5
Criptografia e Teleportação

Apresentaremos neste capítulo duas importantes aplicações do emaranhamento de estados: a *criptografia quântica* e a *teleportação*.

5.1
Criptografia Quântica

Em 1989 (2, 18), foi anunciada a descoberta de um novo sistema de criptografia, baseado nos princípios da mecânica quântica. Neste sistema, a chave utilizada para encriptar mensagens é constituída por uma série de qubits, os quais têm seus estados dados pela polarização de fótons.

Conforme alguns métodos de criptografia clássica, a segurança das chaves depende da fatoração: embora seja fácil para um computador multiplicar dois números muito grandes, é extremamente difícil decompô-los em números primos. Já um computador quântico não teria problemas em efetuar tal operação.

Entretanto, ao contrário da criptografia de chave-pública, a criptografia quântica ainda seria segura mesmo que computadores quânticos fossem utilizados, pois os princípios da mecânica quântica nos garantem que é impossível quebrar uma chave formada por qubits: durante a distribuição da chave quântica, sempre que alguém tenta interceptar os fótons para medir sua polarização, introduz erros que são percebidos tanto pelo remetente quanto pelo destinatário. Por isso dizemos que estas chaves são "inquebráveis".

Atualmente, já existem empresas vendendo produtos que utilizam sistemas de criptografia quântica (20). Utilizando fios de fibra óptica para transportar os fótons polarizados, cientistas da Universidade de Genebra conseguiram realizar experimentalmente o envio de chaves quânticas a uma distância de cinqüenta quilômetros (13), e uma das empresas citadas mostrou que pode distribuí-las a até cento e vinte quilômetros (11).

Há ainda uma outra maneira de distribuir chaves quânticas: através de fótons emaranhados (3). A grande vantagem neste caso é que não há a necessidade de deslocamento de fótons do remetente para o destinatário, embora cada um deles deva receber um dos fótons do par emaranhado.

5.2 Teleportação

Nesta seção apresentaremos outro emprego do emaranhamento na comunicação quântica, a teleportação, no qual promove-se o transporte de estados quânticos sem haver a necessidade do deslocamento de todos os fótons envolvidos, assim como na distribuição de chaves quânticas sem haver a necessidade do deslocamento de todos os fótons envolvidos, assim como na distribuição de chaves quânticas utilizando pares emaranhados. Os primeiros avanços neste tipo de experimento já foram feitos: em 2003, o mesmo grupo de Genebra (14) já citado anteriormente realizou a teleportação (ou seja, a transferência de um estado quântico sem passagem por um meio físico entre os pontos inicial e final) de qubits utilizando um cabo enrolado com comprimento de dois quilômetros, embora a distância real entre os dois laboratórios envolvidos fosse de cinqüenta metros. Já em 2004, um grupo de cientistas da Universidade de Viena conseguiu teleportar qubits a uma distância de seiscentos metros (23), sendo este o melhor resultado obtido até hoje para distribuição dos fótons que compõem o par emaranhado.

5.2.1 Teorema da Não-Clonagem

Ao contrário do pensamento geral, a teleportação não é um experimento restrito aos filmes de ficção científica: como vimos, há alguns anos ele já é uma realidade. É importante entender que o que é de fato transferido de um ponto a outro (sem qualquer canal clássico que os ligue) não são os componentes físicos de um objeto, e sim a informação sobre ele. Ou seja, teleportamos estados quânticos, não sistemas. Assim podemos concluir que o objeto que "aparece"no destino é uma cópia exata, e não o mesmo objeto que encontrava-se na posição inicial. Átomos ainda não foram de fato teleportados mas, se fossem, poderíamos afirmar sem ressalvas que esta réplica não é constituída da mesma matéria do original, e sim de átomos do mesmo tipo, organizados exatamente da mesma maneira.

De alguma forma temos então que obter toda a informação inerente a um sistema. Entretanto, sabemos que ao realizarmos uma medição, invariavelmente perturbaremos o estado observado. Logo, a teleportação só é possível se o estado original for destruído. Uma idéia seria então clonar o estado que se quer teleportar e medir as cópias. Mas veremos que isso não é possível, por contradizer o *teorema da não-clonagem*.

Este teorema afirma que é impossível criar cópias perfeitas de um objeto (um qubit, por exemplo) que encontre-se em um estado desconhecido. Sua

demonstração é bastante simples e será dada a seguir:

Seja $|\phi\rangle \in \mathcal{H}$ um estado desconhecido. Suponhamos que exista um processo capaz de clonar um estado qualquer. Representamos um processo deste tipo por uma transformação linear

$$L : |\phi\rangle|\Psi\rangle \mapsto |\phi\rangle|\phi\rangle|\Psi_\phi\rangle,$$

onde $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ representa o estado do "aparelho"que faz a clonagem. É importante frisar que este estado é sempre o mesmo para qualquer estado $|\phi\rangle$, já que não temos nenhum conhecimento do estado a ser clonado. Além disso, por ser esta uma operação de clonagem, $|\Psi_\phi\rangle$ deve obviamente pertencer ao espaço $\mathcal{K}$. Sejam agora $|1\rangle$ e $|2\rangle$ dois estados *linearmente independentes* a serem clonados. Temos:

$$\begin{aligned} |1\rangle|\Psi\rangle &\mapsto |1\rangle|1\rangle|\Psi_1\rangle \\ |2\rangle|\Psi\rangle &\mapsto |2\rangle|2\rangle|\Psi_2\rangle. \end{aligned}$$

Como o aparelho em questão seria capaz de clonar também o estado $|1\rangle + |2\rangle$, temos ainda:

$$(|1\rangle + |2\rangle)|\Psi\rangle \mapsto (|1\rangle + |2\rangle)(|1\rangle + |2\rangle)|\Psi_{12}\rangle.$$

Sendo L linear podemos somar as duas equações anteriores e concluir:

$$|1\rangle|1\rangle|\Psi_1\rangle + |2\rangle|2\rangle|\Psi_2\rangle = (|1\rangle + |2\rangle)(|1\rangle + |2\rangle)|\Psi_{12}\rangle. \tag{5-1}$$

Seja $|\theta\rangle$ um estado tal que $\langle\theta|1\rangle = 1$ e $\langle\theta|2\rangle = 0$. Fazendo a contração $\theta \otimes \theta\rfloor\cdot$ com os dois lados de (5-1) obtemos $\Psi_1 = \Psi_{12}$. Por um argumento análogo temos $\Psi_2 = \Psi_{12}$ e disto concluímos que

$$|1\rangle|1\rangle + |2\rangle|2\rangle = (|1\rangle + |2\rangle)(|1\rangle + |2\rangle).$$

Fazendo a contração $\theta\rfloor\cdot$ com os dois lados desta última equação, concluímos que $|1\rangle = |1\rangle + |2\rangle$. Com isto terminamos a demonstração do teorema de não-clonagem, pois este resultado contradiz a hipótese de independência linear entre os vetores que supostamente poderiam ser clonados.

Voltando a nossa discussão sobre teleportação, é agora bastante claro que não é possível fazer várias cópias de um mesmo objeto, já que o estado original é sempre destruído para que obtenhamos informações a seu respeito. Na próxima seção, mostraremos finalmente como os cientistas contornaram este problema e puderam realizar em laboratório a experiência da teleportação.

Todas as experiências até hoje foram realizadas com partículas microscópicas e, embora não seja violada nenhuma lei fundamental, ninguém

espera ser possível teleportar pessoas ou objetos macroscópicos em um futuro próximo.

5.2.2 Utilização de Pares Emaranhados para Teleportar Estados Quânticos

Vamos adotar a descrição que é usualmente encontrada na literatura: suponhamos que Alice possui um qubit em um certo estado $|\psi\rangle$, e quer transferi-lo para Bob. Se ela soubesse descrever com precisão o estado de seu bit quântico, poderia corresponder-se com Bob através de um canal clássico (carta, telefone, etc.) e lhe passar toda a informação necessária para que ele preparasse um qubit exatamente equivalente ao dela. Entretanto, como vimos, se $|\psi\rangle$ for desconhecido, Alice não tem como obter toda a informação que precisa: qualquer medição altera o estado de seu qubit, e não é possível clonálo para medir as cópias.

O recurso que utilizaremos para teleportar este estado será o emaranhamento. Vamos supor que uma fonte produza um par emaranhado:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

onde o primeiro qubit é dado a Alice, e o segundo a Bob.

Escrevendo o estado $|\psi\rangle$ que queremos teleportar como $\alpha|0\rangle_a + \beta|1\rangle_a$, temos que o estado inicial do sistema composto pelos três qubits é dado por:

$$|\psi\rangle \otimes |\phi\rangle = (\alpha|0\rangle_a + \beta|1\rangle_a) \otimes \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b),$$

onde o índice a significa que o qubit pertence a Alice, e b, a Bob.

O primeiro passo para que a teleportação seja realizada é Alice aplicar a seguinte transformação unitária a seus dois qubits:

$$\begin{aligned}
|0\rangle_a|0\rangle_a &\mapsto |0\rangle_a|0\rangle_a \\
|0\rangle_a|1\rangle_a &\mapsto |0\rangle_a|1\rangle_a \\
|1\rangle_a|0\rangle_a &\mapsto |1\rangle_a|1\rangle_a \\
|1\rangle_a|1\rangle_a &\mapsto |1\rangle_a|0\rangle_a
\end{aligned}$$

ou, matricialmente,

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

O estado produzido é

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\ [\alpha|0\rangle_a(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b) + \beta|1\rangle_a(|1\rangle_a|0\rangle_b + |0\rangle_a|1\rangle_b)]\,.$$

Depois, Alice deve aplicar ao seu primeiro qubit outra transformação unitária:

$$|0\rangle_a \mapsto \frac{|0\rangle_a + |1\rangle_a}{\sqrt{2}}$$

$$|1\rangle_a \mapsto \frac{|0\rangle_a - |1\rangle_a}{\sqrt{2}}.$$

A matriz que a representa é:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

freqüentemente chamada *transformação de Hadamard*.

O estado do sistema é então transformado em:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2}}\ \left[\alpha\frac{(|0\rangle_a + |1\rangle_a)}{\sqrt{2}}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b) + \beta\frac{(|0\rangle_a - |1\rangle_a)}{\sqrt{2}}(|1\rangle_a|0\rangle_b + |0\rangle_a|1\rangle_b)\right] \\ &= \frac{1}{2}\ [|0\rangle_a|0\rangle_a(\alpha|0\rangle_b + \beta|1\rangle_b) + |1\rangle_a|0\rangle_a(\alpha|0\rangle_b - \beta|1\rangle_b) + \\ &\quad + |0\rangle_a|1\rangle_a(\alpha|1\rangle_b + \beta|0\rangle_b) + |1\rangle_a|1\rangle_a(\alpha|1\rangle_b - \beta|0\rangle_b)]\,. \end{aligned}$$

Assim, se Alice medir um observável deste estado na base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ e obtiver um autovalor associado a $|00\rangle$, utilizará um meio clássico para transmitir a Bob os dois bits de informação resultantes desta medição: 00. Dessa forma, ele terá certeza de que seu qubit encontra-se no estado $\alpha|0\rangle_b + \beta|1\rangle_b$, exatamente igual ao estado que Alice queria teleportar, $|\psi\rangle$.

Entretanto, Alice pode ainda obter 01, 10 e 11 como resultados. Nestes casos, o qubit de Bob encontra-se nos seguintes estados, respectivamente:

$$\begin{aligned} 01 &\mapsto \alpha|1\rangle_b + \beta|0\rangle_b \\ 10 &\mapsto \alpha|0\rangle_b - \beta|1\rangle_b \\ 11 &\mapsto \alpha|1\rangle_b - \beta|0\rangle_b \end{aligned}$$

Para cada um deles, Bob pode aplicar certas transformações unitárias a seu qubit para que seu estado seja igual a $|\psi\rangle$. De fato, se ele recebe os bits 01, deve aplicar

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

ou seja,

$$|0\rangle_b \mapsto |1\rangle_b$$

$$|1\rangle_b \mapsto |0\rangle_b.$$

Caso receba 10, a transformação é

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

logo,

$$|0\rangle_b \mapsto |0\rangle_b$$

$$|1\rangle_b \mapsto -|1\rangle_b.$$

E, finalmente, se for 11, Bob deve aplicar as duas transformações acima: primeiro X, depois Z.

Concluímos que, para teleportar um qubit, precisamos transmitir na verdade apenas dois bits clássicos de informação.