas *string*s após o descarte do bloco de amostra;

4) Baseando-se no valor de p, os interlocutores *A* e *B* dividem *S'[A]* e *S'[B]* em blocos de tamanho k_0.

O valor de k_0 deve ser relacionado com o valor de *p* de modo que os blocos resultantes contenham, aproximadamente, não mais que um erro.

Inicialmente, conforme proposto em (BENNET, 1991), o melhor valor para k_0 deveria ser determinado empiricamente usando-se o conhecimento sobre as características físicas do canal, precisão dos equipamentos de medida e uma estimativa máxima de erros aceitável.

Um valor sugerido para k_0 de modo a satisfazer aproximadamente (com

uma boa probabilidade) a condição de não mais que um erro por bloco é o seguinte:

$$k_0 = (1/p) + (1 / 4p)$$

5) *A* divide *S'[A]* em blocos de tamanho k_0, computa os bits de paridade de cada bloco e envia estes bits de paridade para *B* usando o canal público;

6) *B* compara a sua seqüência de bits de paridade dos seus próprios blocos com a seqüência enviada por *A*;

Há duas possibilidades:

a) Blocos com o mesmo bit de paridade são considerados (provisoriamente) como corretos.

b) Blocos com bit de paridade diferentes são considerados como incorretos.

Cada um dos blocos incorretos é bisseccionado e verifica-se o bit de paridade de cada sub-bloco. Os sub-blocos que são encontrados como incorretos são sucessivamente bisseccionados até que se consiga um conjunto de sub-blocos com o mesmo bit de paridade e o sub-bloco contendo apenas o bit incorreto seja isolado e possa ser corrigido.

A cada subdivisão de um bloco incorreto, *A* e *B* trocam informações sobre a paridade de cada sub-bloco a ser analisado.

Para que *E*, o espião, não obtenha informação o bastante sobre cada bloco ou sub-bloco, uma vez que os bits de paridade sejam revelados publicamente para a comparação, *A* e *B* descartam o último bit de cada bloco ou sub-bloco, após realizada a comparação.

7) Uma vez que todos os possíveis blocos e sub-blocos sejam considerados corretos nessa primeira rodada, *A* e *B* escolhem um novo valor k_j ($k_j > k_0$), tomam a *string* restante dividindo-a em blocos de tamanho k_j e reiniciam o procedimento de comparação de bit de paridade de cada bloco.

Esse sétimo passo é necessário uma vez que a comparação de bits de paridade pode deixar passar alguns erros (basta que haja um número par de erros em um mesmo bloco para que se tenha blocos com bit de paridade igual e conteúdos diferentes).

8) Todo o procedimento entre 5 e 7 é repetido tantas vezes quantas necessárias, até que A e B se dêem por satisfeitos. Um número de rodadas *w* considerado seguro pode ser obtido usando os seguintes critérios:

a) O tamanho de bloco k_{w+1} para a *(w + 1)–ésima* rodada é dado por:

$K_{W+1} = 2\ k_W$ (a cada rodada dobra-se o tamanho dos blocos).

b) As rodadas são repetidas até que o tamanho do bloco exceda ¼ do total de bits iniciais;

c) Ao menos mais duas rodadas são executadas com blocos de tamanho aproximado de ¼ do total de bits.

4.5.2) Amplificação de privacidade

A amplificação de privacidade é o processo pelo qual dois interlocutores

podem extrair uma chave completamente secreta de uma *string* aleatória compartilhada sobre a qual um eventual espião possui algum conhecimento.

Em geral, ambos os interlocutores não conhecem a extensão do conhecimento do espião sobre o dado compartilhado, exceto pelo fato de que ele é necessariamente limitado.

O processo geral de amplificação de privacidade pode ser descrito assim (BENNET, 1995):

Seja *W* uma variável aleatória tal como uma *string* de *n* bits cujo conhecimento completo é compartilhado por dois interlocutores, *A* e *B*.

Um espião *E* possui uma variável correlacionada *V* que provê *t* bits ($t < n$) de informação sobre *W*.

Um exemplo de tal situação é justamente a *string* compartilhada entre *A* e *B* após o processo de reconciliação, com *E* possuindo conhecimento sobre as paridades dos blocos usados na correção de erros e sobre alguns bits eventualmente interceptados na transmissão quântica.

A e *B* escolherão uma função de compressão g que mapeia uma *string* de *n* bits em uma outra de *r* bits. Simbolicamente:

$$g: \{0,1\}^n \rightarrow \{0,1\}^r$$

Seja *K*, a *string* resultante da aplicação de *g* sobre *W*:

$$K = g(W)$$

A função *g* é escolhida publicamente (através de acordo entre A e B usando o canal clássico).

As funções adequadas para este procedimento são as funções universais

de *hash* (*strongly-universal*$_2$ H_3) discutidas em (WEGMAN, 1981). O uso dessas funções garante que, mesmo que *E* possua um conhecimento parcial da *string W* e saiba qual a função *g* escolhida, o conhecimento de *E* sobre a *string K* possa ser tornado tão pequeno quanto se queira através da escolha adequada de parâmetros por *A* e *B*.

Após o procedimento de reconciliação, pode-se considerar que, de modo geral, o espião *E* possui uma *string V*, que apresenta uma correlação com *W* de tal forma que forneça um conhecimento sobre *t* bits de *W*.

Esse conhecimento pode ser modelado (dependendo do cenário considerado para a transmissão/interceptação), por exemplo, como uma das quatro possibilidades abaixo:

a) *E* possui *t* bits de *W*;

b) E possui *t* bits de paridade resultantes da checagem de *W*;

c) E possui o resultado de uma função arbitrária, mapeando *string*s de *n* bits em *string*s de *t* bits;

d) A *string W* transmitida através de uma canal simétrico binário (a probabilidade de receber 0 tendo sido enviado 1 é a mesma de, tendo sido enviado 0, receber 1), cuja probabilidade de erro e satisfaça:

$$h(e) = 1 - t/n$$

Sendo *t/n* a capacidade do canal e *h* a função de entropia para o canal.

Em (BENNET, 1995) demonstra-se que, para qualquer dos casos acima tem-se que *A* e *B* podem filtrar *r* bits de *W* pela aplicação de *g* em *W* tal que:

$$r = n - t - s$$

Sendo *s* uma constante de valor inteiro que é arbitrariamente escolhida pelos participantes *A* e *B* e com $s < n - t$.

Ou, simbolicamente,

$$g: \{0,1\}^n \rightarrow \{0,1\}^{n-t-s}$$

O que denota a escolha de uma função de compressão *g* que mapeie *string*s de *n* bits em *string*s de *n-t-s* bits.

Demonstra-se que assim pode-se manter o conhecimento de *E* exponencialmente pequeno em função de s e que o único conhecimento que *E* pode obter é o tamanho da *string* resultante, já que a função a ser usada é escolhida através de discussão pública.

Satisfazendo as condições acima, a máxima quantidade de bits que *E* poderia conhecer de *W* é dada por:

$$P(E) = 2^{-s} / \ln 2 \text{ bits.}$$

Assim, com uma escolha adequada da função *g* e do parâmetro *s*, pode-se conseguir uma chave *K* da qual o conhecimento de *E* diminui exponencialmente em *s*, tornando a chave final tão segura quanto se queira com um sacrifício de *t-s* bits da *string* obtida após o processo de reconciliação.

Por isso tal processo é chamado de amplificação de privacidade. Para uma escolha adequada dos parâmetros e da função de *hash*, os interlocutores *A* e *B* podem aumentar a segurança de sua chave tanto quanto queiram com o sacrifício de alguns bits da *string* depurada após a reconciliação.

É interessante notar que, caso as *string*s de *A* e *B* difiram em ao menos

um bit após a reconciliação, as *string*s resultantes da aplicação de *hash* serão completamente não-correlacionadas, o que fornece uma ótima maneira de verificação (*a posteriori*) do sucesso da fase de correção de erros.

4.6) Ataques ao protocolo BB84

Em se tratando especificamente de protocolos de criptografia quântica, de um modo geral, podemos ter ataques visando interceptação de informação tanto na fase de transmissão quântica (distribuição das chaves) como na fase clássica correspondente à verificação e correção de erros (reconciliação e amplificação de privacidade).

Além disso, pelo fato de que a interceptação causa alteração nos dados transmitidos, sempre há a possibilidade de um eventual atacante montar alguma estratégia similar aos tradicionais ataques de negação de serviço (*Denial Of Service* ou *DoS*), bastando, para tanto, simplesmente interceptar toda a transmissão quântica e assim forçar os interlocutores autorizados a descartar sub-repticiamente as *string*s obtidas ao final da fase de transmissão quântica devido ao elevado número de erros introduzido.

4.6.1) Classificação dos ataques na transmissão quântica

Em qualquer ataque durante a fase de transmissão quântica, o espião, em algum momento entre a transmissão efetuada por *A* e a recepção realizada por *B*, terá que interagir o seu próprio sistema quântico (sonda) com a partícula em trânsito.

Após a medida realizada por *E* (interação entre a sonda e partícula), a partícula emerge da interação em um estado entrelaçado (a função de onda do

sistema partícula/sonda é diferente da função de onda original da partícula conforme emitida por *A*) que será efetivamente medido por *B*.

Os ataques durante a fase de transmissão quântica podem ser classificados em:

Ataque individual: Estratégia na qual o atacante mede separadamente cada partícula interceptada;

Ataque coletivo: estratégia em que *E* usa uma sonda distinta para cada partícula (para colher e armazenar) e espera para efetivar as medidas conjuntamente de todas as partículas em um momento posterior, tratando todo o conjunto como um único sistema quântico (uma função de onda para o sistema como um todo) aproveitando-se de informações obtidas durante a fase de correção de erros (clássica) para obter um máximo de informação;

Ataque conjunto: Generalização do ataque coletivo em que o atacante usa apenas um único dispositivo para armazenar todas as partículas, tratando todo o conjunto como um único sistema quântico para efetivar medidas em um momento posterior aproveitando informações obtidas durante a fase de correção de erros.

4.6.2) Implementações dos ataques

No caso dos ataques coletivos, embora se considere, de modo geral, que a criptografia quântica seja, em princípio, segura frente a tais ataques, os especialistas não estão de acordo sobre o fato do conjunto de provas parciais, publicadas na literatura corrente sobre o assunto, apresentar subsídios para uma prova formal definitiva.

A imunidade total da criptografia quântica frente a esses ataques

permanece uma conjectura.

No caso de ataques conjuntos, embora sejam possíveis, em princípio, ainda não há propostas na literatura sobre cenários de implementações possíveis desse tipo de ataque.

4.6.3) Vulnerabilidades exploradas em ataques individuais

Os ataques individuais consistem, basicamente, em realizar uma medida da partícula em trânsito e tentar enviar uma partícula para *B* tentando passar despercebido.

Em um mundo ideal, o teorema da não-clonagem garante que não se pode obter informação sobre o estado da partícula sem perturbar o sistema e, como as perturbações introduzidas podem ser facilmente (estatisticamente falando) verificadas por *A* e *B*, o uso de estados quânticos para transmitir a informação garantiria segurança absoluta.

No caso da transmissão quântica real, vários problemas de ordem prática aparecem. Tais problemas podem criar cenários favoráveis para a montagem de ataques individuais.

1) Uso de fótons individuais:

O primeiro deles refere-se à dificuldade de se transmitir e detectar exatamente um fóton por vez.

Na prática, o que se consegue é emitir pulsos de luz de baixa intensidade (pequeno número de fótons) para cada bit.

Para um pulso de luz coerente, a probabilidade de se detectar n fótons é dada por uma distribuição de Poisson com valor médio *m*, sendo o pulso propriamente dito, considerado como uma superposição de estados quânticos com 0, 1, 2, ... fótons.

Sendo m o número de fótons esperado por pulso, pode-se demonstrar (BENNET, 1991) que, se *m* é pequeno, há uma probabilidade $P = m^2/2$ de que um espião possa dividir o pulso em dois pulsos com um ou mais fótons (por exemplo, usando um espelho semi-prateado posicionado em um ângulo de 45^o com a direção de propagação do pulso), medindo um dos feixes e deixando o outro passar sem interferência.

Assim, a impossibilidade prática de conseguir transmitir e medir um fóton de cada vez faz com que a segurança absoluta, de que a interferência gerada por um espião seria necessariamente detectada, seja perdida.

O máximo que se pode fazer, em termos de tecnologia atual e protocolo BB84, é usar pulsos de luz extremamente fracos (assim, se *E* desviar parte do pulso, diminuirá o brilho do pulso transmitido para *B* abaixo do nível de detecção dos aparelhos do mesmo).

2) propriedades físicas do canal:

O segundo problema de ordem prática refere-se ao fato de as próprias qualidades físicas do canal podem introduzir erros na transmissão.

Assim, impurezas na fibra ótica ou mesmo pequenas flutuações nas suas propriedades óticas podem causar alterações no estado dos fótons em trânsito, inclusive absorvendo alguns deles e impedindo a detecção por *B*.

Para utilização de um determinado canal é importante conhecer previamente uma estimativa de erros deste canal o que, na prática, deve ser medido experimentalmente.

Intimamente relacionado com isso está a precisão dos detectores usados por *B* e dos polarizadores usados por *A* para preparar os fótons a serem enviados. As taxas de erro destes instrumentos, combinadas com a qualidade da fibra, gerarão uma quantidade de erros que pode ser confundida com interceptação

pelos usuários do canal.

Outro problema, intimamente relacionado a esse, diz respeito ao comprimento máximo da fibra usada. Usando feixes suficientemente fracos, a atenuação da fibra se torna um limitante em termos de distância e, claro, a detecção e ampliação do sinal fatalmente mudaria o estado dos fótons, inviabilizando a transmissão quântica.

3) Confiabilidade do canal:

Quanto aos ataques propriamente ditos, dentre as várias estratégias disponíveis para um espião, além da divisão do pulso de luz em mais de um feixe, já discutida, deve-se garantir o uso de uma canal de transmissão confiável (unjammable channel) ou seja, um canal no qual um espião não possa enviar e/ou alterar dados sem ser detectado.

Caso contrário, é fácil ver que o espião poderia simplesmente interromper o canal fisicamente, posicionar seus equipamentos em algum ponto do caminho entre *A* e *B*, e se fazer passar por *A*, enviando fótons para *B* e, ao mesmo tempo, se fazer passar por *B* recebendo os fótons de *A*.

O resultado seria que *E* passaria a ter uma *string* em comum com *A* e outra em comum com *B* e assim poderia interceptar (e ler !) todas as mensagens entre A e B, inclusive falsificando e alterando mensagens.

Na impossibilidade de prover um canal seguro, *A* e *B* devem possuir alguma informação secreta inicial em comum (uma chave de autenticação primária) para poderem se reconhecer mutuamente antes de iniciar a transmissão quântica.

Para todas as futuras transmissões após a primeira, *A* e *B* devem, nesse caso, manter sempre uma parte da *string* final resultante dos processos de transmissão quântica, reconciliação e amplificação de privacidade (que só será

conhecida por *A* e *B*). Desse modo, além de sacrificar alguns bits da *string* resultante do processo de reconciliação e amplificação, alguns bits ainda deveriam ser guardados (i.e. não utilizados imediatamente) para servirem como chave de autenticação para a próxima sessão de transmissão.

É interessante notar que o mecanismo de ataque acima descrito (posicionar um transmissor/receptor executando BB84 entre *A* e *B*) poderia, em princípio, ser usado para se construir estações repetidoras entre *A* e *B* que seriam seguras desde que efetivamente monitoradas e controladas pelos proprietários legítimos do canal, aumentando indefinidamente as distâncias de transmissão.

4) Escolha não-aleatória nas medidas de polarização pelo receptor:

No BB84, *B* deve escolher aleatoriamente o posicionamento do seu medidor para cada fóton.

Verifica-se que, caso *B* não faça suas escolhas aleatoriamente e, ao invés disso, siga um padrão nas suas escolhas, um espião *E* poderá detectar qualquer regularidade na seqüência de escolhas e se aproveitar desse conhecimento ou nas próximas comunicações entre *A* e *B*, ou então usando este conhecimento para detectar os próximos fótons da transmissão em curso.

Isso pode ser especialmente útil para o espião no caso em que ele consiga, por exemplo, dividir os pulsos de luz em dois feixes conforme descrito no item 1 acima.

De posse da capacidade de estimar o padrão de medidas a ser selecionado por *B*, conseguindo dividir os pulsos em mais de um feixe e acompanhando a discussão pública para reconciliação e amplificação de privacidade, o espião poderia, com grande probabilidade, obter uma *string* final exatamente igual a de *A* e *B*.

Uma maneira de se evitar esse problema seria controlar os medidores

usando um software que gerasse uma seqüência aleatória (e não apenas pseudo-aleatória) de orientações dos medidores, alternando entre direção vertical e diagonal aleatoriamente.

Uma maneira de produzir seqüências realmente aleatórias de medidas seria usar, por exemplo, uma seqüência que seguisse o padrão de alguma medida quântica efetivamente realizada em laboratório.

Uma possibilidade, seria acompanhar o decaimento de alguma substância radioativa com um contador *Geiger* e transformar a conseqüente seqüência de *bips* em uma *string* onde um *bip* corresponderia ao valor 1 e a ausência de *bip* ao valor zero. Várias *string*s desse tipo poderiam ser previamente preparadas em laboratório e fornecidas a *A* e *B* de modo que pudessem usá-las quando necessário (sempre que uma comunicação fosse iniciada) em um algoritmo de controle dos medidores.

Obviamente, o uso repetido da mesma seqüência incorreria no mesmo problema.

As garantias de segurança que a distribuição de chaves usando criptografia quântica podem fornecer baseiam-se, principalmente, na aleatoriedade das escolhas dos participantes, tanto para polarizar os fótons enviados, quanto na escolha das bases de realização das medidas e na irreverssibilidade das medidas quânticas.

Caso um dos dois fatores esteja ausente, introduz-se vulnerabilidades que podem ser facilmente exploradas a partir do conhecimento dos protocolos e, nesse caso, a força do método pode se tornar sua maior fraqueza.

5) Preparação não aleatória dos fótons enviados por *A*:

Diretamente relacionado com o problema discutido acima, caso *A* siga um padrão não-aleatório na preparação dos fótons, se um espião posicionado

entre *A* e *B* descobrir este padrão, ele poderia, a partir da discussão pública, quando *B* informasse quais as bases usadas nas suas medidas, conhecer exatamente em quais medidas haveria concordância entre *A* e *B*. Assim, poderia terminar com uma *string* igual à *string* de *A* e *B* (com grande probabilidade) e sem a necessidade de interceptar a transmissão quântica (exceto para descobrir o padrão).

Para usar uma seqüência realmente aleatória, pode-se implementar uma solução análoga àquela descrita no item acima. Usar uma seqüência aleatória de bits conseguida através da observação de algum evento quântico de caráter naturalmente aleatório para estabelecer um controle automático dos polarizadores.

Novamente, cabe lembrar que cada seqüência só deveria ser usada uma única vez.

Capítulo 5 - O protocolo de Ekert de criptografia quântica

Ekert (EKERT, 1991) idealizou um protocolo que, supostamente, eliminaria algumas das deficiências do protocolo BB84 e introduz, ao mesmo tempo, uma série de inovações em segurança.

O protocolo de Ekert usa, de maneira bastante inovadora, fótons em estados correlacionados (fótons EPR) para a distribuição de chaves na fase de comunicação quântica.

A verificação de uma eventual espionagem e interceptação na fase de comunicação quântica é feita através da verificação estatística da violação esperada na desigualdade de Bell para o arranjo envolvendo uma fonte de fótons EPR e os participantes da comunicação, *A* e *B*.

Assim, de modo inesperado, a análise de correlações de fase no experimento EPR, originalmente proposta por Einstein para questionar os fundamentos da Teoria Quântica, acabou encontrando uma aplicação prática na construção de protocolos de criptografia.

Para a compreensão do funcionamento do protocolo, são pré-requisitos uma análise do experimento EPR com fótons e o entendimento do Teorema de Bell. Tais noções serão apresentadas nas seções seguintes, antes da descrição do protocolo propriamente dito.

5.1) O argumento EPR para fótons

Um exemplo de aplicação do argumento EPR é um sistema de dois fótons cujas propriedades estejam correlacionadas (sejam interdependentes).

Um sistema assim pode ser conseguido através de um átomo excitado (estado de energia alto) que decaia para um estado de energia mais baixo

emitindo dois fótons em sentidos opostos (perdendo a energia excedente na forma de luz).

Novamente trata-se de um evento puramente quântico.

Tudo o que a teoria diz é que, dado um conjunto de átomos em estado excitado, depois de um dado tempo, uma porcentagem deles voltará ao estado fundamental (mais baixa energia), mas não permite dizer quais nem quando exatamente isso ocorrerá.

A teoria também diz que os fótons emitidos terão suas funções de onda embaralhadas de tal forma que seus atributos dinâmicos serão exatamente iguais (exceto o sentido do movimento, já que se moverão em sentidos contrários, de acordo com as leis de conservação).

Assim, duas partículas geminadas possuem uma correlação nas suas funções de onda de tal forma que é sabido, de antemão, que os valores de seus atributos dinâmicos, quando medidos nas mesmas condições, serão sempre iguais.

Novamente, um observador pode escolher realizar a medida de um atributo dinâmico (por exemplo, a polarização) dos dois fótons posicionando seus aparelhos de medida à direita, a uma distância d_1 e à esquerda a uma distância d_2 ($d_2 > d_1$).

Conforme a teoria quântica, os fótons, antes da medição, não possuem uma polarização definida e, também de acordo com a teoria, os valores dos atributos dinâmicos de ambos estão correlacionados. Isso quer dizer, nesse caso, que se o observador realizar uma medida da direção de polarização do fóton *A*, a medida da direção de polarização do fóton *B* será a mesma se for escolhida a mesma direção para o eixo óptico do aparelho de medida.

Caso o observador posicione o eixo do medidor M_1, posicionado em d_1, na direção vertical, sabe-se que o fóton *A* tem 50% de chance de estar polarizado na direção vertical e 50% de chance de estar polarizado na direção horizontal.

Se, por exemplo, *A* for efetivamente medido e estiver polarizado na direção vertical, isso quer dizer que o fóton *B*, que ainda não foi medido passará a ter uma polarização definida na direção vertical (e apenas nessa direção).

Assim, se o observador em d_1 posicionar o seu cristal de calcita com o eixo óptico na direção vertical, a teoria diz que ele obterá, para essa medida, que o fóton estará polarizado na direção vertical ou que o fóton estará polarizado na direção horizontal (com 50% de chance para cada possibilidade e o mesmo valendo para qualquer ângulo de alinhamento escolhido). Supondo que d_1 observe um fóton polarizado na vertical, então, se d_2 posicionar o seu cristal com o eixo alinhado na direção vertical ele observará (com 100% de chance) também um fóton polarizado na vertical e, se ele posicionar o seu cristal alinhado na direção horizontal (formando 90^o com a vertical) ele observará (também com 100% de chance) que o fóton não estará polarizado na direção horizontal.

Resumindo, a situação pode ser entendida em termos de medidas binárias do seguinte modo:

1) Seja uma fonte que produz pares de fótons EPR que se deslocam em sentidos opostos;

2) Um medidor em d_1, posicionado no caminho de um dos fótons, pode posicionar o seu medidor em um ângulo qualquer com relação à vertical. Quando o medidor for atingido pelo fóton, a teoria diz que o fóton estará polarizado naquela direção (bit 1) ou estará polarizado na direção perpendicular (bit 0).

3) Uma vez realizada a medida de d_1, a teoria afirma que, se M_2 for alinhado no mesmo ângulo que M_1, ele certamente medirá um fóton polarizado naquela direção (bit 1) e, se for posicionado na direção perpendicular, ele não medirá um fóton polarizado naquela direção (bit 0).

5.2) O teorema de Bell

Uma análise detalhada das condições estipuladas por Einstein para o experimento EPR levou John Bell, em um artigo crítico sobre o experimento EPR, a demonstrar (HERBERT, 1985) uma desigualdade, conhecida como desigualdade de Bell, sobre o comportamento esperado das medidas realizadas pelos observadores posicionados em d_1 e d_2.

A prova de Bell é feita por contradição (*reductio ad absurdum*) e sua estrutura é a seguinte:

1) Para toda uma classe de experiências com partículas fortemente correlacionadas (EPR e variantes), é aceita a pressuposição de localidade;
2) Esta pressuposição conduz a uma desigualdade que deve ser satisfeita em todos os resultados experimentais;
3) As experiências contradizem a desigualdade, logo, a pressuposição de localidade é considerada incorreta.

Bell definiu um atributo a ser medido, chamado de correlação de polarização (*CP*).

CP é definido de tal modo que o valor de *CP* é igual a 1 se ambos os observadores obtiverem o mesmo resultado ao realizar a medida no respectivo fóton e é igual a zero se obtiverem resultados diferentes. Assim:

1) Se os medidores de d_1 e d_2 estiverem ajustados no mesmo ângulo, então, como os fótons estão correlacionados e ambos obterão o mesmo resultado, o valor de *CP* é igual a 1.

$$\text{Se } \theta_1 - \theta_2 = 0^o \Rightarrow CP = 1.$$

2) Se os medidores de d_1 e d_2 estiverem ajustados em um ângulo diferindo de exatamente 90^o, então, como os fótons estão correlacionados e ambos obterão resultados contrários, o valor de *CP* é igual a 0. Se um fóton estiver polarizado na direção escolhida por um dos observadores, o seu parceiro correlacionado estará não-polarizado na direção escolhida pelo outro observador e vice-versa.

$$\text{Se } \theta_1 - \theta_2 = 90^o \Rightarrow CP = 0.$$

O atributo *CP* é obtido a partir da medida conjunta da polarização de ambos os fótons correlacionados e pode ser interpretado considerando que *CP=1* indica que toda a série de medidas realizadas por observadores em d_1 e d_2 em um número grande de fótons correlacionados concorda sempre (ambos sempre obtém a mesma medida) enquanto que *CP=0* indica que ambos sempre discordam nas suas medidas. A análise de Bell se refere ao que acontece quando os medidores são alinhados em ângulos diferentes de 0^o e 90^o, cujo resultado é trivial.

A Teoria quântica indica que, para partículas correlacionadas e com medidores alinhados cujos ângulos formados pelos eixos ópticos difiram por θ, a probabilidade de que d_1 e d_2 efetuem uma medida e observem um fóton polarizado ao longo de seus respectivos eixos (ambos obtém 1) é dada por:

$$P = \cos^2\theta$$

Assim, *CP* pode ser identificado como sendo a probabilidade de que d_1 e d_2 consigam medir seus respectivos fótons como estando polarizados nas

direções escolhidas quando estas direções fazem entre si ângulo de θ graus.

A desigualdade de Bell, na versão binária, pode ser obtida assim:

1ª Situação:

1) Supondo d_1 alinhado na vertical ($\theta_1 = 0^o$);
2) Supondo d_2 alinhado com $\theta_2 = 30^o$;

Nesse caso, observa-se, experimentalmente que $CP = ¾$ e $1 - CP = ¼$.

Isso quer dizer que, se os medidores em d_1 e d_2 forem orientados desse modo, para um grande número pares de fótons correlacionados medidos, d_1 e d_2 concordarão, em média, com 3 a cada 4 bits medidos (a probabilidade de d_1 e d_2 obterem o mesmo bit 1 é de 75% e a de obterem bits diferentes é, conseqüentemente, de 25% ou seja, 1 erro a cada 4 bits). Esse resultado experimental é compatível com a teoria quântica, pois, aplicada a teoria, obtém-se $P = ¾$.

Definindo P_{erro} como sendo o limite de $1 - CP$ para um grande numero de fótons, a desigualdade de Bell para esse caso se escreve na forma:

$$P_{erro} \leq ¼$$

Indicando que não pode haver mais que 1 erro em cada quatro medidas combinadas.

Situação 2:

1) Supondo d_1 alinhado a 30^o da vertical ($\theta_1 = 30^o$);

2) Supondo d_2 alinhado com $\theta_2 = 60^o$;

Nesse caso, também se obtém $CP = ¾$ e $1 - CP = 1/4$. Com 3 acertos a cada 4 tentativas ou, alternativamente, 1 erro a cada 4 tentativas.

Note-se que o resultado experimental indica que o valor de *CP* é independente dos ângulos escolhidos e depende apenas da diferença relativa entre eles.

Novamente, d_1 e d_2 concordarão, em média, com 3 a cada 4 bits medidos (a probabilidade de d_1 e d_2 obterem o mesmo bit 1 é de 75% e a de obterem um bit diferente é de 25%).

Portanto:

$$P_{erro} \leq ¼$$

Indicando que não pode haver mais que 1 erro em cada quatro medidas combinadas.

Situação 3:

1) Supondo d_1 alinhado a 30^o da vertical ($\theta_1 = 60^o$);
2) Supondo d_2 alinhado com $\theta_2 = 90^o$ (direção horizontal);

Nesse caso, também se obtém $CP = ¾$.

Portanto, $P_{erro} \leq ¼$, indicando que não pode haver mais que 1 erro em cada quatro medidas combinadas.

A validade das observações 1, 2 e 3 corresponde à experiência e, também, ao previsto pela teoria quântica.

Situação 4:

Partindo da situação 3, se d_1 retornar o seu medidor para o alinhamento $\theta_1 = 0^o$ imediatamente antes de receber o fóton *A*, e supondo que a decisão de d_1 de realinhar o seu medidor M_1 não possa afetar a medida realizada por d_2 (pressuposição de localidade de Einstein) então, a probabilidade de que d_1 e d_2 observassem bits diferentes deveria ser:

$$1 - CP = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}$$

Uma vez que, sempre que houve uma diferença de 30^o (situações 1, 2 e 3) o valor de *1 – CP* era igual a ¼ e agora tem-se uma diferença de 90^o (3×30^o) entre os ângulos dos medidores.

Nesse caso, se a escolha de d_1 é independente da escolha de d_2 e a escolha de d_1 não pode afetar a escolha de d_2 (pressuposição de localidade) a desigualdade de Bell indica que:

$$P_{erro} \leq \frac{3}{4}$$

Assim, nesse caso, deveria haver, no máximo 3 erros (A e B não medem a mesma coisa) para cada 4 fótons observados.

No entanto, se a partir da situação 3, θ_1 voltar a ser 0^o então, o conhecimento experimental sobre fótons correlacionados diz que deveria ser exatamente $P = 0$ (pois $\theta = 90^o$) e, conseqüentemente:

$$1 - P = P_{erro} = 1$$

Assim se os fótons estiverem correlacionados e se os medidores forem

orientados em direções diferindo de 90^o, as medidas de d_1 e d_2 nunca concordarão. Isso também está de acordo com a Teoria Quântica ($\cos^2 90^o = 0$).

Assim, devido à contradição entre a desigualdade de Bell e o resultado experimental, a premissa usada deve estar incorreta.

Como a pressuposição de localidade leva a uma contradição com o resultado das medidas experimentais, esta pressuposição deve ser falsa.

A conclusão final é que, qualquer sistema fortemente correlacionado (como os fótons e os pares elétron-antielétron EPR) deve necessariamente desobedecer à desigualdade de Bell. Sistemas fracamente correlacionados (que podem ser simulados experimentalmente através de mecanismos locais) obedecerão à desigualdade de Bell e, devido a esse fato, podem ser facilmente distingüíveis dos sistemas de partículas em estado realmente geminado.

O teorema de Bell tem diversas implicações filosóficas e, também, como será visto mais adiante, o desacordo ou acordo com a desigualdade de Bell para o sistema constituído dos usuários *A* e *B* do canal quântico usando o protocolo de Ekert, servirá como parâmetro para identificar a eventual interceptação por parte de um espião *E*.

5.3) O protocolo de Ekert

Assim como no BB84, o protocolo de Ekert pode ser dividido em duas partes, uma quântica e uma clássica.

A primeira parte refere-se à comunicação através do canal quântico para a geração de duas *string*s que A e B usarão como chave primária.

A segunda parte, realizada através de um canal clássico comum, refere-se aos processos de amostragem e verificação de erros, reconciliação das *string*s e amplificação de privacidade.

Nesta segunda parte, o procedimento utilizado é o mesmo usado no BB84, com os usuários autorizados do canal obtendo uma *string* comum a ambos e cujo conhecimento por um eventual espião pode ser limitado, com uma escolha adequada de parâmetros e o uso de funções da *hash*, a ser tão pequeno quanto se queira.

Ambos os protocolos usam a fase quântica como uma maneira de realizar a distribuição de chaves (distribuição de chaves quântica). A diferença fundamental entre os dois se dá no modo de implementação da fase quântica.

O protocolo de Ekert usará o fenômeno da correlação de fases e isso, como será mostrado, apresenta uma série de vantagens, teóricas e práticas sobre o BB84.

5.3.1) Implementação da parte quântica.

Um arranjo mínimo para a implementação se constitui em uma fonte de fótons EPR, capaz de produzir fótons correlacionados a uma taxa conhecida e conectada a dois canais para a transmissão de fótons.

Um dos canais será conectado à aparelhagem de medida e detecção de fótons de *A* e o outro à aparelhagem de *B* (designados como canal *A* e *B* respectivamente) e, claro, um canal de comunicação clássico entre *A* e *B* para os procedimentos de reconciliação, amplificação de privacidade e a troca de mensagens codificadas propriamente dita (cf. figura 5.1).

Assim, no caso geral do protocolo de Ekert, a fonte de fótons não fica necessariamente sob o controle de *A* ou de *B*. O que se tem é uma fonte de fótons posicionada em algum ponto do caminho entre *A* e *B* e que emitirá fótons para ambos os usuários do canal quântico.

Eventualmente, pode-se imaginar o caso em que *A* e *B* possuam, cada qual a sua própria fonte, podendo iniciar a comunicação através do envio de

fótons ao seu parceiro ou ainda o caso em que *A* ou *B* possuem uma única fonte EPR. Contudo, tais casos podem ser trivialmente reduzidos ao caso geral.

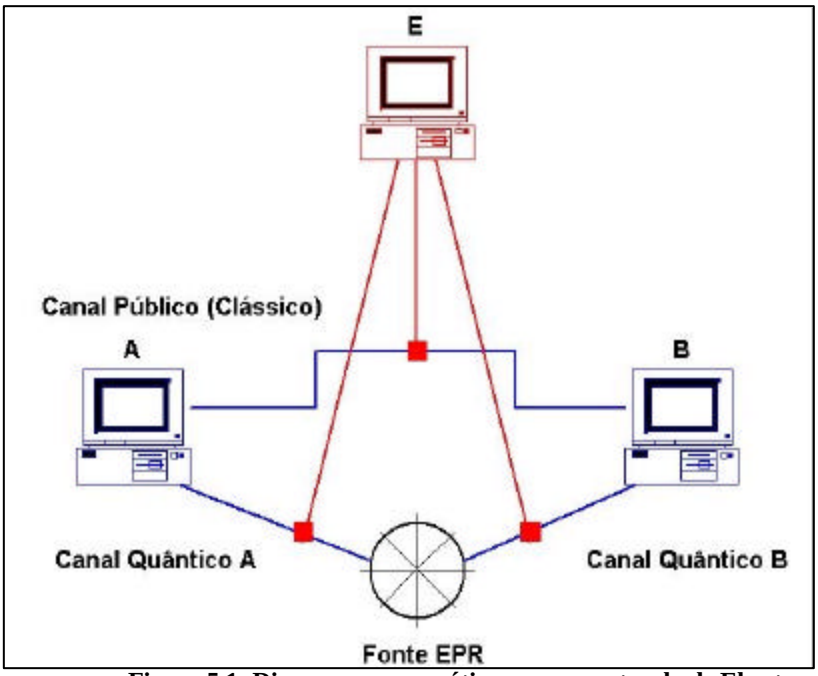

Figura 5.1: Diagrama esquemático para o protocolo de Ekert

A idéia básica consiste no seguinte:

1) Possuindo uma fonte EPR que opere a uma taxa conhecida, *A* e *B* começam, em um determinado momento, que pode ser combinado previamente, ou sinalizado com a transmissão de alguns bits de alerta através do canal clássico ou do próprio canal quântico, a receber os fótons provenientes da fonte;

2) No caso do protocolo de Ekert, serão usadas 3 bases, os detectores de *A* e *B* poderão ser alinhados na direção vertical (direção 1 ou V-H), direção

formando 30^o com a vertical (direção 2) e direção formando 60^o com a vertical (direção 3);

3) Para cada fóton, *A* e *B* posicionam seus detectores, alinhando os eixos óticos de seus cristais de calcita aleatoriamente em uma das 3 direções;

4) Para cada fóton medido, ambos anotam a direção escolhida e a polarização medida;

5) Após receber um determinado número de fótons, *A* e *B* interrompem a recepção e trocam informação, usando um canal público clássico, sobre qual a base usada na medida de cada fóton (mas, como no BB84, não revelado o resultado da medida);

6) Cada fóton da seqüência em que ambos tenham escolhido a mesma base gerará um bit da *string* que será usada como chave primária (como no BB84);

7) Cada fóton, para o qual tenham sido usadas bases diferentes, será usado para formar duas *string*s de teste a partir da quais será verificada a violação da desigualdade de Bell (no BB84 eles eram descartados);

8) Caso não seja verificada uma violação da desigualdade (o que quer dizer que o sistema não está fortemente correlacionado como deveria estar para fótons EPR puros), *A* e *B* deduzem que a comunicação foi interceptada, jogam fora os resultados obtidos e reiniciam o procedimento.

9) Caso seja observada a violação da desigualdade na proporção esperada para um sistema fortemente correlacionado, *A* e *B* passam para a parte clássica do protocolo.

Pode-se notar que a parte crítica do protocolo está nos itens 6, 7 e 8.

Dependendo das bases escolhidas por *A* e *B*, podem ocorrer 3 possibilidades:

1) *A* e *B* escolhem a mesma base, seja a direção 1, 2 ou 3 ($\theta_{AB} = 0^o$);

2) *A* escolhe a direção 1 e *B* escolhe a direção 3 ($\theta_{AB} = 60^o$);

3) *A* escolhe 1 e *B* escolhe 2 ou *A* escolhe 2 e *B* escolhe 3 ($\theta_{AB} = 30^o$)

A partir das seqüências de bits obtidas nas situações 1, 2 e 3, serão geradas 3 *string*s. A *string* 1 será usada como chave primária e as *string*s 2 e 3 serão usadas como *string*s para testes da desigualdade de Bell.

Se o fóton estiver polarizado na direção medida por *A* e *B*, será contado como bit 1 e, se o fóton estiver polarizado na direção perpendicular, será considerado como 0.

Deve-se lembrar que os dois fótons estarão polarizados do mesmo modo para ambos os observadores se a base escolhida for a mesma.

Assim, considerando, por exemplo, a direção vertical, se o fóton for medido como estando polarizado nesta direção (desvio para a esquerda pelo cristal de calcita) será contabilizado como 1 e, se estiver polarizado na direção horizontal (desvio para a direita), será contabilizado como 0.

Para a verificação da desigualdade de Bell, as *string*s 2 e 3 obtidas por *A* e *B* deverão ser trocadas entre eles e cada um fará a verificação da coincidência ou não dos bits do seguinte modo:

1) Para a *string* 2 ($\theta_{AB} = 60^o$), a desigualdade de Bell indica que deve haver, no máximo, 2 erros em cada 4 bits ($P \leq 50\%$ sendo que, experimentalmente, se observa $P \geq 75\%$ para fótons geminados);

2) Para a *string* 3 ($\theta_{AB} = 30^o$), a desigualdade de Bell indica que deve haver, no máximo, 14 erros em cada 100 bits ($P \leq 14\%$ sendo que, experimentalmente, se observa $P \geq 25\%$);

Em ambos os casos, se os sistemas estiverem fortemente correlacionados (fótons EPR puros), as desigualdades devem ser violadas e o número de erros observados deve ser maior.

Caso os erros permaneçam dentro dos limites indicados pela desigualdade (média menor ou igual a 50% para a *string* 2 e média menor ou igual a 14% para a *string* 3), *A* e *B* considerarão que houve interceptação e descartarão a chave primária obtida (*string* 1).

Na prática, se a taxa de erros for bem menor que 75% para a *string* 2 ($\theta_{AB} = 60^o$) ou bem menor que 25% para a *string* 3 ($\theta_{AB} = 30^o$), *A* e *B* consideram a desigualdade não violada e descartam a chave primária (*string* 1).

Uma vez obtida a chave primária e verificada a desigualdade, passa-se à parte clássica do protocolo.

5.3.2) Implementação da parte clássica

Apesar das diferenças na parte quântica, a parte clássica do protocolo de Ekert pode ser implementada da mesma forma que o descrito no Capítulo 3 para o protocolo BB84.

O objetivo da parte clássica é o de obter, a partir da chave primária resultante da parte quântica, uma chave final, que possa ser usada para uma comunicação através de um canal clássico, usando o código de Vernam (Capítulo 2, seção 2.2.1.1).

Para isso, deverão ser aplicados, em seqüência:

1) Um procedimento de estimativa da taxa de erros na transmissão (que incluirá indistintamente, taxa de erros introduzida pelo canal, fótons não detectados por A ou B, falhas nos detectores, erros nos contadores, ruído térmico e outra possíveis fontes de erro, incluindo interceptação apenas parcial de fótons

por um espião);

2) Um procedimento de reconciliação;

3) Um procedimento de amplificação de privacidade.

Uma vez obtida a *string* que funcionará como chave primária na parte quântica, podem se aplicar os mesmos procedimentos para estimar taxa de erros introduzida pelo canal ou por uma possível interceptação parcial, através da troca de uma parte da *string* e verificação dos bits não concordantes.

Obtida uma estimativa da taxa de erros, pode-se estimar o tamanho de blocos necessários e executar o processo de reconciliação conforme descrito na seção 3.3.1.

O processo de amplificação de privacidade segue o mesmo procedimento descrito na seção 3.3.2.

Quanto ao resultado final, foi demonstrado (WAKS, 2004) que o procedimento clássico para obtenção da chave final leva a uma expressão para o conhecimento que pode ser obtido por um eventual espião em qualquer das fases do protocolo que é análoga à expressão obtida para o protocolo BB84.

Assim, através da escolha do parâmetro de segurança *s* (quantidade de bits sacrificados na aplicação da função de *hash*) por *A* e *B*, pode-se tornar o conhecimento de E sobre a chave obtida exponencialmente pequeno em *s*.

O valor obtido para a quantidade de bits final que poderia ser obtida por E, conforme demonstrado em (WAKS, 2004), é exatamente o mesmo obtido para o BB84 para uma função de *hash* que comprima a *string* de *n* bits (resultante do procedimento de reconciliação) em uma *string* de *n-t- s* bits.

$$P = 2^{-s} / \ln 2$$

5.4) Segurança no protocolo de Ekert

O que garante a segurança no protocolo de Ekert?

Ekert, no seu artigo original em que propõe o protocolo (EKERT, 1991), conjecturou que o uso da desigualdade de Bell seria uma garantia da inviolabilidade do protocolo frente à espionagem do canal, uma vez que um espião não poderia obter conhecimento sobre as partículas em estado correlacionado sem induzir alterações detectáveis por A e B.

No entanto, do ponto de vista prático/experimental, é insuficiente mostrar que o fato de se interceptar o canal induziria a erro detectável nos dados, pois, em sistemas reais, mesmo nas melhores condições, sempre há uma taxa de erros que não pode ser distinguida de interceptação com conseqüente alteração de estado das partículas.

Para uma garantia efetiva de segurança, as fases de reconciliação e amplificação de privacidade são essenciais.

O protocolo de Ekert apresenta uma série de possibilidades que permitem um incremento da segurança se comparado ao BB84. Dois pontos em especial, um de natureza teórica e outro de natureza prática, merecem um destaque especial, não tendo análogos no protocolo BB84.

5.4.1) Chaves em estado de realidade suspensa

O primeiro ponto refere-se ao armazenamento das chaves.

Apesar do BB84 solucionar de forma eficiente o problema de distribuição de chaves, o uso do código de Vernam ou de algum equivalente completamente inviolável exige chaves muito extensas, pois um código completamente seguro exige chaves com, pelo menos, o mesmo tamanho que a mensagem a ser codificada, conforme demonstrado por Shannon na sua Teoria

Matemática da Comunicação (SHANNON, 1948).

Coloca-se então o problema do armazenamento seguro dessas chaves.

No BB84, as chaves devem ser usadas imediatamente ou, eventualmente, ser armazenadas classicamente.

Caso não se possua um canal quântico totalmente seguro, o armazenamento de chaves para uso como autenticação antes de se iniciar o protocolo propriamente dito passa a ser uma parte obrigatória do processo para garantir a segurança conforme discutido na Seção 3.4.4.

No protocolo de Ekert, o uso da não-localidade e de estados correlacionados permite se conjecturar sobre a possibilidade do armazenamento quântico das chaves.

Para ver como isso poderia ser implementado, basta considerar que A e B poderiam armazenar os fótons recebidos sem fazê-los passar pelo aparelho de medida (i.e. não alterando os seus estados) e mantê-los armazenados indefinidamente nesse estado não-medido.

A e B só realizariam as medidas de polarização em algum momento posterior, quando as chaves fossem necessárias.

Nesse caso, um eventual espião se veria na difícil tarefa de tentar obter uma informação que ainda não existe, pois os fótons, embora correlacionados, continuam obedecendo à mecânica quântica e não possuem, antes de medidos, qualquer polarização definida.

Os fótons usados na transmissão quântica poderiam assim, ser mantidos armazenados indefinidamente nesse estado de realidade apenas potencial e as chaves só seriam efetivamente geradas quando necessário.

Infelizmente, a tecnologia de armazenamento de fótons e a manutenção de seus atributos dinâmicos indefinidos por períodos arbitrários de tempo ainda não é viável tecnologicamente, mas, por outro lado, não há questões de princípio que impeçam a implementação futura desse tipo de segurança.

5.4.2) Uso seguro de pulsos de luz

Conforme discutido na Seção 4.4.4, a dificuldade de se obter fontes de luz que emitam fótons isolados representa uma vulnerabilidade importante na fase quântica do BB84.

Essa, claro, é uma limitação tecnológica e não existe nenhuma questão de princípio que proíba a construção de fontes tão precisas.

No entanto, o uso de fótons individuais apresenta o problema de que fótons isolados são especialmente sensíveis a impurezas no canal de transmissão, fazendo com que a manutenção da polarização em estado aleatório por longas distâncias se torne especialmente problemática implicando em sérias limitações práticas na execução do BB84 para situações de comunicação a longa distância.

No caso do protocolo de Ekert, foi demonstrado (WAKS, 2004) que o resultado obtido para o máximo conhecimento possível para um espião pode ser tornado exponencialmente pequeno em termos de um parâmetro de segurança s escolhido por A e B conforme discutido na Seção 4.3.2, o mesmo resultado obtido para o BB84. Outro ponto interessante é que a demonstração usa um argumento bem mais genérico que o usado por Bennet para o BB84.

Para o protocolo de Ekert, o valor foi derivado sem nenhuma asserção especial sobre o tipo de fonte usada para emitir os fótons, ao contrário do BB84 onde essa suposição é explicitamente usada e necessária.

Assim, o protocolo de Ekert é inerentemente imune a ataques que usem a divisão do pulso de luz e a medição de apenas alguns fótons pelo espião. A vulnerabilidade do BB84 a esse tipo de ataque mostra a vantagem do esquema de Ekert em termos de segurança.

Embora a demonstração seja bastante técnica, pode-se sentir o sabor da

prova através do argumento simples que segue.

Conforme discutido na Seção 3.4.4, um pulso fraco de luz pode ser considerado como uma sobreposição de estados quânticos com 0, 1, 2, ... fótons.

Isso quer dizer que se pode associar uma onda ψ a um pulso que é a resultante da sobreposição de ondas ψ_0, ψ_1, ψ_2, ..., cada uma descrevendo um estado com 0,1,2,... fótons. A sobreposição destes estados quânticos pode ser, ela mesma, considerada como um estado quântico.

Sendo o pulso constituído por muitos fótons, os dois pulsos emitidos pela fonte para *A* e *B* se constituem de dois sistemas cujas ondas apresentam correlação forte.

Ora, caso E tente desviar uma parte do feixe enviado a *B* (caracterizado originalmente por ψ_B) para realizar suas próprias medidas, ele produzirá dois feixes ψ'_B e ψ''_B, cada um deles composto por alguns fótons que constituíam o pulso original, enviando ψ'_B para *B* e recebendo ψ''_B.

Quando E efetivamente realizar a medida de ψ''_B, estará alterando o estado deste pulso, de modo que a soma (ondulatória, conforme o princípio da superposição) de ψ'_B e ψ''_B será diferente da onda ψ_B original, destruindo a correlação perfeita com ψ_A.

Alternativamente, basta considerar que, para todos os efeitos, ψ_B será medido duas vezes, enquanto ψ_A será medido apenas uma vez por *A*.

O mesmo raciocínio pode ser generalizado para o caso em que *E* desvia parte do pulso *A* e parte do pulso *B*. Como *E* não pode controlar quais as decisões de *A* e *B* quanto aos ângulos escolhidos para suas próprias medidas, mesmo que ele faça duas medidas iguais em cada feixe desviado, ao final haverá vários pulsos para os quais as decisões de *A* e *B* quanto ao alinhamento de seus instrumentos vai diferir tanto entre eles mesmos quanto com a decisão tomada por *E*, quebrando a correlação perfeita e, assim, diminuindo a taxa de violações

da desigualdade de Bell que um sistema verdadeiramente correlacionado deveria apresentar.

Assim, pode-se concluir que o uso de pulsos ao invés de fótons discretos não é uma exigência do protocolo de Ekert como quesito determinante da segurança.

5.5) Problemas e vulnerabilidades no protocolo de Ekert

Apesar das vantagens em termos de segurança sobre o BB84, o protocolo de Ekert, como em geral acontece com qualquer nova tecnologia, apresenta os seus próprios problemas.

Para a investigação básica de criptografia quântica, dois deles se destacam:

1) A segurança da fonte de fótons:

A principal vulnerabilidade associada ao protocolo de Ekert refere-se ao fato de que a fonte de fótons não se encontra, em princípio, sob a guarda nem de A, nem de B.

Desse modo, E pode tentar uma estratégia muito mais agressiva que a descrita na Seção 3.4.4 (item 3) e simplesmente suprimir completamente a fonte de fótons correlacionados por uma outra fonte, sob seu controle, capaz de emitir fótons preparados de forma previamente conhecida por E ou então capaz de emitir 3 pulsos de luz correlacionados (um dos quais E poderia armazenar e medir oportunamente, após conhecimento da discussão pública entre A e B).

Essa possibilidade de ataque foi levantada pelo próprio Ekert, que conjecturou, mas não demonstrou, de maneira conclusiva que o protocolo seria seguro mesmo face a uma fonte de fótons projetada para imitar a estatística EPR

e ao mesmo tempo vazar informações para E.

Posteriormente, em (BENNET; 1995) foi demonstrado que *E*, mesmo tendo total controle da fonte e conhecimento sobre a polarização dos fótons enviados, não poderia obter conhecimento efetivo sobre as *string*s de *A* e *B* sem introduzir a mesma taxa de erros de aproximadamente 25% encontrada no protocolo BB84 original.

Infelizmente, esta demonstração se baseou em um modelo simplificado do protocolo, não sendo suficiente para garantir a segurança no caso mais geral.

Finalmente, em (WAKS, 2004), foi demonstrado para o caso mais geral de ataque desse tipo (e para qualquer ataque do tipo individual), que E não poderia obter um conhecimento final sobre as *string*s superior a $2^{-s}/ln2$ conforme discutido anteriormente.

2) O uso da desigualdade de Bell como teste de verificação:

Outra vulnerabilidade consiste no uso da desigualdade de Bell como parâmetro de conferência sobre eventual interceptação.

Conforme foi mostrado anteriormente, uma seqüência de pares de fótons sem correlação forte real (como o que poderia ser simulado por um atacante) apresentaria, no caso ideal, uma taxa de erros menor no resultado final que aquela apresentada por pares fortemente correlacionados.

Ora, em sistemas reais sempre existe uma quantidade de erros associada às propriedades físicas do canal e dos aparelhos de medida. Caso essa taxa de erros do caso real não seja devidamente computada, pode-se imaginar a possibilidade dos erros associados ao canal e instrumentos de medida produzirem uma quantidade de erros que simule uma violação da desigualdade de Bell ao introduzir alguns erros a mais nas *string*s de teste.

Como um sistema fortemente correlacionado legítimo deveria produzir

mais erros que um sistema preparado por *E*, o ataque poderia passar despercebido com a quantidade de erros adicional simulando a violação esperada da desigualdade de Bell.

Para levar em conta as imperfeições do canal, Ekert sugeriu o uso da desigualdade de Clauser-Horne-Shimony-Holt (CHSH), ao invés da desigualdade de Bell pura.

A desigualdade CHSH foi usada por Clauser e seus colaboradores em 1969 para investigar experimentalmente o teorema de Bell (HERBERT, 1985) e foi obtida a partir de considerações experimentais adaptando o raciocínio original de Bell levando em conta a baixa eficiência dos detectores então existentes.

Embora não altere os procedimentos do protocolo em si, as taxas de erros obtidas para as *string*s de teste, obtidas na fase quântica, passam a ser comparadas com desigualdade CHSH ao invés da desigualdade de Bell propriamente dita.

Tal procedimento evita que os erros experimentais adulterem os resultados obtidos simulando uma correlação forte onde não há nenhuma.

5.6) Obtendo distâncias maiores usando protocolo de Ekert

A primeira implementação prática do BB84, descrita em (BENNET, 1991), foi construída e testada para uma distância entre *A* e *B* de meros 35 cm.

A limitação do BB84 para distâncias muito grandes está diretamente vinculada à necessidade de se usar pulsos de luz o mais fracos possíveis (com poucos fótons) de forma a se proteger de um possível ataque por divisão do pulso que garantiria a *E* a obtenção de alguns fótons de cada pulso que poderiam ser medidos posteriormente sem alertar *A* ou *B* da interceptação.

Com o avanço da tecnologia (obtenção de fontes perfeitas produzindo

fótons individuais a taxas exatamente conhecidas, uso de medidores de polarização cada vez mais exatos e de detectores cada vez mais sensíveis e imunes a ruído), há uma tendência de que essas limitações se tornem cada vez menos restritivas em termos de distâncias alcançáveis na prática.

Por outro lado, sendo o protocolo de Ekert imune a ataques desse tipo, abre-se a possibilidade de que possa ser usado para comunicações a distâncias consideravelmente maiores, usando pulsos de luz de curta duração mais intensos.

Com efeito, vários autores, por exemplo (JENNEWEIN, 1999), (WAKS, 2004), têm publicado trabalhos, tanto teóricos quanto experimentais que tratam sobre manutenção de estados correlacionados por longas distâncias e a conseqüente viabilidade da utilização do protocolo de Ekert para usuários espacialmente afastados.

Nesse último trabalho, especialmente, foi mostrado teoricamente que o protocolo de Ekert pode ser usado (considerando canais não-ideais) por distâncias de até 170 Km e foi proposto um mecanismo baseado em fótons correlacionados que permitiria a implementação de repetidores e a conseqüente extensão de canais quânticos usando o protocolo de Ekert por distâncias arbitrariamente grandes.

Capítulo 6 – Atualidades e perspectivas em criptografia quântica

Os desenvolvimentos atuais e futuros no campo da criptografia quântica passam pela solução de diversos desafios, tanto teóricos quanto técnicos, muitos dos quais ainda, no estágio atual, não podem nem ser avaliados adequadamente.

Um exemplo simples, que ilustra bem estes desafios é o fato de que, embora os trabalhos teóricos originais sobre o asssunto datem da década de 80 (baseados em um trabalho ainda mais antigo de Wiesner, escrito por volta de 1970), a primeira demonstração prática de um sistema usando criptografia quântica só pôde ser realizada em 1991 usando o protocolo BB84 (BENNET, 1991).

Há desafios teóricos e práticos em diversos campos, a Física, a Engenharia e a Informática sendo apenas alguns deles.

6.1) Desafios teóricos

No campo teórico, pode-se destacar:

1) Análise de vulnerabilidades potenciais nos diversos esquemas já propostos usando os princípios da Teoria Quântica:

Trata-se do uso intensivo de ferramentas próprias da Teoria Quântica, especialmente no que se refere a questões do que é ou não possível em princípio ou ainda no desenvolvimento de novas ferramentas teóricas de análise.

Além de estabelecer limites do que é ou não possível fazer baseado nas leis da Física, trata-se, também, de se prestar atenção em novos desenvolvimentos teóricos e experimentais nas diversas áreas relevantes da Física para poder aproveitar as novas descobertas, reforçando ou descartando protocolos propostos.

Um exemplo de pesquisas aparentemente não relacionadas que acabaram por se tornar objeto de estudo de pesquisadores da área de criptografia quântica é a análise do uso de Mensurações Quânticas Não-Demolidoras (QND), conceito introduzido por Braginski para o uso na detecção de ondas gravitacionais (HERBERT, 1985).

Embora sugerido em um contexto bastante distante da área de criptografia, a implementação de sistemas de medição e detecção usando QND (ainda além da tecnologia atual, mas inteiramente consistente com as leis da Física) poderia, em princípio, abrir caminho para estratégias de ataque não consideradas explicitamente no estabelecimento dos protocolos mais básicos como BB84 e Ekert (NAIK, 1999).

Dentre os campos de pesquisa mais importantes, destaca-se a pesquisa de possíveis estratégias de ataque.

Embora o caso de ataques individuais seja atualmente o mais amplamente estudado, estudos de casos e provas gerais de segurança contra ataques coletivos e conjuntos ainda são uma fronteira a explorar.

Mesmo que tais casos sejam inviáveis, tendo em vista a tecnologia atualmente disponível ou previsível, protocolos efetivamente seguros deveriam ser seguros contra qualquer estratégia de ataque concebível e compatível com as leis da Física.

2) Análise de vulnerabilidades nos processos de reconciliação e amplificação de privacidade usando Matemática, Estatística e Teoria da Comunicação:

Trata-se do desenvolvimento de novos algoritmos ou do refinamento dos já existentes para os processos de reconciliação e de novos desenvolvimentos, especialmente matemáticos, para análise e implementação prática das funções de compressão usadas na amplificação de privacidade.

Embora estes processos não sejam processos quânticos propriamente ditos, acabam por se tornar um limitante da eficiência do protocolo no que se refere a taxas de transmissão e são determinantes para garantir a segurança dos protocolos quando implementados em situações reais.

Trabalhos nessa área envolvem novos algoritmos para reconciliação como em (NAKASSIS, 2004) ou modificações de cunho estatístico nos esquemas originais como por exemplo em (ARDEHALI, 1998). Esse último consiste de uma modificação simples no protocolo BB84 original, em que o transmissor A (em concordância com B), escolhendo enviar os fótons de uma determinada base com probabilidade superior `a de sua base conjugada e usando métodos mais refinados de correção de erros leva, a melhoras consideráveis na eficiência do protocolo.

3) Criação de novos protocolos que usem sistemas quânticos com mais que dois estados discretos:

Pesquisa, tanto teórica quanto experimental, de sistemas baseados na codificação de informação usando partículas cujos atributos dinâmicos possam

assumir mais que dois valores distintos.

Esse tipo de pesquisa tem valor tanto diretamente no desenvolvimento de novos protocolos, quanto no estudo de possíveis vulnerabilidades nos protocolos já existentes.

4) Desenvolvimento de mecanismos para implementação de repetidores quânticos:

Trata-se das especificações teóricas de sistemas capazes de estender linhas de comunicação quânticas para distâncias cada vez maiores.

Os mecanismos comuns, usados nos canais clássicos para repetição envolvem armazenamento e amplificação dos sinais utilizados. Tais mecanismos podem ser considerados, do ponto de vista da Teoria Quântica, como medições, introduzindo alterações incontroláveis e irreversíveis nos estados quânticos e conseqüente perda de informação, capaz de inviabilizar completamente os protocolos quânticos.

Assim, são necessárias pesquisas para o estabelecimento de esquemas de repetição capazes de manter inalterados as informações codificadas nos estados das partículas em trânsito.

Uma linha de trabalho bastante promissora nessa área é apresentada em (WAKS, 2004).

5) Correções teóricas em protocolos para adaptação a condições reais.

Trata-se da adaptação dos protocolos, conforme discutidos teoricamente, a situações experimentais reais.

Nesse nível, pode-se citar, por exemplo, o uso da desigualdade CHSH ao invés da desigualdade de Bell original no protocolo de Ekert, sugerida pelo próprio Ekert para implementações reais.

A implementação de variantes do esquema original de Ekert, usando estados anti-correlacionados e a desigualdade de Wigner (e não a de Bell) para avaliar a presença de interceptação, é descrita em (BOVINO, 2004).

6.2) Desafios técnicos

Além dos problemas de cunho teórico discutidos na seção anterior, várias questões de ordem prática estão diretamente relacionadas com a implementação dos protocolos quânticos já existentes, a criação de novos protocolos ou de variantes mais seguras dos protocolos propostos:

1) Desenvolvimento de fontes de fótons de baixo custo e tamanho reduzido.

2) Desenvolvimento de fontes de vários fótons entrelaçados.

3) Desenvolvimento de detectores de baixo ruído para funcionamento em temperatura ambiente e de alta eficiência quântica.

4) Integração da rede quântica com a infraestrutura de cabeamento ótico já existente.

5) Tecnologias para armazenamento e preservação do estado de

polarização de fótons não medidos.

6) Transmissões quânticas ao ar livre, sem o uso de canais de fibra ótica.

A maioria destas questões envolvem soluções de engenharia extremamente refinadas como, por exemplo, no caso do item 3.

Atualmente, os detectores de fótons (a aparelhagem usada para registrar os fótons nos canais direito ou esquerdo após o desvio pelo cristal de calcita) baseiam-se no uso de fotodiodos de avalanche, componentes que apresentam bom ganho (até um simples fóton pode ser detectado) mas, ao mesmo tempo, a desvantagem de apresentar um elevado valor de ruído térmico, devido à necessária amplificação do sinal.

Para minimizar o problema, o fotodiodo deve ser mantido a temperaturas relativamente baixas (da ordem de 170 K) e deve haver uma sincronia adequada entre emissor e receptor, no caso do BB84, e entre os dois receptores e a fonte, no caso do protocolo de Ekert, para evitar que sejam computadas falsas medidas devido ao ruído em momentos nos quais nenhum fóton é esperado.

Os itens 1 e 2, por outro lado, envolvem o trabalho cooperativo de físicos experimentais e engenheiros para se obter fontes confiáveis, com taxas e características de emissão estáveis e bem conhecidas.

O item 5 é de fundamental importância para possibilitar o armazenamento dos fótons recebidos para o armazenamento seguro de chaves em potencial (fótons ainda não medidos), conforme descrito na Seção 5.4.1, assim como para o estudo de ataques coletivos e conjuntos.

Finalmente, as linhas de pesquisa relacionadas ao item 6 procuram obter

sistemas capazes de operar usando transmissões na atmosfera, o que permitiria o uso, por exemplo, de criptografia quântica em comunicações via satélite.

6.3) Desafios humanos

Um dos grandes desafios no desenvolvimento da criptografia quântica é justamente o seu caráter multidisciplinar.

O desenvolvimento e a implementação prática de protocolos quânticos exige conhecimentos que vêm de diversa áreas, como a Física Básica, Matemática, Estatística, Engenharia, Segurança de Redes, Informática. Assim, um dos desafios acaba sendo o de formar equipes de pesquisadores com conhecimentos de diversas áreas e interesses comuns.

Uma necessidade simples de destacar é a falta de *hackers* especializados para o desenvolvimento e aperfeiçoamento de estratégias de ataque em implementações reais.

Outra constatação é o próprio teor das publicações nessa área, que tende a ser, essencialmente, de dois tipos:

1) Publicações apenas para divulgação científica em um nível muito básico e pouco rigorosas.

2) Excessivamente especializadas e carregadas do jargão da Física, ficando, muitas vezes, quase ilegíveis para pesquisadores de outras áreas afins, especialmente da área de Informática (especialmente para programadores e especialistas em segurança).

Conclusão

Diversos esquemas de sistemas criptográficos quânticos vêm sendo propostos, todos eles buscando atingir o status de "absolutamente seguros".

No entanto, mesmo no caso dos protocolos quânticos originais mais antigos, aqui apresentados, essa meta ainda está longe de ser atingida.

Especialmente se forem levadas em conta os diversos problemas práticos e tecnológicos que se apresentam, percebe-se que ainda há um longo caminho a se percorrer antes de se falar em sistemas absolutamente seguros para uso em larga escala (comercial ou global).

Do ponto de vista tecnológico, as linhas de pesquisa atuais apontam o protocolo de Ekert (e variantes) como a base para desenvolvimentos futuros e para possíveis aplicações comerciais, tendo em vista as potencialidades e imunidade a certos tipos de ataques discutidas no Capítulo 5.

À medida que novos avanços ocorrem nesse campo, assim como na área de computação quântica e de comunicações quânticas, os profissionais das áreas envolvidas com informática, transmissão de dados e segurança computacional, especialmente aqueles que, no futuro, terão que lidar com essas tecnologias no seu cotidiano, e precisarão de cada vez mais conhecimentos sobre fundamentos e aplicações da teoria quântica.

No caso específico da criptografia quântica, embora apenas um conhecimento genérico e fenomenológico superficial de algumas propriedades gerais da teoria seja suficiente para se compreender genericamente o funcionamento dos principais protocolos como demonstrado neste trabalho, deve-se perceber que um entendimento mais profundo de todas as suas implicações e nuances envolve, necessariamente, conhecimento muito mais refinado e abalizado de vários aspectos formais, conceituais e factuais da Teoria

Quântica e das propriedades empíricas da Física de Partículas Elementares.

A Teoria Quântica foi formulada em resposta ao conhecimento empírico, cada vez mais refinado, da estrutura da matéria no início do século XX. Embora formulada para lidar com sistemas elementares, suas conseqüências, aplicações e resultados vêm mudando a forma como os cientistas compreendem o mundo, e suas aplicações tecnológicas vêm, cada vez mais, influindo na sociedade.

Tecnologias como os armamentos nucleares, a eletrônica moderna, a genética molecular e a própria informática são exemplos de aplicações da Teoria Quântica nos mais diversos campos do conhecimento.

Tanto a Eletrônica, quanto a Genética e a Informática são tecnologias que podem ser usadas, compreendidas e aplicadas, na grande maioria das vezes, sem uma referência explícita à infra-estrutura quântica que as sustenta. O mesmo ocorre no caso dos armamentos nucleares em que as implicações políticas ofuscam completamente a natureza das tecnologias envolvidas na sua produção.

No caso da criptografia e da computação quânticas, pela primeira vez observa-se tecnologias que trarão, necessariamente, conseqüências diretas e explícitas ao cotidiano das pessoas, tanto dos profissionais envolvidos, quanto dos usuários dessas tecnologias.

É concebível que, num futuro não muito distante, cidadãos "cultos" precisem ter conhecimentos conceituais básicos de teoria quântica para realizar mesmo pequenas tarefas do cotidiano. Este futuro pode estar mais próximo do que se imagina. Atualmente, várias corporações e órgãos governamentais como Deutsche Telekon, Id Quantique (www.idquantique.com/qkd.html) e o exército americano, já possuem produtos patenteados para o uso em protocolos de criptografia quântica.

Tal ponto de vista pode parecer um tanto exagerado. Mas, provavelmente, qualquer consideração sobre o uso disseminado de computadores eletrônicos pessoais por cidadãos comuns, para a realização de

tarefas tão corriqueiras quanto pagar uma conta em um terminal bancário eletrônico ou através de uma rede mundial de computadores, provavelmente teria parecido igualmente despropositada nos primórdios do desenvolvimento da computação eletrônica.

Assim, para os profissionais ligados a diversas áreas tecnológicas, a familiaridade com o arcabouço conceitual da Teoria Quântica e da sua aplicabilidade nos seus respectivos campos, e em especial para os profissionais de informática, poderá se tornar um imperativo crescente nos próximos anos.

Ao autor parece importante que tais profissionais comecem a se familiarizar, desde já, com a Teoria Quântica e com as aplicações relevantes, tanto por uma questão de preparação e adaptação às exigências sociais, profissionais e econômicas futuras, quanto pelas contribuições que profissionais e pesquisadores adequadamente formados/informados podem dar para esses desenvolvimentos.

Referências:

AGRAWAL, M. , KAYAL, N. , SAXENA, N. ; **PRIMES is in P.**
Agosto, 2002.[WWW]
http://www.utm.edu/research/primes/references/refs.cgi/AKS2002

ARDEHALI, M. , BRASSARD, G. , CHAU, H. , LO, H. ; **Efficient Quantum Key Distribution.**
Maio, 1998.[WWW]
http://arxiv.org/abs/quant-ph/9803007

BENNET, C. , BESSETTE, F. , BRASSARD, G. , SALVAIL, L. , SMOLIN, J. ; **Experimental Quantum Cryptography.**
Setembro 1991. [WWW].
URL: www.cs.uccs.edu/~cs691/crypto/BBBSS92.pdf

BENNETT, C. , BRASSARD, G. , EKERT, A. ; **Quantum Cryptography.** Scientific American, v. 267, n. 4, Oct 1992, pp. 50-57.

BENNETT, C. , BRASSARD, G. , CRÉPEAU, C. , MAURER, U. ; **Generalized Privacy Amplification.**
Maio 1995. [WWW]
URL: http://citeseer.ist.psu.edu/23662.html

BOVINO, F. , COLLA, A. , CASTAGNOLI, G. , CASTELLETO, S. , DEGIOVANNI, I. , RASTELLO, M. ; **Experimental Eavesdropping Attack Against Ekerts's Protocol Based on Wigner's Inequality.**
Agosto, 2003.[WWW]
http://arxiv.org/abs/quant-ph/0308030

BRASSARD, G. , SALVAIL, L. ; **Secret-Key Reconciliation by Public Discussion.**
1994.[WWW]
URL: http://citeseer.ist.psu.edu/96923.html

CACHIN, C. , MAURER, U. ; **Linking Information Reconciliation and Privacy Amplification.**
Outubro, 1935.[WWW]
URL: http://citeseer.ist.psu.edu/57498.html

DIRAC, P.; **The Principles of Quantum Mechanics.** 4a. ed. Oxford: Oxford University Press, 1958.

EINSTEIN, A. , PODOLSKY, B. , ROSEN, N. ; **Can Quantum Mechanical Description of Physical Reality Be Considered Complete ?**
Março, 1935. [WWW]
URL: http://www.burgy.50megs.com/epr.htm
Publicado Originalmente em: Physical Review, May 15, 1935,V.47, p777-780.

EKERT, A. ; **Quantum Criptography Based on Bell's Theorem.** Physical Review Letters, vol. 67, n. 06, 1991, pp. 661-663.

HERBERT, N.; **A Realidade Quântica.** 1a. ed. Rio de Janeiro: Francisco Alves Editora, 1985.

JENNEWEIN, T; SIMON, C; WEIHS, G; WEINFURTER, H; **Quantum Cryptography with Entangled Photons**, Physical Review Letters, vol. 84, n. 20, 2000, pp. 4729-4732.

LO, H. ; **Method for Decoupling Error Correction from Privacy Amplification.**
Abril, 2003.[WWW]
URL: http://arxiv.org/abs/quant-ph/0201030
Publicado Originalmente em: New Journal of Physics 5 (2003) 36.1-36.24.

MAGNIEZ, F.; **Cryptographie Quantique.**
Maio 1993. [WWW].
URL: www.cs.McGill.ca/~crepeau/PS/Mag93.ps

NAIK, D. , PETERSON, C. , WHITE, A. , BERGLUND, A. , KWIAT, P. ; **Entangled State Quantum Criptography: Eavesdropping on the Ekert Protocol.**
Dezembro, 1999.[WWW]
http://arxiv.org.org/abs/quant-ph/9912105

NAKASSIS, A. , BIENFANG, J. , WILLIANS, C. ; **Expeditious Reconciliation for Practical Quantum Key Distribution.**
Abril, 2004. [WWW]
URL: http://antd.nist.gov/pubs/orlando.pdf

SCHNEIER, B.; **Applied Cryptography**. 2ª. ed. New Jersey: John Wiley and Sons, 1996.

SHANNON, C. ; **A Mathematical Theory of Communication.** , The Bell System Technical Journal, 1948, Vol. 27, pp. 379-423, 623-656.

SLUTSKY, B. , RAO, R. , SUN, P. , TANCEVSKI, L. , FAINMAN, S. ; **Defense Frontier Analysis of Quantum Cryptographic Systems.**
Maio, 1998.[WWW]
http://kfir.ucsd.edu/papers/defense.pdf
Publicado originalmente em: Applied Optics, May 10,1998, V37, No. 14.

VOLOVICH, I. V.; **On Classical and Quantum Cryptography.**
Agosto 2001. [WWW].
URL: http://arxiv.org/abs/quant-ph/0108133

WAKS, E. , ZEEVI, A. , YAMAMOTO, Y. ; **Security of Quantum Key Distribution with Entangled Photons Against Individual Attacks.**
Dezembro, 2000.[WWW]
http://arxiv.org/abs/quant-ph/0012078

WIESNER, S. ; **Conjugate Coding**, Sigact News, vol. 15, n. 1, 1983, pp 78-88.
Manuscrito original datado de 1970.