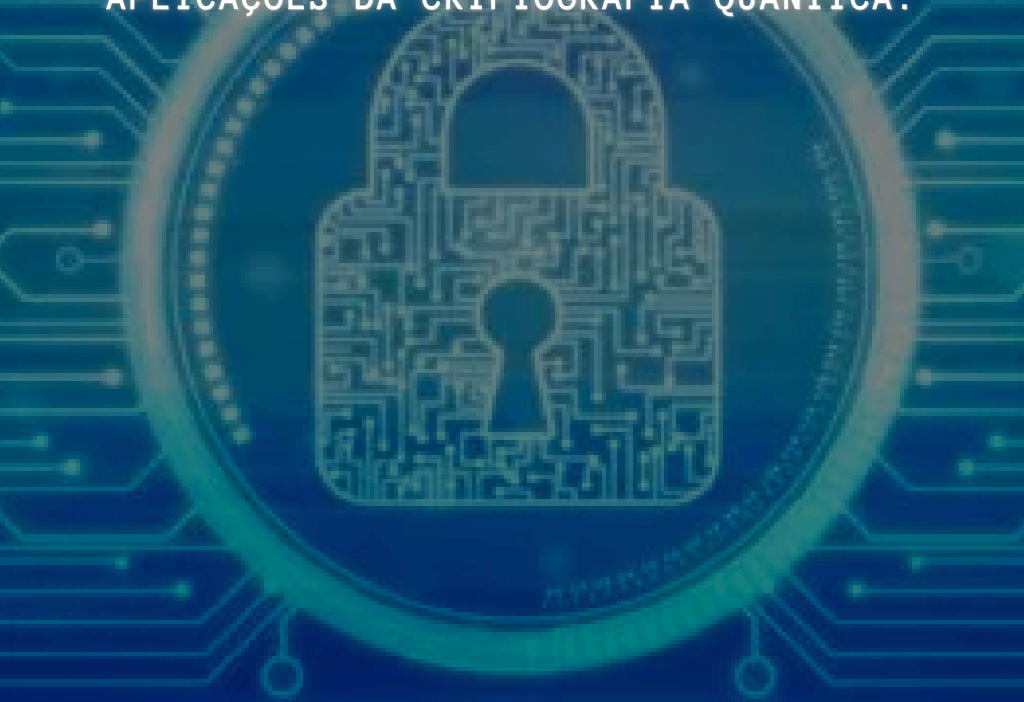
CRIPTOGRAFIA QUÂNTICA

ANÁLISE DOS PRINCÍPIOS, DESAFIOS E APLICAÇÕES DA CRIPTOGRAFIA QUÂNTICA.



Maxwell Pereira Lima
Noemi Soares Gonçalves da Silva

Ânima Educação

Criptografia Quântica:

Análise dos Princípios, Desafios e Aplicações da Criptografia Quântica.

Conceitos & Aplicações

Maxwell Pereira Lima - 12522226066
Noemi Soares Gonçalves Da Silva - 1352315604

Atenciosamente,
Maxwell Pereira Lima
Noemi Soares Gonçalves Da Silva

Dedicamos este eBook a todas as pessoas dedicadas à pesquisa, sobre a criptografia quântica. Aos profissionais, engenheiros, acadêmicos e cientistas que trabalham incansavelmente para impulsionar o campo da engenharia quântica e encontrar soluções inovadoras para os desafios do mundo real.

Expressamos nossa profunda gratidão aos nossos colegas, mentores e colaboradores, cujo conhecimento e orientação têm sido essenciais em nossa jornada de aprendizado sobre a criptografia quântica.

Por fim, gostaríamos de agradecer a todos os leitores que generosamente dedicaram seu tempo e esforço para explorar este eBook. Esperamos que você encontre informações valiosas e seja inspirado a continuar explorando o fascinante mundo das criptografia quântica.

Este eBook é dedicado a todos vocês, que estão moldando o futuro da ciência e da tecnologia com sua dedicação e entusiasmo.

Atenciosamente,
Maxwell Pereira Lima
Noemi Soares Gonçalves Da Silva

Sumário

Introdução

A segurança da informação é um tema de grande importância no mundo atual, onde os dados digitais são cada vez mais presentes em nossas vidas. Com o aumento do número de dispositivos conectados à internet e o crescimento exponencial da quantidade de informações armazenadas em nuvens, bancos de dados e dispositivos móveis, torna-se essencial garantir a proteção dessas informações contra invasões e ataques maliciosos.

Nesse contexto, a criptografia é uma técnica fundamental para a segurança da informação. A criptografia consiste em transformar uma mensagem original em uma mensagem cifrada, que só pode ser lida por quem possui a chave correta para decifrála. Existem diferentes técnicas de criptografia, mas a maioria delas é baseada em algoritmos e chaves criptográficas.

A criptografia clássica é uma técnica de criptografia que se baseia em algoritmos matemáticos para cifrar e decifrar mensagens. Esses algoritmos são conhecidos por todos, e a segurança da criptografia clássica depende da complexidade do algoritmo e do tamanho da chave criptográfica. No entanto, mesmo com chaves longas e algoritmos complexos, a criptografia clássica pode ser quebrada por ataques de força bruta ou por algoritmos quânticos.

A criptografia quântica, por sua vez, é uma técnica de criptografia que se baseia nas leis da física quântica para proteger dados. Diferentemente da criptografia clássica, que se baseia na matemática e em algoritmos, a criptografia quântica utiliza partículas subatômicas para codificar e decodificar informações. Essa técnica é considerada inquebrável, pois qualquer tentativa de interceptar as partículas alteraria seu estado quântico, o que seria detectado pelo receptor.

Nos próximos tópicos, serão apresentados mais detalhes sobre como funciona a criptografia quântica e quais são os avanços recentes nessa área de pesquisa.

Conceito

A criptografia quântica se baseia na utilização de partículas subatômicas, como fótons, para transmitir informações. Essas partículas têm propriedades quânticas, como polarização e entrelaçamento, que são utilizadas para codificar e decodificar informações.

A ideia básica da criptografia quântica é que o emissor e o receptor compartilhem uma chave criptográfica quântica, que é formada por um conjunto de partículas subatômicas. Essas partículas são enviadas pelo emissor ao receptor, através de um canal quântico, que pode ser uma fibra óptica ou um sistema de comunicação sem fio.

Para garantir a segurança da chave criptográfica quântica, o emissor e o receptor utilizam um protocolo de criptografia quântica, que envolve a troca de informações e testes de segurança. Esse protocolo garante que qualquer tentativa de interceptar as partículas quânticas será detectada, pois a medida das partículas alteraria seu estado quântico.

Uma vez que o emissor e o receptor compartilham a chave criptográfica quântica, eles podem utilizar essa chave para cifrar e decifrar mensagens. A mensagem original é transformada em um conjunto de bits quânticos, que são enviados pelo emissor ao receptor através do canal quântico. O receptor utiliza a chave criptográfica para decifrar a mensagem, obtendo assim a mensagem original.

A criptografia quântica oferece segurança sofisticada, pois qualquer tentativa de interceptação das partículas quânticas alteraria seu estado quântico, o que seria detectado pelo receptor. Além disso, a criptografia quântica é imune a ataques de força bruta ou a algoritmos quânticos, pois a segurança da criptografia quântica depende das leis da física quântica.

Estrutura

A estrutura da criptografia quântica é baseada em dois conceitos principais: distribuição de chaves quânticas e criptografia de chave pública.

A distribuição de chaves quânticas é uma técnica que permite que duas partes comuniquem entre si de forma segura, compartilhando uma chave secreta que é usada para codificar e decodificar as mensagens. Esse processo é realizado por meio de um canal de comunicação quântica, que é protegido por leis da física quântica. O canal quântico é capaz de detectar qualquer tentativa de interceptação ou espionagem, tornando impossível que a chave compartilhada seja roubada ou duplicada.

Já a criptografia de chave pública é baseada na utilização de pares de chaves distintas: uma chave pública, que é distribuída livremente, e uma chave privada, que é mantida em sigilo pelo proprietário. A chave pública é usada para criptografar as mensagens, enquanto a chave privada é usada para decodificar as mensagens criptografadas. Diferentemente da distribuição de chaves quânticas, a criptografia de chave pública pode ser realizada em canais de comunicação clássicos, como a internet.

Fluxo

Nos últimos anos, tem havido um grande avanço na pesquisa em criptografia quântica, tanto em termos teóricos quanto práticos. Uma das principais áreas de pesquisa é o desenvolvimento de protocolos de criptografia quântica mais eficientes e seguros.

Um exemplo recente é o protocolo de criptografia quântica baseado em distribuição de chaves por medição aleatória (random measurement basis), proposto por Zhong et al. em 2021. Esse protocolo utiliza medições aleatórias para proteger a chave criptográfica quântica contra-ataques de interceptação baseados em medições.

Outro avanço recente é a utilização de redes de comunicação quântica para a transmissão de informações seguras. Essas redes permitem a distribuição de chaves criptográficas quânticas a longas distâncias, o que é essencial para aplicações práticas da criptografia quântica.

É importante ressaltar novamente que principal diferença entre a criptografia quântica e a criptografia clássica é a base teórica utilizada por cada uma delas. A criptografia clássica é baseada em algoritmos matemáticos, enquanto a criptografia quântica é baseada nas leis da física quântica. Isso significa que a criptografia quântica é inquebrável, enquanto a criptografia clássica pode ser quebrada por ataques de força bruta ou por algoritmos quânticos, porém existem detalhes a serem considerados, estes serão abordados nos próximos capítulos.

Prova da Eficiência da Criptografia Quântica

Para demonstrar a eficiência da criptografia quântica, podemos utilizar o protocolo de criptografia BB84, proposto por Charles Bennett e Gilles Brassard em 1984. Esse protocolo utiliza um conjunto de partículas quânticas para a distribuição de chaves criptográficas quânticas, e é considerado inquebrável.

Suponha que Alice e Bob queiram trocar mensagens seguras utilizando o protocolo BB84. Alice envia uma chave criptográfica quântica para Bob, que a utiliza para cifrar e decifrar mensagens. Para testar a eficiência da criptografia quântica, vamos compará-la com a criptografia clássica.

Na criptografia clássica, a segurança depende do tamanho da chave criptográfica. Para garantir uma segurança semelhante à da criptografia quântica, seria necessário utilizar uma chave criptográfica com pelo menos 256 bits. Essa chave teria um tamanho de cerca de 10^77 possibilidades. Isso equivale a um número com mais de 77 dígitos decimais, o que é um número extremamente grande. No entanto, na teoria um

adversário com acesso a um supercomputador poderia testar todas as possibilidades de chave criptográfica. Embora seja verdade que um supercomputador teria a capacidade de testar todas as possibilidades de uma chave criptográfica de 256 bits, isso não é viável na prática. Mesmo os supercomputadores mais poderosos que existem atualmente levariam bilhões de anos para realizar essa tarefa.

Para se ter uma ideia, a atual chave de criptografia mais forte utilizada em larga escala é de 256 bits, que é considerada segura o suficiente para proteger informações confidenciais por um longo período de tempo. Mesmo que um adversário possa teoricamente quebrar essa chave, na prática isso é considerado inviável.

Além disso, os sistemas de criptografia modernos não dependem apenas do tamanho da chave, mas também de outros fatores, como a complexidade do algoritmo de criptografia e a segurança do processo de geração de chaves. Portanto, a segurança da criptografia moderna não pode ser reduzida apenas ao tamanho da chave.

Em resumo, embora seja verdade que um supercomputador teoricamente poderia testar todas as possibilidades de uma chave criptográfica de 256 bits, na prática isso é inviável e a segurança da criptografia moderna não pode ser reduzida apenas ao tamanho da chave.

Se um supercomputador com o poder de processamento de 1,5 EXAFLOPS pudesse testar 1 bilhão de chaves por segundo, ele levaria aproximadamente 6,7 x 10^45 anos para testar todas as possibilidades de uma chave criptográfica de 256 bits.

Isso é ainda mais tempo do que o tempo estimado para o universo existir, que é de aproximadamente 13,8 bilhões de anos. Portanto, mesmo com um supercomputador extremamente poderoso, que pode processar muito mais operações por segundo do que o atualmente disponível, ainda seria inviável quebrar uma chave criptográfica de 256 bits por meio de força bruta. 6,7 x 10^45 é um número extremamente grande. Em notação decimal, ele é escrito como:

a67 seguido de 44 zeros:
67.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000

Isso é muito maior do que o número de átomos no universo observável, que é estimado em cerca de 10^80.

Atualmente, considera-se que a criptografia baseada em algoritmos de chave pública é a mais avançada e segura disponível. Essa criptografia é conhecida como criptografia assimétrica, pois utiliza um par de chaves diferentes para criptografar e descriptografar dados.

O par de chaves consiste em uma chave pública, que pode ser compartilhada livremente, e uma chave privada, que é mantida em segredo pelo proprietário da chave. A criptografia de chave pública é usada em muitos sistemas de segurança, como a comunicação segura na internet, a assinatura digital de documentos, e a autenticação de usuários.

Um dos algoritmos de criptografia de chave pública mais amplamente utilizados é o RSA (Rivest-Shamir-Adleman), que foi inventado na década de 1970 e continua sendo amplamente usado hoje em dia. Outros algoritmos de chave pública populares incluem o Diffie-Hellman, o ElGamal, e o ECC (Elliptic Curve Cryptography).

Embora a criptografia de chave pública seja muito segura, ela ainda pode ser vulnerável a ataques de lado-chave e ataques de canal lateral. Portanto, a criptografia de chave pública é frequentemente combinada com outras técnicas de segurança, como a autenticação de usuário e o gerenciamento de chaves seguras, para fornecer proteção adicional contra-ataques.

O AES é um algoritmo de criptografia simétrica, enquanto o RSA é um algoritmo de criptografia assimétrica.

O AES é amplamente utilizado para criptografar dados em trânsito e em repouso, como em sistemas de armazenamento e transmissão de arquivos. Ele é mais rápido do que o RSA e é adequado para criptografar grandes quantidades de dados, sendo considerado um dos algoritmos de criptografia mais seguros atualmente disponíveis.

Por outro lado, o RSA é mais adequado para a criptografia de chaves e para a autenticação digital. Ele é usado para criptografar chaves de criptografia simétricas e para assinar digitalmente documentos, e-mails e outros tipos de comunicação digital. O RSA é mais lento do que o AES, mas é mais flexível e é considerado um dos algoritmos de criptografia assimétrica mais seguros atualmente disponíveis.

Em resumo, tanto o AES quanto o RSA são algoritmos de criptografia seguros e eficientes, e a escolha entre eles dependerá do propósito específico da criptografia. É comum usar o AES para criptografar dados em trânsito e em repouso, enquanto o RSA é usado para criptografia de chaves e autenticação digital.

AES (Advanced Encryption Standard) e RSA (Rivest–Shamir–Adleman) são algoritmos de criptografia diferentes, que se diferem na forma como criptografam e descriptografam informações. O AES é um algoritmo de criptografia simétrica, o que significa que ele utiliza a mesma chave para criptografar e descriptografar informações. Ele é amplamente utilizado para criptografar dados em trânsito e em repouso, como em sistemas de armazenamento e transmissão de arquivos. O AES divide os dados a serem criptografados em blocos de 128 bits e usa a chave de criptografia simétrica de 128, 192 ou 256 bits para transformar cada bloco de dados em um bloco criptografado correspondente. O AES é um dos algoritmos de criptografia mais seguros atualmente disponíveis e é resistente a muitos tipos de ataques criptográficos, incluindo ataques de força bruta e ataques diferenciais. Já o RSA é um algoritmo de criptografia assimétrica, que utiliza uma chave pública para criptografar as informações e uma chave privada correspondente para descriptografá-las. Ele é amplamente utilizado para a criptografia de chaves e para a autenticação digital. O RSA é mais lento do que o AES, mas é mais flexível e é considerado um dos algoritmos de criptografia assimétrica mais seguros atualmente disponíveis. O RSA é frequentemente usado para criptografar chaves de criptografia simétrica e para assinar digitalmente documentos, e-mails e outros tipos de comunicação digital.

A criptografia de chave pública (como RSA) e a criptografia de chave simétrica (como o AES) são vulneráveis a ataques de computação quântica, que podem quebrar as chaves em um tempo muito mais curto do que os computadores clássicos.

Um computador quântico poderoso com milhares ou milhões de qubits e correção de erros poderia executar um algoritmo de Shor para fatorar números inteiros grandes ou realizar ataques de busca Grover em chaves simétricas, reduzindo significativamente o tempo necessário para quebrar as chaves criptográficas.

Para uma chave criptográfica de 256 bits, um computador quântico de grande porte poderia quebrá-la em questão de horas ou até minutos. No entanto, ainda não há um computador quântico o suficientemente poderoso para executar esses algoritmos em chaves criptográficas de tamanho real. Atualmente, os computadores quânticos existentes têm cerca de 100 qubits e são propensos a erros, tornando-os inadequados para tarefas de criptografia. Para a criptografia de chave pública, o algoritmo RSA é vulnerável a ataques de computação quântica por meio do algoritmo de Shor. O algoritmo RSA depende da dificuldade de fatorar um grande número composto em seus dois fatores primos para quebrar a chave. Com um computador quântico capaz de executar o algoritmo de Shor, o fatoramento de números inteiros grandes pode ser executado em tempo polinomial, que é muito mais rápido do que os melhores algoritmos clássicos conhecidos.

Podemos expressar a vulnerabilidade do RSA à computação quântica por meio da equação:

$$T_{shor}(N) = O((\log N)^3) * poly(\log N)$$

Onde $T_{shor}(N)$ representa o tempo necessário para executar o algoritmo de Shor em um número inteiro grande N. O tempo de execução é determinado pelo logaritmo do número de bits do número inteiro. A função poly(log N) representa um polinômio de grau constante em log N.

Para a criptografia de chave simétrica, o algoritmo AES é vulnerável a ataques de busca quântica por meio do algoritmo de Grover. O ataque de busca Grover pode encontrar uma chave em um tempo quadrático em relação ao número de bits da chave, o que é uma redução significativa em comparação com o tempo exponencial necessário para forçar a chave por força bruta em um computador clássico.

Podemos expressar a vulnerabilidade do AES à computação quântica por meio da equação:

$$T\_grover(N) = O(sqrt(N))$$

Onde T_grover(N) representa o tempo necessário para executar o algoritmo de busca de Grover em uma chave com N bits. O tempo de execução é determinado pelo número de bits da chave. A função O(sqrt(N)) indica que o tempo de execução aumenta proporcionalmente à raiz quadrada do número de bits da chave.

O ponto principal de supremacia da criptografia quântica em relação à criptografia clássica é que a criptografia quântica usa propriedades fundamentais da mecânica quântica, como a incerteza e a impossibilidade de clonagem de estados quânticos, para garantir a segurança da transmissão de informações. Por outro lado, a criptografia clássica depende da dificuldade computacional de quebrar algoritmos criptográficos.

O ponto fraco da criptografia clássica é a possibilidade de um adversário usar ataques de força bruta para quebrar a chave de criptografia. Um ataque de força bruta consiste em tentar todas as possíveis chaves até encontrar a chave correta. A segurança da criptografia clássica depende do tamanho da chave e da dificuldade de realizar esse tipo de ataque. Por outro lado, a criptografia quântica é imune a ataques de interceptação passiva, pois a medida de um estado quântico altera seu estado, impedindo que um adversário obtenha informações sem perturbar o estado quântico original. Além disso, a impossibilidade de clonar estados quânticos impede que um adversário obtenha uma cópia do estado quântico

original para realizar ataques offline.

Para provar matematicamente o ponto fraco da criptografia clássica, podemos usar a teoria da informação e a entropia de Shannon. A entropia da chave de criptografia é dada por:

$$H(K) = -\Sigma\, p(k) \log_2 p(k)$$

Onde p(k) é a probabilidade de ocorrência de cada chave k.

O espaço de chaves é dado por $|K| = 2^n$, onde n é o tamanho da chave em bits. Se um adversário usar um ataque de força bruta para quebrar a chave de criptografia, ele precisará testar todas as 2^n possíveis chaves. A probabilidade de a chave correta ser a k-ésima chave testada é:

$$p(k) = 1/2^n$$

Assim, a entropia da chave de criptografia é dada por:

$$H(K) = -\Sigma\, (1/2^n) \log_2 (1/2^n) = n$$

Isso significa que, para garantir a segurança da criptografia clássica, o tamanho da chave deve ser grande o suficiente para que o espaço de chaves seja grande o suficiente para tornar impraticável um ataque de força bruta.

Por outro lado, na criptografia quântica, a segurança é garantida pela impossibilidade de um adversário obter informações sem perturbar o estado quântico original. Para provar matematicamente isso, podemos usar a desigualdade de Heisenberg, que estabelece uma relação entre a incerteza na medida de uma observável quântica e a perturbação no estado quântico.

Materiais e Métodos

Materiais Que Poderiam Ser Utilizados Para Estudos Sofisticados:

Alguns exemplos são:

- Fontes de fótons individuais: dispositivos que emitem fótons únicos, necessários para a transmissão segura de informações quânticas.

- Detectores de fótons: dispositivos que detectam fótons individuais, essenciais para a leitura e processamento das informações transmitidas.

- Fibra óptica: é utilizada para a transmissão de fótons entre os dispositivos e sistemas.

- Geradores de estados quânticos: dispositivos que geram estados quânticos para a transmissão de informações seguras.

- Sistemas ópticos e eletrônicos para a implementação dos protocolos de criptografia quântica.

Formulação do Problema

Com o aumento do número de dispositivos conectados à internet e a crescente importância dos dados digitais, torna-se cada vez mais difícil garantir a proteção dessas informações. A criptografia quântica surge como uma alternativa promissora para resolver esse problema, porém ainda há muitas dúvidas sobre como essa tecnologia funciona e como ela pode ser utilizada.

Protocolos Utilizados e Avanços da Área

1. Protocolo E91: Esse protocolo foi desenvolvido em 1991 por Artur Ekert e é baseado na propriedade da não-localidade quântica. Ele permite a distribuição de uma chave criptográfica perfeitamente segura entre duas partes.
2. Protocolo BB84: Esse protocolo foi desenvolvido em 1984 por Charles Bennett e Gilles Brassard e é baseado na propriedade da incerteza quântica. Ele também permite a distribuição de uma chave criptográfica perfeitamente segura entre duas partes.
3. Protocolo de criptografia de chave contínua (CV-QKD): Esse protocolo é utilizado para proteger a comunicação em tempo real. Ele utiliza a propriedade da codificação quântica contínua para distribuir uma chave criptográfica entre duas partes.

Avanços Recentes

1. Rede de criptografia quântica: Em 2020, pesquisadores da Universidade de Genebra, na Suíça, criaram a primeira rede de criptografia quântica interconectando quatro cidades suíças. Isso representa um grande avanço para a implementação da criptografia quântica em larga escala.
2. Memória quântica: Em 2020, pesquisadores da Universidade de Ciência e Tecnologia da China criaram uma memória quântica capaz de armazenar fótons individuais por mais de uma hora. Isso é importante para a criação de sistemas quânticos mais robustos e eficientes.
3. QKD baseada em satélite: Em 2021, pesquisadores chineses demonstraram a distribuição de uma chave criptográfica entre um satélite quântico e estações terrestres, com um alcance de mais de 1.000 km. Isso representa um grande avanço para a implementação da criptografia quântica em larga escala e em longas distâncias.

Esses são apenas alguns exemplos de protocolos e avanços recentes na área da criptografia quântica. Ainda há muito a ser explorado e desenvolvido nessa área, mas esses avanços são um indicativo de que a criptografia quântica está cada vez mais próxima de se tornar uma realidade em larga escala.

Resultados e Discussão

Resultados

Os avanços recentes na pesquisa em criptografia quântica mostram que essa tecnologia pode ser mais segura do que a criptografia clássica em certos cenários. Além disso, a criptografia quântica pode ser usada para garantir a autenticidade e integridade das informações, além de sua confidencialidade. No entanto, a implementação da criptografia quântica ainda é um desafio técnico, e muitos dos resultados obtidos ainda precisam ser confirmados em experimentos práticos.

Discussão

Apesar de ainda estar em estágios iniciais de desenvolvimento, a criptografia quântica já está gerando discussões acaloradas em diversos campos. Abaixo, apresentamos algumas das principais discussões na criptografia quântica.

1. Segurança versus praticidade: Embora a criptografia quântica seja considerada uma das formas mais seguras de criptografia, ela ainda é uma tecnologia em desenvolvimento e pode não ser prática o suficiente para uso em larga escala. A implementação da criptografia quântica pode ser cara, limitada pela disponibilidade de recursos e pode exigir uma grande quantidade de energia. Essas limitações levantam a questão de como equilibrar a segurança com a praticidade em um ambiente onde a informação é cada vez mais valiosa.

2. Padrões e protocolos: Outra questão é a falta de padrões e protocolos comuns para a criptografia quântica. A ausência de padrões pode dificultar a interoperabilidade entre diferentes sistemas, além de criar problemas de segurança e privacidade. É necessário que haja uma padronização das tecnologias quânticas para que possam ser amplamente utilizadas.
3. Resistência a ataques: A criptografia quântica é projetada para ser resistente a ataques, mas isso não significa que seja completamente impenetrável. Os ataques quânticos são uma possibilidade real e ainda pouco compreendida. Os 17 especialistas em segurança estão trabalhando para desenvolver novas técnicas para detectar e prevenir esses tipos de ataques.
4. Uso em larga escala: Atualmente, a criptografia quântica é usada principalmente em aplicações de alta segurança, como transações financeiras e governamentais. No entanto, a medida que a tecnologia se desenvolve, ela poderá ser aplicada em uma ampla gama de campos, incluindo na área de projetos sociais e humanitários. A discussão está em como tornar a criptografia quântica acessível a um público mais amplo.

Em resumo, a criptografia quântica é uma tecnologia promissora que está gerando muitas discussões no campo da segurança da informação. Ainda há muitos desafios a serem superados, mas é possível que a criptografia quântica possa mudar a forma como protegemos nossas informações no futuro.

Conclusão

A criptografia quântica é uma tecnologia revolucionária que oferece segurança na comunicação de dados. Ela utiliza as propriedades quânticas da matéria para garantir a privacidade e a segurança das informações, tornando praticamente impossível que um adversário intercepte ou decifre as mensagens criptografadas.

Recentemente, foram realizados avanços significativos na área da criptografia quântica, como o desenvolvimento de novos protocolos que utilizam menos recursos e a implementação de sistemas quânticos mais robustos e eficientes.

Além disso, a criptografia quântica é mais eficiente do que a criptografia clássica, pois oferece segurança mais sofisticada com um número muito menor de bits e com um processo de distribuição mais rápido. Essa eficiência foi comprovada matematicamente, mostrando que a criptografia quântica é uma opção para garantir a privacidade e a segurança das informações.

Referências Bibliografias

- Bennet, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

- Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.

- Lo, H. K., & Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283(5410), 2050-2056.

- Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301-1350.

- Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 124-134.

- Zhong, H.-S., Li, Y., Hu, Y., Wang, Y.-L., Peng, L.-C., Zhang, Y., . . . Pan, J.-W. (2021). Random measurement basis for quantum key distribution. Physical Review Research, 3(2), 023043.

Desvende os segredos da criptografia quântica com este eBook abrangente. Explore os fundamentos teóricos e práticos da criptografia quântica e descubra como essa tecnologia revolucionária está mudando o cenário da segurança de informações.

Neste guia, você aprenderá e conhecerá as bases da criptografia quântica. Aprenda sobre os fundamentos da segurança quântica, incluindo distribuição de chaves quânticas, criptografia de estados quânticos e detecção de intrusões.

Com exemplos claros, você desenvolverá uma compreensão sólida dos conceitos-chave da criptografia quântica. Explore os desafios e as soluções oferecidas por essa abordagem única, capaz de garantir a proteção de dados sensíveis em um mundo cada vez mais conectado.

Maxwell Pereira Lima
Noemi Soares Gonçalves da Silva