1 Introdução

No início do século 20 começou a ser desenvolvida uma teoria que iria mudar para sempre a nossa percepção da natureza. Seu nome, a mecânica quântica, e seus criadores, Einstein, Bohr, Planck, entre outros.

A teoria quântica explicou fenômenos que a teoria clássica não conseguia compreender, como exemplo, podemos citar o efeito fotoelétrico. Além disso, previa comportamentos radicalmente diferentes do nosso dia-a-dia para partículas microscópicas como os fótons.

Possivelmente a propriedade mais curiosa descoberta a respeito das partículas microscópicas foi a dualidade onda-partícula. Ou seja, a luz possui propriedades ondulatórias, como interferência, bem como propriedades corpusculares como o fato de ser constituída de fótons que são indivisíveis e cuja energia individual depende apenas da freqüência de oscilação.

Ao longo do século XX a teoria quântica passou por diversas aprimorações aumentando cada vez mais nosso conhecimento sobre ela. Durante boa parte desse período a mecânica quântica não teve nenhuma aplicação direta nas nossas vidas tendo ficado restrita a discussões teóricas nos círculos acadêmicos.

As primeiras aplicações começaram a despontar no horizonte à medida que a tecnologia ligada a física do estado sólido avançou. Dispositivos eletrônicos como transistores e eletro-ópticos como lasers e LEDs requerem um conhecimento da teoria quântica para serem projetados. No entanto os modelos que descrevem esses dispositivos ainda são semiclássicos, no sentido em que os fótons e elétrons não são tratados individualmente.

Outro grande conceito desenvolvido no século XX, dessa vez por Shannon, foi a teoria da informação. Seus conceitos ainda são usados, sobretudo em telecomunicações e computação. As idéias de Shannon sobre processamento de informação, compressão de dados, etc... são essenciais para a compreensão de qualquer sistema que lida com informação.

Sem dúvida alguma uma das maiores invenções do século passado foi o transistor, que possibilitou a construção de computadores cada vez mais complexos e menores. Essa tendência vem se confirmando há pelo menos 30 anos no mundo da computação. Tamanha tem sido essa miniaturização, que as

estruturas dos dispositivos atuais utilizados nos computadores estão com dimensões próximas às de dezenas de átomos. Como essa tendência deve se confirmar nos próximos anos, podemos ter certeza de que teremos dispositivos cujas dimensões dos componentes serão da ordem de Ångstroms. Como a informação é processada através de bits (que é a menor unidade elementar de informação) e esses serão manipulados e armazenados nessas estruturas microscópicas, podemos afirmar que a manipulação desses bits será comandada pelas leis da mecânica quântica. Com isso temos a união de duas grandes teorias do século 20 em uma única teoria chamada teoria da informação quântica [1].

Dentro dessa nova teoria duas aplicações principais apareceram, a comunicação (criptografia e teleportação) e a computação quântica. Na realidade a primeira não é nada mais do que operações lógicas da computação quântica e já tiveram demonstrações experimentais, com a criptografia já entrando em um estado mais adiantado. A computação quântica é aquela que no momento apresenta o maior desafio tecnológico, pois embora muito já seja conhecido sobre a teoria, a implementação experimental se resume a sistemas extremamente simples sem aplicação prática até o presente momento.

O bit é a unidade fundamental da teoria de informação clássica, enquanto o análogo quântico foi batizado de *qubit*, isto é, *quantum bit*. Durante o texto os dois termos serão utilizados freqüentemente. O bit será utilizado quando refere-se a unidade de informação que temos acesso ou quando é processado por uma máquina clássica, enquanto o *qubit* será utilizado quando o bit estiver codificado em uma entidade quântica como um fóton, ou quando estiver sendo processado em um dispositivo quântico.

O objetivo desse trabalho é em um primeiro plano fazer uma análise sobre a criptografia quântica, cobrindo os principais pontos bem como os desafios tecnológicos existentes. Uma das formas de transmissão dos *qubits*, a codificação por freqüência, será estudada em detalhes, bem como será feita uma proposta para a sua melhoria. Medidas experimentais serão realizadas para comprovar a teoria desenvolvida.

1.1 Criptografia Quântica

A idéia é que Alice (o transmissor) envie uma mensagem para Bob (o receptor) de tal forma que um possível espião (Eva) não consiga ler a mensagem de forma alguma. Na realidade a arte da criptografia é muito antiga e até Júlio César supostamente utilizava uma cifra [2]. Ela simplesmente consistia em deslocar as letras duas posições para cima em relação ao alfabeto. Os métodos atuais de criptografia são muito mais sofisticados envolvendo cálculos matemáticos extremamente complexos requerendo computadores poderosos.

Existe uma forma de codificação chamada cifra de Vernam [3] que é 100% segura matematicamente. Essa cifra, no entanto, depende de uma chave que Alice e Bob têm que compartilhar antes que a transmissão possa ser feita. Essa chave tem que ser totalmente desconhecida por Eva, ou seja, a chave não pode ser enviada no mesmo canal de transmissão da mensagem sob o risco de ser interceptada. Por essa razão nenhum canal de comunicação clássico é 100% seguro, existindo sempre a possibilidade dele ser monitorado por Eva. A primeira opção para a distribuição da chave é utilizar algum serviço de entrega para que a Alice possa entregar a chave fisicamente ao Bob, por exemplo, uma empresa de guarda de valores entregando um disco contendo a chave. Essa opção além de muito cara não é totalmente segura, assumindo que Eva tenha poder de fogo suficiente para assaltar um carro-forte e que a informação a ser roubada utilizando a chave valha esse esforço.

A segunda (e bem mais elegante) opção é utilizar a mecânica quântica. Se codificarmos os bits a serem transmitidos em entidades quânticas como por exemplo um fóton, esses bits que agora passam a ser denominados *qubits*, adquirem propriedades bastante interessantes. A mais útil para nós no momento é o fato de eles sofrerem distúrbios ao serem observados. Através de uma monitoração cuidadosa do canal medindo a taxa de erro do sistema Alice e Bob têm como determinar se Eva tentou adquirir informação sobre a chave que está sendo transmitida. Como Alice e Bob só têm como saber se um espião está monitorando a transmissão durante o envio da mensagem, não é interessante utilizar a criptografia quântica para realizar uma comunicação. A aplicação desse método fica mais interessante para a distribuição de uma chave secreta, ou seja, para distribuir a chave necessária à cifra de Vernam. Logo, o termo mais

apropriado é chamado de QKD ou Distribuição Quântica de Chaves. A idéia da QKD será discutida com mais detalhes no próximo capítulo, bem como as técnicas para as transmissões dos *qubits*.

1.2 Teleportação quântica

Provavelmente esta é a aplicação mais curiosa da teoria de informação quântica. Apesar do nome lembrar muito os filmes de ficção científica, veremos que essa aplicação possui um nome muito avançado para uma idéia relativamente simples se as questões filosóficas não forem levadas em conta.

Um requisito básico para a teleportação é um par de partículas emaranhadas, normalmente chamado de par EPR, homenagem ao famoso artigo de Einstein, Podolsky e Rosen de 1935. Esse trabalho foi o ápice de uma famosa discussão entre Einstein e Bohr a completeza da teoria quântica [4]. O que nos interessa entretanto é que um par EPR, são duas partículas que são criadas juntas, por exemplo num decaimento de um estado excitado de um cristal não-linear, tipicamente saindo em direções opostas. Essas partículas possuem uma correlação marcante entre alguma propriedade (o exemplo mais comum é a polarização de fótons). Dependendo do tipo, ou elas possuem a mesma polarização ou polarizações opostas. Isso significa que ao medir uma partícula, automaticamente conhecemos o estado da outra. Em 1964, John Stewart Bell, no que foi uma das mais importantes descobertas teóricas da segunda metade do século XX, contrapôs os conceitos de realismo e localidade através de seus teoremas. Isso levanta discussões filosóficas profundas como problemas de causalidade e comunicação mais rápida do que a luz. Para uma discussão bem mais profunda e interessante ver [4] e [5].

A teleportação tem como função, transportar um estado quântico (extremamente frágil) através de um ambiente potencialmente perigoso, como um canal de comunicações. Um estado quântico é muito frágil pois qualquer interação com o meio externo faz com que ou ele se destrua ou se emaranhe com ele, tornando a informação codificada nele perdida. Dependendo do grau de emaranhamento ele pode ser recuperado, mas se ele se tornar parte de um sistema

quântico mais complexo (algumas partículas), somente um computador quântico pode conseguir extraí-lo de volta.

Um fato que não foi mencionado mas que é de extrema importância para a informação quântica em geral, é que um estado quântico desconhecido não pode ser clonado, isso é, não podem existir máquinas copiadoras quânticas [6]. A única exceção para essa regra é se a medida for feita no auto-estado do observável, por exemplo, se um polarizador estiver perfeitamente alinhado com a direção de polarização de um fóton. Se ele pudesse ser copiado perfeitamente não existiria necessidade para a teleportação. Alice poderia simplesmente medir o fóton, copiá-lo e enviar um número muito grande de cópias para Bob. Uma delas com certeza alcançaria o destino. Outra alternativa seria medir o fóton e dizer ao Bob qual a polarização deste, para que ele possa ser recriado.

A teleportação funciona da seguinte maneira: Uma fonte de pares EPR fica situada em algum lugar entre Alice e Bob. Em algum momento um par EPR é gerado com um dos fótons indo para Alice e o outro para Bob. Eles guardam os seus respectivos fótons até que o estado quântico desconhecido a ser teleportado $|\psi_A\rangle$ chegue a Alice. A notação *bra-ket* criada por Dirac para a mecânica quântica será utilizada nesse trabalho. Para maiores detalhes [7] é uma boa referência, ou qualquer outro livro de mecânica quântica. Alice possui então dois estados, $|\psi_A\rangle$ e $|\psi_C\rangle$ enquanto Bob possui o estado $|\psi_B\rangle$, sendo que esses dois últimos são os fótons do par EPR. Quando esse estado está nas mãos de Alice ela realiza uma espécie de projeção em um dos estados da base de Bell, com os estados de $|\psi_A\rangle$ em $|\psi_C\rangle$ chamada de Medição de um Estado de Bell ou *Bell-State Measurement* (BSM) [6]. Ela então, avisa a Bob por meio de um canal clássico (qualquer canal que utiliza meios de informação clássicos para transmissão é dito um canal clássico, podendo ser desde um simples anúncio em um jornal a um canal óptico de alta capacidade) qual o tipo de BSM foi feito. Dependendo do resultado da projeção, Bob realiza uma entre quatro operações em $|\psi_B\rangle$, lembrando que esse é o fóton do par EPR que ele possui. Sem entrar nos detalhes matemáticos ele torna-se idêntico a $|\psi_A\rangle$, enquanto o fóton $|\psi_A\rangle$ original em Alice é destruído. Logo, $|\psi_A\rangle$ é transmitido de Alice até Bob sem sofrer nenhuma modificação. A informação na realidade é transmitida através do par EPR e do

canal clássico. É importante frisar que *sem o canal clássico a teleportação não funcionará*, pois Bob não tem como saber que tipo de BSM foi realizado em Alice e sua escolha será aleatória, só conseguindo reproduzir o estado quântico em uma fração das tentativas de transmissão *sendo que ele não saberá quais fótons foram teleportados corretamente*. Esse requerimento da presença do canal clássico impede que noções inteiramente clássicas como causalidade (que implica numa realidade local) sejam violadas. A figura 1 representa um esquema do sistema.

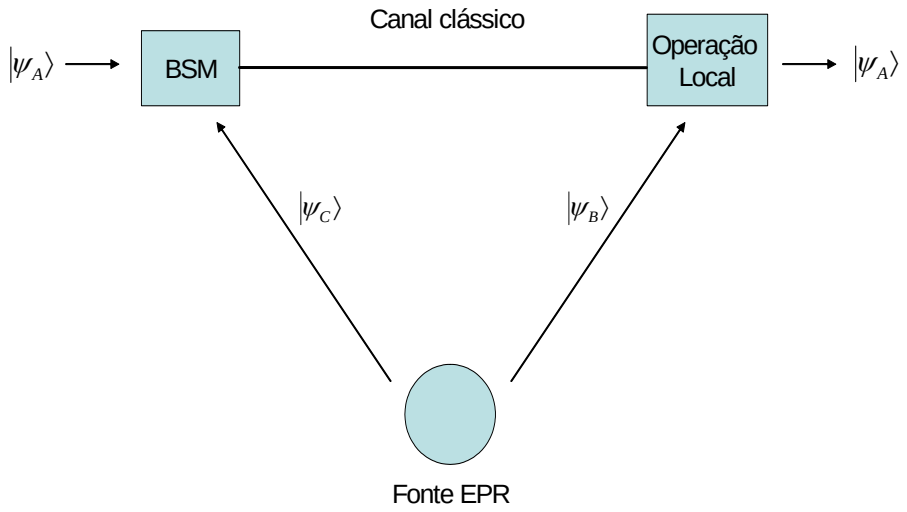

Figura 1: Esquema simplificado de um sistema de teleportação de *qubits* utilizando fótons. O *qubit* $|\psi_A\rangle$ é transmitido de Alice a Bob utilizando o par EPR composto de $|\psi_B\rangle$ e $|\psi_C\rangle$.

1.3 Computação quântica

Esta, com certeza, é a aplicação mais complexa da teoria de informação quântica. Enquanto a criptografia e a teleportação utilizam 1 e 3 *qubits* respectivamente, a computação irá tratar de sistemas de diversos *qubits* (milhares, dependendo do caso). Devido a natureza da mecânica quântica e propriedades

como emaranhamento e superposição, a complexidade do sistema cresce exponencialmente com o número de *qubits* envolvido com o problema, tornando-se quase intratável após alguns poucos *qubits*.

Há muito ceticismo entre alguns membros da comunidade acadêmica quanto à construção do computador quântico tamanha a sua complexidade. De qualquer forma já houve um grande ganho no conhecimento da teoria quântica e possíveis aplicações surgirão somente com o desenvolvimento de certos algoritmos quânticos.

A razão pelo grande interesse sobre a computação quântica é o imenso ganho na velocidade de processamento para certas operações ao se utilizar um algoritmo quântico, em relação a um clássico. Para deixar claro para o leitor, um algoritmo quântico só pode ser realizado por um computador quântico, ou seja, um computador em que os bits a serem processados (*qubits*) são guardados e transportados por entidades quânticas enquanto um algoritmo clássico é processado pelos computadores que utilizamos no dia-a-dia. Para dar uma idéia desse ganho, o melhor exemplo é o problema de fatoração que é de grande interesse para a criptografia clássica. Um computador clássico leva muito tempo para conseguir fatorar um número muito grande. Esse fato é utilizado no sistema RSA (nomeado após as três pessoas que o inventaram) de criptografia atualmente utilizado em todo o mundo. O RSA será explicado melhor no capítulo seguinte, mas por hora, basta saber que um possível *hacker* levaria muitos anos (possivelmente bilhões) utilizando um computador clássico para descobrir quais os números fatorados a partir de um outro número muito grande. Esses números fatorados constituem justamente a chave de um sistema de criptografia pública. Foi demonstrado recentemente por Shor [6] que um computador quântico utilizando um algoritmo quântico desenvolvido por ele, levaria segundos para realizar tal operação. Obviamente isso representa uma ameaça para os sistemas criptográficos atuais. Mas, além disso, mostra todo o potencial da computação quântica. De fato, todos os algoritmos quânticos desenvolvidos até hoje ou apresentam uma melhora em relação aos algoritmos clássicos, ou são iguais.

A razão pelo ganho exponencial (como é o caso do algoritmo de Shor) ou polinomial como é o caso do algoritmo de busca desenvolvido por Grover [6] é dada pelo processamento quântico paralelo inerente à própria mecânica quântica.

Um *qubit* de dois estados (por exemplo, o *spin* de uma partícula) pode ser representado por:

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{1.1}$$

que é uma superposição dos auto-estados $|0\rangle$ e $|1\rangle$ que correspondem aos *spin-down* e *spin-up* da partícula. A probabilidade de obter cada um desses estados ao se realizar uma medição é a^2 e b^2 respectivamente. Isso resulta numa propriedade interessante dos estados quânticos que não possui análogo clássico: uma partícula quântica não pode ser descrita somente com dois estados. Na realidade ela pode estar em uma superposição de dois estados $|0\rangle$ e $|1\rangle$. Obviamente ao ser medida, a partícula irá se encontrar em um desses dois estados, mas *é impossível saber qual deles deterministicamente antes de realizar a medida*. Tudo que sabemos é a probabilidade de encontrarmos a partícula em um dos estados.

Sem entrar em muitos detalhes, todos os algoritmos quânticos mostram que ao se aplicar uma operação de evolução unitária a *qubits*, a operação é aplicada em todos os *qubits* guardados na memória do computador em um único passo. Esse ganho é realmente espantoso se comparado a um sistema clássico em que a operação é aplicada bit a bit. A situação parece ser boa demais para ser verdade até por que na realidade ao se realizar uma medição não se obtém todos os valores simultaneamente. Por essa razão não é trivial o desenvolvimento de um algoritmo quântico, pois é preciso projetá-lo de forma a conseguir aproveitar o potencial da computação quântica. Já existem alguns algoritmos que oferecem um ganho exponencial como é o caso do algoritmo de fatoração de Shor.

A situação experimental da computação quântica está muito atrás da teoria. Somente portas lógicas quânticas foram até agora realizadas. Para a eventual construção de um computador quântico universal, milhares destas portas serão utilizadas no mesmo sistema. O problema atual é conseguir utilizar várias portas em conjunto sem que os estados quânticos individuais emaranhem-se. Os três métodos mais utilizados hoje em dia são *cavity* QED (Eletrodinâmica quântica), íons armadilhados e NMR (Ressonância Nuclear Magnética) que é o sistema mais provável a conseguir processar vários *qubits* simultaneamente. Uma solução através de semicondutores (pontos quânticos) pode vir a revolucionar esse campo, porém ainda está muito imatura para ser colocada em prática.