Protocolos de QKD

Criptografia Quântica

A criptografia quântica envolve técnicas de segurança baseadas em fenômenos quânticos. Sua principal aplicação é a Distribuição de Chaves Quânticas (QKD), é usada para garantir a segurança na troca de chaves criptográficas. Além disso, existem métodos como "cara ou coroa"(quantum key tossing) quântico e Transferência Inconsciente (oblivuous transfer), que também exploram princípios quânticos para a segurança de informações.

Distribuição de Chaves Quânticas (QKD)

A Distribuição de Chaves Quânticas (Quantum Key Distribution,QKD) tem o objetivo de gerar e transmitir com segurança uma chave secreta, normalmente para o uso de apenas duas pessoas. A comunicação durante o processo de criação da chave é feita em um canal quântico, e outra parte em um canal clássico, as mensagens quânticas são impossíveis de medir totalmente ou serem copiadas(clonar) uma função de onda. Dessa forma, enquanto a criptografia clássica preconiza que sempre é possível interceptar uma mensagem sem ser percebido, a criptografia quântica permite protocolos em que isto é impossível.

EXEMPLO:

Imagine que você e seu amigo têm um segredo e querem conversar de maneira segura para que ninguém mais entenda. Vocês decidem usar uma chave especial para codificar suas mensagens. Mas há um problema: se alguém pegar essa chave, poderá ouvir suas conversas secretas.
Na criptografia normal, se alguém pega a chave, pode usá-la para entender o que vocês estão dizendo. Isso é como um espião que escuta suas conversas sem você perceber.
Aqui é onde entra a criptografia quântica. Ela usa a física das coisas bem pequenas (chamadas partículas quânticas) para resolver esse problema. Quando você envia a chave usando essas partículas, se alguém tentar pegá-las para ouvir, elas vão mudar de uma forma que todos vão notar. É como se as partículas se assustassem e contassem para vocês que alguém está tentando ouvir.
Então, usando a criptografia quântica, você e seu amigo podem saber se alguém está tentando escutar suas conversas secretas. Isso torna muito mais difícil para os espiões ficarem de olho nas suas mensagens, porque eles não podem pegar a chave sem que vocês percebam. É como se a chave tivesse um alarme embutido que dispara quando alguém tenta mexer nela.

A criptografia quântica usa partículas de luz chamadas fótons, nas mensagens. Esses fótons podem ser "girados" de diferentes maneiras, chamamos de polarizações. E não precisam estar exatamente alinhados.
O truque é escolher como ler esses fótons, para criar uma incerteza de como eles serão lidos. Isso acontece porque há várias maneiras de como ler eles.
Essa incerteza é o que torna difícil de alguém roubar os fótons e entender as mensagens codificadas. A escolha de como ler os fótons é como uma senha que só quem sabe pode entender as mensagens. No entanto, essa forma de trocar mensagens é um pouco mais lenta e complicada.
Então, para ter mais segurança, aceitamos que o processo seja um pouco mais devagar. Mas essa segurança extra torna quase impossível que alguém roube as mensagens enquanto estão sendo enviadas.

Protocolo BB84

Considere que Amanda e Bruno criam uma senha secreta conforme o protocolo BB84. Para isso, Amanda e Bruno se comunicam por um canal quântico, utilizando a polarização do fóton para codificar o bit, seja na base retilínea de polarização (horizontal ou vertical) ou na base diagonal (diagonal +45º ou diagonal -45º). Para medir a polarização do fóton precisamente (com 100% de certeza), o detector deve utilizar a mesma base, caso contrário, vai haver apenas 50% de probabilidade de acerto.

Neste protocolo, Amanda gerará uma sequência aleatória de bits (0 ou 1) e uma sequência aleatória de bases (retilínea ou diagonal), e ela enviará os fótons para o Bruno contendo estes bits em suas respectivas bases. No entanto, Bruno não sabe em qual base os fótons foram enviados, então ele vai gerar uma sequência de bases aleatórias para o detector. Após a comunicação, Amanda e Bruno anunciam as bases utilizadas e são mantidos apenas os bits que utilizaram a mesma base para enviar e detectar. Logo, há uma eficiência de 50%.

“Cara ou Coroa” quânticos

Amanda e Bruno, querem jogar "cara ou coroa" mesmo estando longe. Amanda escolhe uma maneira secreta de jogar a moeda e envia fótons para Bruno, que mandam as escolhas dela.

Bruno recebe esses fótons e tenta adivinhar como Amanda jogou a moeda para cada fóton.

Amanda conta a Bruno se ele acertou ou errou, mas para garantir que Bruno não trapaceou, Amanda envia a sequência original das jogadas de moeda.

Bruno confere as respostas dele com as jogadas originais de Amanda. Se tudo estiver certo, significa que ninguém trapaceou.

Dessa forma, eles podem jogar o jogo à distância e verificar se tudo foi justo, usando a luz de maneira especial para manter tudo certo e seguro.

Para que o trapaceio seja impossível, tanto Amanda quanto Bruno precisam fazer coisas que não podem ser feitas facilmente.

Bruno trapaceando: Bruno não pode acertar adivinhando a base que Amanda usou com uma chance maior que 50%. Isso é difícil porque ele teria que prever como Amanda escolheu para cada fóton, e isso é impossível.

Amanda trapaceando: Amanda também não pode mentir sobre a base que usou para Bruno. Bruno vai verificar os resultados das duas sequências, e a mentira de Amanda seria pega.

Outra tentativa de Amanda: Amanda poderia mandar cada bit em uma base diferente, mas ainda assim não poderia responder com uma base e sequência que faça todos os bits que Bruno mediu naquela base coincidirem com o que Amanda enviou.

Usando o efeito EPR para trapacear: A tentativa de trapaceio usando o efeito EPR também não funciona. Isso ocorre porque, se Bruno acerta na primeira medição, a segunda medição de Amanda sobre o fóton guardado será oposta ao resultado que Bruno obteve, e isso seria estranho.

Portanto, o protocolo BB84 é projetado para que, em cada tentativa de trapacear, a situação se torna complicada e as contradições aparecem, garantindo que o sistema seja seguro.

Transferência Inconsciente

Arinaldo e Baica não confiam um no outro. Eles querem compartilhar informações sem contar coisas demais uma para o outro. Arinaldo é o que envia as mensagens, e Baica é quem recebe.

A ideia é que Arinaldo envia duas mensagens exatamente iguais para Baica. Mas há uma reviravolta: Arinaldo só tem uma chance de 50% de realmente enviar cada mensagem. Se pelo menos uma mensagem for enviada com sucesso, só Baica vai saber.

Isso é criado para que Arinaldo e Baica possam resolver problemas juntos sem contar tudo um para o outro. Eles não precisam de uma pessoa extra para ajudar. É como se eles pudessem compartilhar coisas importantes enquanto mantêm outras partes em segredo.
Na computação clássica tem vários protocolos de transferência inconsciente, que utilizam criptografia assimétrica, mas eles só conseguem garantir a segurança contra-ataques externos ou trapaças a um dos participantes desta comunicação. Já os protocolos quânticos de OT são capazes de garantir um alto grau de confiabilidade para os dois participantes da comunicação.
Neste jeito de trocar informações, Arinaldo faz algo especial com duas partículas pequeninas. Ele as envia para o Baica. Baica decide se vai medir as partículas em um jeito ou em outro. Depois, Baica conta a Arinaldo se as medições deram certo. Se não deram certo, Arinaldo manda de novo as partículas e Baica tenta outra vez. Se tudo der certo, Arinaldo descobre como Baica mediu as partículas.
Isso é feito para que Arinaldo e Baica possam compartilhar informações importantes sem contar tudo. Eles usam a maneira como as partículas se comportam para fazer isso.
Esse jeito de trocar informações é muito seguro. Se Baica tentar trapacear medindo as partículas de maneiras diferentes, suas chances de sucesso são muito, muito baixas. Baica também não pode trapacear guardando as partículas antes do último passo, porque isso não funciona.
Alguns pensam em usar algo chamado EPR para melhorar ainda mais a segurança, mas isso não é possível com a tecnologia de hoje.

Simplificação de cada protocolo

Distribuição de chave quântica (QKD*): é um método de comunicação seguro que implementa um protocolo criptográfico envolvendo componentes da mecânica quântica. Ele permite que duas partes produzam uma chave secreta aleatória compartilhada conhecida apenas por elas, que pode ser usada para criptografar e descriptografar mensagens.*
Protocolo BB84*: usam os estados de polarização de fótons para transmitir as informações. O remetente (tradicionalmente chamado de Amanda) e o receptor (Bruno) são conectados por um canal de comunicação quântica que permite a transmissão de estados quânticos. No caso dos fótons, esse canal é geralmente uma fibra óptica ou simplesmente espaço livre. Além disso, eles se comunicam através de um canal clássico público, por exemplo, usando transmissão radiofônica ou a Internet.*
Protocolo de "Cara ou Coroa" Quântico*:* é uma forma de usar partículas pequenas, como elétrons, para tomar decisões. Você e outra pessoa têm cada uma uma partícula. Vocês decidem juntos qual propriedade da partícula medir, mas não contam um ao outro o resultado. Se os resultados forem os mesmos, vocês fazem uma escolha. Se forem diferentes, vocês podem fazer outra coisa. A coisa interessante é que, por causa das regras quânticas, os resultados sempre serão iguais, mesmo que as partículas estejam em estados diferentes antes da medição. Isso torna a decisão um pouco como jogar "cara ou coroa", mas usando as coisas estranhas da física quântica.
P**rotocolo de Oblivious Transfer (Transferência Inconsciente)**: é um método de comunicação onde um remetente envia várias informações para um receptor, mas o remetente não sabe qual informação o receptor recebeu. Isso protege a privacidade e é usado em segurança da informação.
Protocolo E91: usa pares emaranhados de fótons. Estes podem ser criados por Amanda, por Bruno ou por alguma fonte separada de ambos, os fótons são distribuídos para que Amanda e Bruno terminem com um fóton de cada par.