A **criptografia quântica** é um afluente em desenvolvimento da criptografia que utiliza os princípios da Mecânica Quântica para garantir uma comunicação segura. Com ela, emissor e receptor podem criar e partilhar uma chave secreta para criptografar e decifrar suas mensagens.

A criptografia quântica destaca-se face aos outros métodos criptográficos por não necessitar de comunicações secretas prévias, permitir a detecção de intrusos e ser segura mesmo que o intruso possua um poder computacional ilimitado. Na verdade, ela é totalmente segura, exceto nas situações em que o intruso consiga remover e inserir mensagens do canal de transmissão (poder ler e remover a mensagem, criar uma cópia e reenviá-la). Assim, esta técnica criptográfica seria mais segura que as utilizadas atualmente, pois se baseia em leis da física, enquanto as atuais asseguram os dados com base em funções que são secretas somente porque o poder computacional é limitado.

É importante observar que a criptografia quântica só será utilizada para produzir e distribuir as chaves, não para transmitir a mensagem. A chave gerada poderá ser utilizada com qualquer algoritmo de criptografia escolhido. O algoritmo mais comumente associado com a criptografia quântica é o one-time pad, pois ele tem comprovadamente uma segurança perfeita quando usado com uma chave aleatória e do mesmo tamanho que a mensagem.

One-time pad consiste num algoritmo em que o purotexto é combinado, caractere por caractere, a uma chave secreta aleatória que para isso deve ter, no mínimo, o mesmo número de caracteres do purotexto. Para garantir que a criptografia seja imperscrutável, a chave só deve ser usada uma única vez, sendo imediatamente destruída após o uso.

Distribuição de Chaves Quânticas

Para compreender este Sistema de Distribuição de Chaves são necessários alguns conhecimentos de Mecânica Quântica. Esta ciência nos diz que as partículas não existem num estado quântico específico, mas sim em vários estados ao mesmo tempo, com diferentes probabilidades de estarem em cada um caso alguém as observe. O Princípio da Incerteza de Heisenberg garante-nos não ser possível determinar em simultâneo todos os estados físicos de uma partícula sem interferir na mesma, alterando-a de forma inegável. A comunicação quântica envolve criptografar informação em estados quânticos, ou qubits, ao invés dos bits usados na comunicação clássica. Normalmente, fótons ou fotões são usados como qubits.

A criptografia quântica explora certas propriedades desses estados quânticos para garantir sua segurança. Existem diferentes formas de distribuição de chaves quânticas, mas elas podem ser divididas em duas categorias principais, dependendo de qual propriedade ela utiliza.

Protocolos de Preparar e Medir

Diferente da física clássica, o ato de medir é parte importante da mecânica quântica. Em geral, medir um estado quântico desconhecido irá modificar aquele estado de alguma forma. Isso pode ser explorado de forma a detectar um espião na comunicação, que necessariamente terá que medir um estado quântico e acabará por alterá-lo.

Protocolos baseados em Emaranhamento Quântico

O estado quântico de dois (ou mais) objetos separados pode se tornar ligado de uma tal maneira que eles têm que ser descritos como um estado quântico emaranhado, não como

objetos individuais. Isso é conhecido como emaranhamento quântico e significa, por exemplo, que realizar uma medida em um objeto irá afetar o outro. Se um par de objetos emaranhados é compartilhado por emissor e receptor, qualquer pessoa tentando interceptar uma das partículas irá alterar todo o sistema, permitindo que sua presença seja detectada.

Protocolo BB84

Esse protocolo, conhecido como BB84 em função de seus inventores e do ano de publicação, foi originalmente descrito utilizando os estados de polarização dos fótons para transmitir a informação. Ao trocarem entre as suas várias posições possíveis, os fótons vibram e se, num grupo de fótons, todos vibram na mesma direção, então eles estão polarizados. Utilizando filtros polarizadores é possível restringir a passagem aos fótons polarizados numa determinada direção, bloqueando os restantes. Para medir a polarização de um fóton são utilizadas bases de medida, que são compostas por duas direções que façam um ângulo reto. Por exemplo: horizontal e vertical, ou diagonal à esquerda e à direita. No entanto, quaisquer dois pares de variáveis conjugadas pode ser utilizado para o protocolo.

Os estados de polarização mais utilizados são:

- Base retilínea com vertical (0°) e horizontal (90°),
- Base diagonal com os ângulos de 45° e 135°
- Base circular com a direita e esquerda, seguindo a regra da mão direita.

Base	0	1
+	↑	→
×	↗	↘

O Emaranhamento Quântico

O **emaranhamento** (ou entrelaçamento quântico) é um fenômeno no qual duas ou mais partículas ficam intrinsecamente ligadas, de modo que o estado quântico de cada partícula não pode ser descrito independentemente do estado das outras, mesmo que estejam separadas por vastas distâncias.

- **"Ação fantasmagórica à distância"**: Albert Einstein referiu-se a isso como "ação fantasmagórica à distância" porque a medição do estado de uma partícula instantaneamente determina o estado da(s) outra(s), independentemente da separação espacial entre elas.
- **Correlação Perfeita**: As propriedades das partículas emaranhadas (como spin ou polarização) são perfeitamente correlacionadas.

A Superposição Quântica

A **superposição** é a capacidade de um sistema quântico existir em múltiplos estados possíveis simultaneamente, até que seja medido.

- **Exemplo do "Gato de Schrödinger"**: O famoso experimento mental do Gato de Schrödinger ilustra esse conceito, onde um gato hipotético dentro de uma caixa estaria simultaneamente vivo e morto até que a caixa fosse aberta e seu estado observado.
- **Bits Quânticos (Qubits)**: Na computação quântica, essa propriedade é crucial. Um bit clássico pode ser 0 ou 1, mas um qubit (bit quântico) pode ser 0, 1, ou uma superposição de 0 e 1 ao mesmo tempo, permitindo que os computadores quânticos processem enormes quantidades de informação paralelamente.
- **Colapso da Função de Onda**: O estado de superposição é mantido enquanto o sistema não é observado. No momento da medição, o sistema "colapsa" para um estado definido (por exemplo, o gato é encontrado vivo ou morto).

O "Apocalipse Quântico" é um termo popular usado para descrever o **potencial impacto devastador que computadores quânticos avançados poderão ter na segurança da informação global**, especificamente na criptografia de dados atual.

Significado

- **Quebra de Criptografia Atual:** A maioria dos sistemas de segurança online (como transações bancárias, comunicações governamentais e dados pessoais) baseia-se em métodos de criptografia que seriam extremamente difíceis ou levariam milhares de anos para serem decifrados por computadores clássicos. No entanto, um computador quântico suficientemente poderoso poderia quebrar esses códigos em uma fração de tempo muito menor (de horas para segundos, em alguns casos), usando algoritmos específicos.
- **"Q-Day":** Esse cenário é por vezes referido como o "Q-Day" (Quantum Day, ou Dia Quântico).
- **Ameaça à Confidencialidade:** Se isso acontecesse, arquivos secretos criptografados, comunicações confidenciais e a segurança de infraestruturas críticas poderiam ser comprometidos e revelados.

Preocupação e Soluções

Apesar do nome alarmante, a preocupação com o "apocalipse quântico" é um fator motivador para o desenvolvimento de novas tecnologias de segurança:

- **Criptografia Pós-Quântica:** Pesquisadores e empresas, como o Google e o Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA, estão trabalhando no desenvolvimento de novos padrões de criptografia (chamada criptografia pós-quântica ou "quantum-safe") que sejam resistentes a ataques de computadores quânticos.
- **Preparação Contínua:** A transição para esses novos métodos de segurança já está em andamento, como medida preventiva para proteger dados no futuro.