CRIPTOGRAFIA QUÂNTICA

LABORATÓRIO DE SEGURANÇA CIBERNÉTICA

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

SUMÁRIO

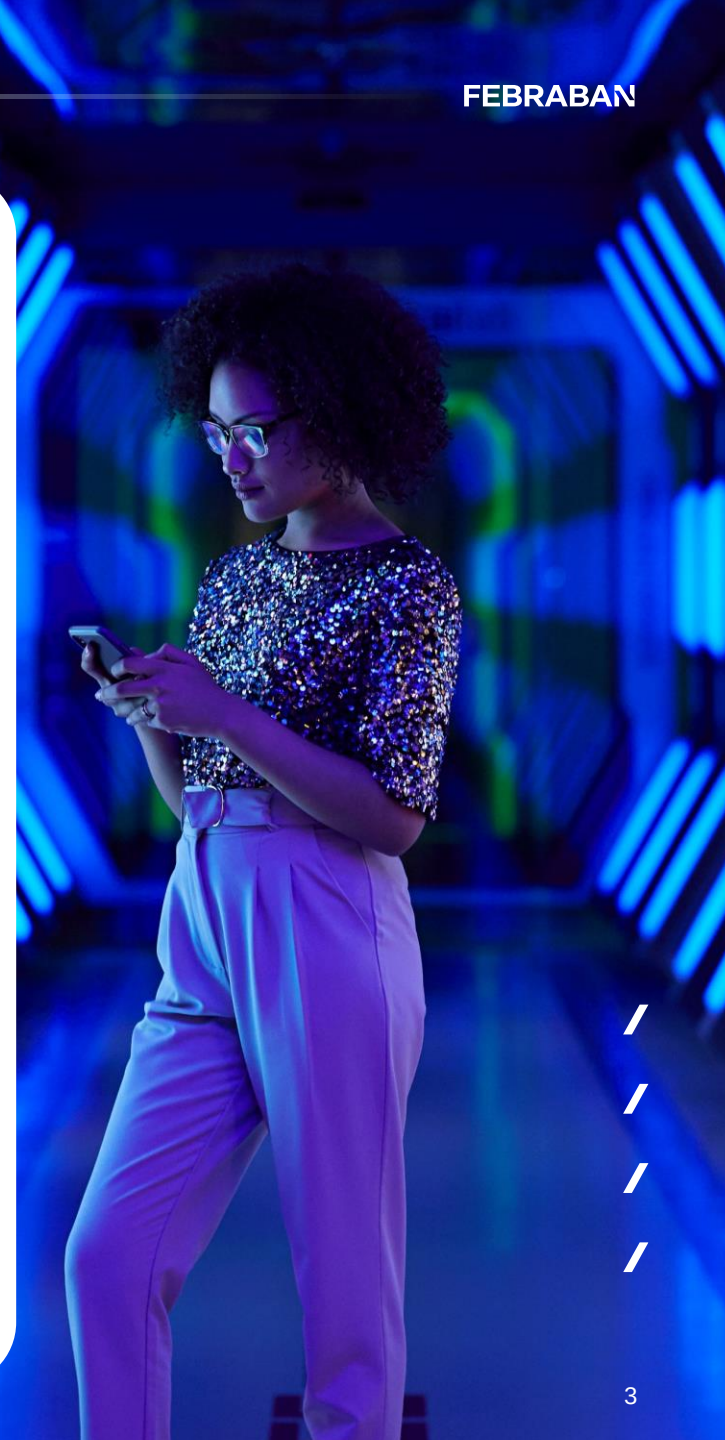
1 INTRODUÇÃO

No vasto mundo da segurança cibernética, a criptografia desempenha um papel crítico na proteção das informações. A capacidade de codificar mensagens e dados de forma que apenas as partes pretendidas possam decifrá-los tem sido um pilar central nas estratégias de defesa contra ameaças cibernéticas. Mas, à medida que a tecnologia avança, novos desafios emergem, e o surgimento da criptografia quântica é um testamento dessa evolução.

Este estudo busca explorar a intersecção entre a ciência quântica e a criptografia, detalhando o impacto que essa nova vertente pode ter na segurança cibernética, com um foco especial nas instituições financeiras brasileiras. O Brasil, como uma das maiores economias do mundo, possui um setor financeiro robusto que depende fortemente da criptografia para proteger as transações e dados sensíveis de seus clientes. Portanto, entender as potenciais implicações da criptografia quântica é de suma importância para a integridade e confidencialidade do setor.

A criptografia quântica é uma abordagem baseada nas propriedades singulares da mecânica quântica, e promete revolucionar a maneira como vemos a segurança de dados. Contudo, assim como qualquer tecnologia emergente, ela traz consigo tanto oportunidades quanto riscos. Ameaças que, até então, eram teoricamente impossíveis no paradigma clássico da criptografia, podem se tornar realidade no âmbito quântico.

A segurança cibernética está em constante evolução, e a criptografia quântica é a próxima fronteira. Neste estudo, embarcaremos juntos nesta jornada, analisando o passado, presente e futuro da criptografia em um mundo influenciado pela mecânica quântica.



A criptografia clássica é uma disciplina que se vale de conceitos matemáticos para codificar e decodificar dados. Sua função principal é possibilitar que um usuário guarde informações sigilosas ou as transmita por meios não seguros, como a Internet, de modo a torná-las ilegíveis para qualquer pessoa que não seja o destinatário pretendido. Para garantir uma transmissão segura, um algoritmo é empregado, unindo a mensagem original a informações suplementares para gerar um texto cifrado. Esse algoritmo é conhecido como cifra, e as informações suplementares são chamadas de chave.

No contexto digital, a criptografia se baseia em três princípios fundamentais: **confidencialidade, integridade e autenticação**. Esses princípios garantem que as informações sejam confiáveis e acessíveis apenas para os usuários autorizados. Cada um desses princípios é reforçado por meio da aplicação de técnicas criptográficas específicas.

A confidencialidade é mantida por meio da criptografia dos dados usando chaves públicas e privadas. A integridade é assegurada por funções de hash e assinaturas digitais. A autenticação é estabelecida por meio do uso de chaves privadas controladas exclusivamente pela entidade. Atualmente, a criptografia desempenha um papel essencial nas operações comerciais diárias e é especialmente prevalente nos métodos de comunicação na Internet entre os usuários e as aplicações web.

Esses princípios impulsionaram o avanço para a criptografia quântica, que fundamenta sua segurança nos princípios da mecânica quântica.

2 CRIPTOGRAFIA CLÁSSICA VS CRIPTOGRAFIA QUÂNTICA

A criptografia clássica é um campo de estudo que se baseia em princípios matemáticos para garantir a segurança da comunicação e da informação. Ela remete a civilizações antigas e é fundamentalmente construída **em dois tipos principais de algoritmos: a cifra de substituição e a cifra de transposição**.

A **cifra de substituição** é um método de criptografia que envolve a substituição de cada caractere individual de um texto claro (mensagem original) por outro caractere, de acordo com um conjunto predefinido de regras. Um exemplo simples é a cifra de César, onde cada letra da mensagem é substituída por uma letra fixa a um número específico de posições adiante no alfabeto. Por exemplo, com um deslocamento de três posições, "A" seria substituído por "D," "B" por "E," e assim por diante. Esse método é facilmente quebrado com técnicas de força bruta e análise estatística, mas era amplamente utilizado na antiguidade e representa o princípio fundamental da cifra de substituição na criptografia clássica.

Já a **cifra de transposição** é um método de criptografia que se baseia na reorganização dos caracteres de uma mensagem sem alterar os próprios caracteres. Em vez de substituir letras ou símbolos, como na cifra de substituição, a cifra de transposição envolve a mudança da ordem dos caracteres na mensagem. Isso é feito aplicando uma técnica específica, como inverter a ordem dos caracteres, agrupá-los em blocos de tamanho fixo ou reorganizá-los de acordo com uma chave. A segurança desse método reside na complexidade do esquema de transposição, que deve ser conhecido apenas pelo remetente e pelo destinatário para decifrar a mensagem. Embora seja mais resistente do que a cifra de substituição, a cifra de transposição também é vulnerável a ataques quando não são usadas técnicas de transposição complexas.

Métodos de Criptografia

Existem dois principais métodos de criptografia: a criptografia simétrica e a criptografia assimétrica. A **criptografia simétrica** é um método de criptografia em que a mesma chave é utilizada tanto para cifrar quanto para decifrar informações. Isso implica que tanto o remetente quanto o destinatário precisam compartilhar a mesma chave secreta previamente para realizar a comunicação segura. Quando uma mensagem é enviada, a chave simétrica é usada para cifrá-la, tornando-a ilegível, e, em seguida, o destinatário a decifra usando a mesma chave, restaurando-a à sua forma original. A principal vantagem da criptografia simétrica é sua eficiência e velocidade, mas a segurança depende da proteção rigorosa da chave compartilhada, uma vez que qualquer pessoa com acesso a essa chave pode descriptografar as mensagens.

Em contraste, a **criptografia assimétrica**, também conhecida como criptografia de chave pública, é um método criptográfico em que um par de chaves é usado: uma chave pública e uma chave privada. A chave pública é amplamente distribuída e utilizada para cifrar mensagens, enquanto a chave privada, mantida em sigilo pelo destinatário, é empregada para decifrar as mensagens cifradas. Essa abordagem elimina a necessidade de compartilhar a mesma chave secreta entre as partes e oferece vantagens em termos de segurança e autenticação.

A chave pública pode ser usada para verificar a origem das mensagens, enquanto a chave privada garante que apenas o destinatário autorizado possa decifrá-las, proporcionando um alto nível de segurança na comunicação digital.

A **infraestrutura de chaves públicas** (PKI - Public Key Infrastructure) é um conjunto de políticas, procedimentos e tecnologias que facilitam a criação e a gestão de pares de chaves públicas e privadas. Isso inclui a certificação de entidades (como sites da web ou indivíduos) por meio de autoridades de certificação confiáveis, que emitem certificados digitais contendo chaves públicas e informações de identificação. Quando um usuário se conecta a um site seguro, o certificado digital do site é verificado pelo navegador usando a chave pública da CA. Assim, a PKI desempenha um papel fundamental na segurança da comunicação digital, garantindo a autenticidade e a confiabilidade das chaves públicas usadas na criptografia assimétrica.

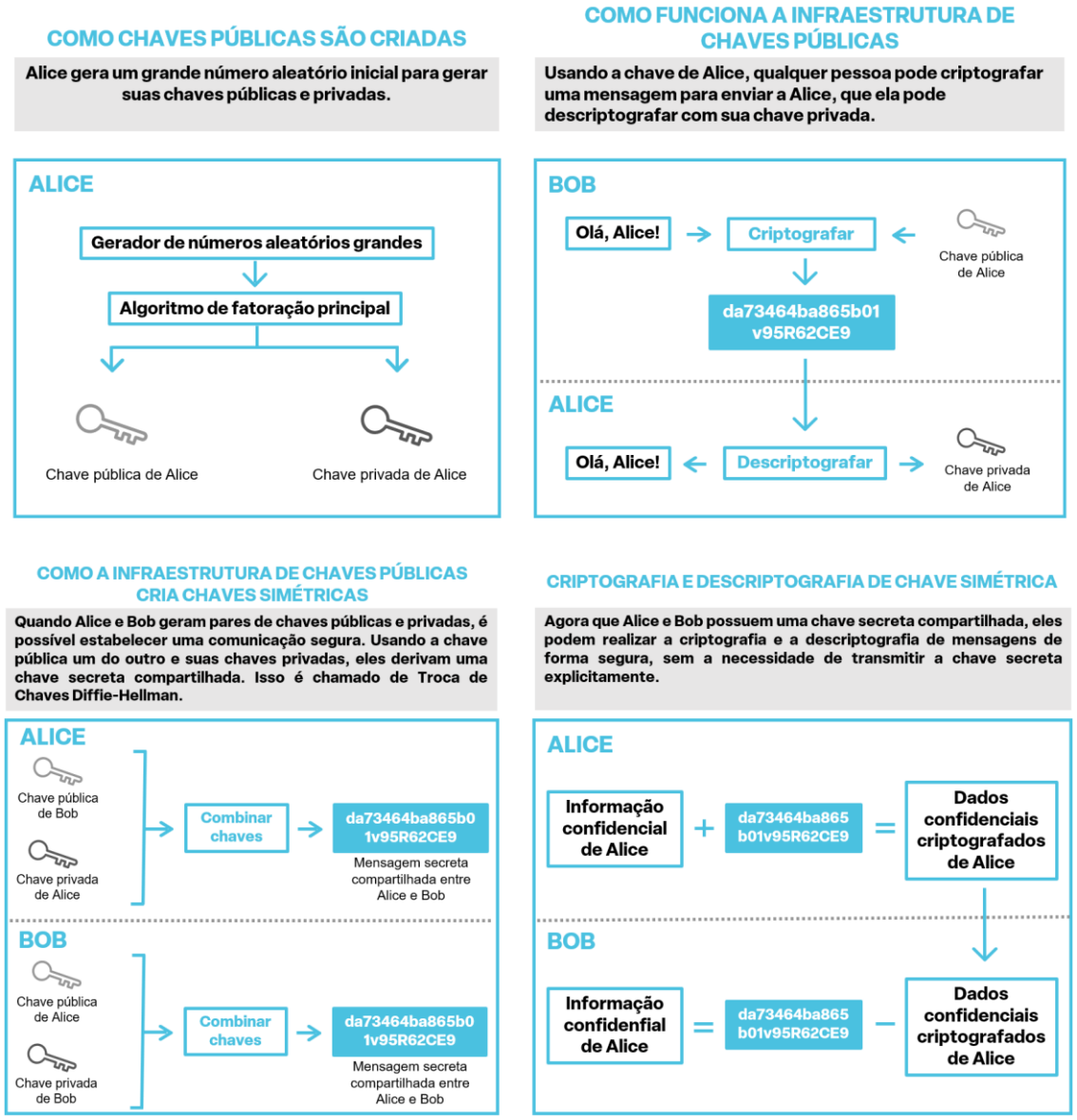
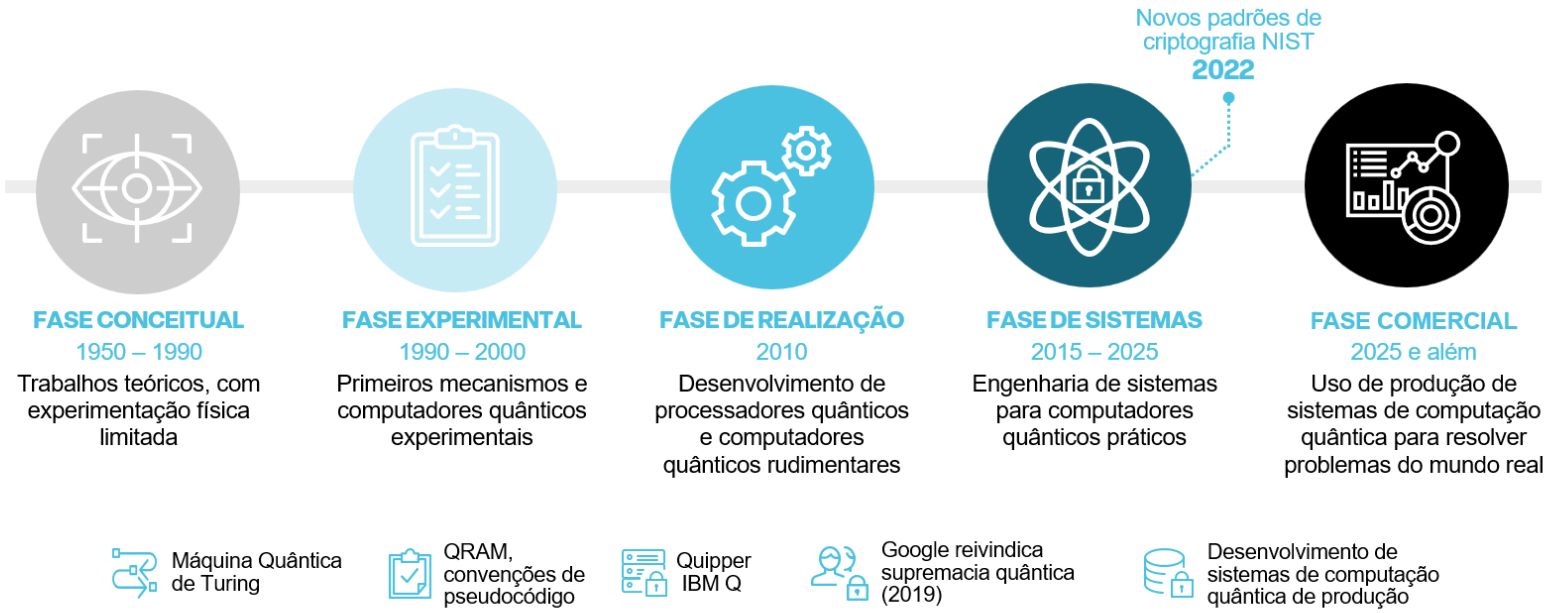


Figura 1. Chaves Públicas e Privadas

A computação quântica é uma área da informática que se baseia nos princípios da mecânica quântica para processar informações de maneira significativamente mais poderosa do que os computadores clássicos. Enquanto os computadores tradicionais usam bits para representar informações como 0s e 1s, os computadores quânticos usam qubits, que têm a capacidade de representar 0s, 1s ou qualquer combinação de ambos simultaneamente, graças ao fenômeno da superposição.

Além disso, os qubits podem estar entrelaçados, o que significa que ações em um qubit podem afetar instantaneamente outros qubits entrelaçados, independentemente da distância entre eles. Isso torna a computação quântica capaz de resolver problemas complexos, como fatorização de números inteiros grandes e otimização, em uma fração do tempo necessário pelos computadores clássicos. A computação quântica tem o potencial de transformar diversas áreas, incluindo criptografia e pesquisa científica.

A LINHA DO TEMPO DA COMPUTAÇÃO QUÂNTICA



Fonte: Intel

A história da computação quântica começa em 1981, quando Richard Feynman propôs a ideia de que um computador quântico poderia simular sistemas quânticos de forma eficiente. Em 1994, Peter Shor desenvolveu um algoritmo quântico que poderia fatorizar números inteiros grandes de maneira eficiente, ameaçando a segurança dos sistemas de criptografia baseados em fatorização. Paralelamente, Lov Grover desenvolveu um algoritmo quântico para pesquisa não ordenada, o que poderia ter implicações significativas em algoritmos de busca. A partir dos anos 2000, houveram avanços notáveis na construção de qubits e computadores quânticos, com empresas e instituições de pesquisa competindo na corrida para desenvolver máquinas quânticas cada vez mais poderosas. **Hoje, a computação quântica está em constante evolução, com o potencial de revolucionar áreas como criptografia, pesquisa em materiais e otimização.**

A criptografia quântica, por sua vez, é um campo avançado da criptografia que utiliza princípios da mecânica quântica para proteger informações de maneira extremamente segura. Ela se baseia na propriedade fundamental da mecânica quântica de que a observação de uma partícula pode alterar seu estado, o que é conhecido como o princípio da não clonagem. Na criptografia quântica, as chaves de criptografia são geradas e transmitidas como partículas quânticas, como fótons [Figura 2].

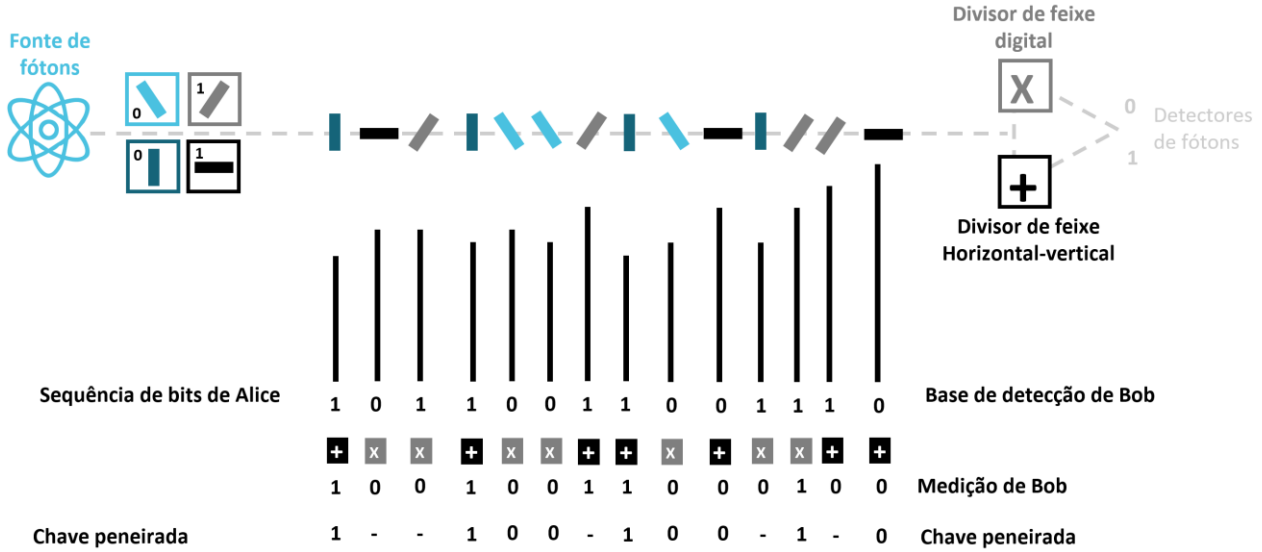


Figura 2. Esquema de funcionamento de distribuição de chaves quânticas

Ao contrário da criptografia clássica, que depende de algoritmos matemáticos, a criptografia quântica utiliza as propriedades inerentes da mecânica quântica para garantir a transmissão segura de dados. Esta abordagem é baseada em dois princípios fundamentais: superposição quântica e emaranhamento quântico [2] [3]. A superposição quântica permite que as partículas quânticas existam em vários estados simultaneamente.

No contexto da criptografia, significa que uma mensagem codificada quântica pode representar todas as combinações possíveis de informações de uma só vez. Essa propriedade garante que qualquer tentativa de interceptar ou espionar a comunicação perturbe o delicado estado quântico, alertando tanto o remetente quanto o destinatário sobre a violação.

No emaranhamento quântico, quando duas partículas quânticas se emaranham, seus estados se tornam inerentemente ligados, independentemente da distância entre eles. Qualquer mudança no estado de uma partícula afeta instantaneamente a outra, mesmo que estejam separadas por anos-luz.

Qualquer mudança no estado de uma partícula afeta instantaneamente a outra, mesmo que estejam separadas por distâncias enormes. Esse fenômeno permite o estabelecimento de um mecanismo seguro de distribuição de chaves, conhecido como **distribuição de chaves quânticas (QKD)**.

O QKD viabiliza a criação de chaves de criptografia resistentes à interceptação, pois qualquer tentativa de observar ou adulterar as partículas emaranhadas interromperia a chave e alertaria as partes legítimas envolvidas.

Avanços e promessas na Tecnologia Quântica

À medida que as tecnologias quânticas continuam a avançar, também aumenta a promessa da criptografia quântica. Esforços de pesquisa e desenvolvimento estão em andamento para tornar a criptografia quântica mais prática e acessível para organizações e indivíduos.

No momento, países como Áustria, China, Japão, Suíça e Estados Unidos estão comprometidos em implementar o QKD como suporte à criação de One-Time Pads (OTPs). As OTPs são chaves extensas que são previamente compartilhadas entre o remetente e o destinatário. Ao contrário de outros métodos criptográficos em que as chaves são empregadas repetidamente, **uma OTP é uma chave de uso único, projetada para proteger uma única comunicação e deve ter o mesmo comprimento que a mensagem que está sendo transmitida**.

Qualquer algoritmo que pertença à categoria de "problemas desafiadores na teoria dos números" e envolva "funções de alçapão unidirecionais" pode ser usado para a troca de chaves.

Recentemente, os pesquisadores têm se empenhado em desenvolver esquemas criptográficos que preservem a infraestrutura criptográfica atual, ao mesmo tempo em que substituem os problemas de teoria dos números que são vulneráveis a ataques de computadores quânticos [10]. Isso permitiria a substituição de apenas uma parte reduzida da infraestrutura de chave pública, especificamente a combinação de espaço de chaves, por algoritmos resistentes à computação quântica.

A criptografia baseada em rede (Lattice) e a criptografia baseada em hash fornecem duas opções que permitem aos pesquisadores manter a infraestrutura existente que suporta a troca de chaves Diffie-Hellman e a assinatura digital, ao mesmo tempo em que oferecem resistência à criptoanálise quântica.

A **Lattice** pode ser aplicada a uma ampla gama de serviços criptográficos, como criptografia, assinatura de mensagens e hashing, tornando-a uma opção amplamente considerada para a era pós-quântica da criptografia.

Até que se prove o contrário, ela continua sendo uma alternativa segura. No entanto, os algoritmos de criptografia de chave pública baseados em redes não se adaptam tão facilmente a essa transição.

Por outro lado, a **criptografia baseada em hash** é uma abordagem criptográfica alternativa à prova de resistência quântica, focada principalmente na criação de assinaturas digitais que verificam a autenticidade de documentos ou mensagens, assegurando que eles tenham origem no remetente original. Atualmente, não existem esquemas criptográficos baseados em hash para cifrar e decifrar mensagens por meio de troca assimétrica de chaves públicas (PKE), sendo necessário o uso de métodos criptográficos suplementares para outros serviços criptográficos.

Segurança e Criptografia

A segurança da criptografia e a segurança cibernética são duas áreas interligadas, mas distintas, que desempenham papéis cruciais na proteção de dados e sistemas na era digital. A criptografia é o processo de transformar informações em um formato ilegível para terceiros, garantindo a confidencialidade dos dados. No entanto, a segurança da criptografia se concentra especificamente nas técnicas, algoritmos e protocolos utilizados para proteger a integridade e a confiabilidade da criptografia em si. Isso envolve a seleção de algoritmos resistentes a ataques, o gerenciamento de chaves criptográficas e a prevenção de vazamento de informações sensíveis por meio de vulnerabilidades na criptografia.

Por outro lado, a segurança cibernética é um campo mais amplo que abrange a proteção de sistemas, redes e dados contra uma variedade de ameaças, que incluem ataques cibernéticos, malware, acesso não autorizado e muito mais. A criptografia desempenha um papel fundamental na segurança cibernética, pois é uma das ferramentas mais eficazes para proteger dados em trânsito e em repouso. Isso significa que a segurança cibernética engloba não apenas a proteção da criptografia em si, mas também o monitoramento, a detecção e a prevenção de ataques que visam explorar ou comprometer sistemas criptografados.

Em resumo, enquanto a segurança da criptografia concentra-se nas técnicas e práticas que garantem a robustez e a confiabilidade dos algoritmos criptográficos, a segurança cibernética se estende a medidas mais amplas de proteção, incluindo a integração da criptografia como parte de uma estratégia de defesa global contra ameaças cibernéticas. Ambos são elementos essenciais para manter a integridade e a privacidade dos dados em um mundo digital cada vez mais interconectado.

3 SEGURANÇA

As principais diferenças em termos de segurança entre a criptografia clássica e a criptografia quântica residem nas vulnerabilidades e nos métodos de proteção. Na criptografia clássica, a segurança se baseia em problemas matemáticos difíceis de resolver, como a fatorização de números inteiros grandes na criptografia de chave pública. No entanto, com o avanço da computação, algoritmos e poder de processamento mais rápidos, esses problemas podem ser solucionados, tornando a segurança vulnerável a ataques futuros.

Em contrapartida, a criptografia quântica oferece uma segurança intrinsecamente diferente. Ela se baseia nas propriedades fundamentais da mecânica quântica, como a superposição e o emaranhamento, para proteger a informação. O princípio da incerteza de Heisenberg torna a interceptação da chave quântica impossível sem perturbar seu estado quântico, o que alerta as partes envolvidas sobre a violação da segurança. Em resumo, enquanto a segurança da criptografia clássica depende da dificuldade de resolver problemas matemáticos, a criptografia quântica se baseia em princípios quânticos que oferecem uma camada adicional de proteção, tornando-a potencialmente mais robusta contra ameaças avançadas.

Os avanços na pesquisa em computação quântica atingiram um estágio em que se espera que, nos próximos dez anos, **um computador quântico funcional capaz de quebrar a criptografia atualmente em uso se torne uma realidade** [1].

Uma das classes de problemas que os computadores quânticos resolvem com maior eficiência é a chamada "estimativa de fase," que envolve identificar onde duas frequências diferentes se sobrepõem.

O problema da fatoração primária e o problema do logaritmo discreto podem ser reformulados como problemas de estimativa de fase. Em 1994, Peter Shor demonstrou que os computadores quânticos podem explorar características da física quântica para resolver esses problemas de forma eficaz, sem depender da força bruta.

Isso torna qualquer informação criptografada usando sistemas de chave pública vulnerável à descriptografia quando confrontada com computadores quânticos.

Os atores de ameaça empregam principalmente duas técnicas para comprometer os algoritmos utilizados na criptografia moderna. A primeira envolve a **engenharia reversa das operações matemáticas realizadas pelo algoritmo**, enquanto a segunda consiste na tentativa de adivinhar a(s) chave(s) secreta(s) por meio de ataques de força bruta. A primeira técnica muitas vezes resulta de erros humanos no processo de desenvolvimento de software.

Durante a criação de programas de criptografia e descriptografia, os desenvolvedores podem inadvertidamente cometer equívocos na implementação das operações matemáticas, criando vulnerabilidades que permitem que invasores contornem os métodos criptográficos por meio da engenharia reversa.

A segunda técnica, que envolve **ataques de força bruta**, é geralmente inviável para algoritmos implementados corretamente com chaves suficientemente complexas. Mesmo quando utilizam aceleradores de hardware, como Unidades de Processamento Gráfico (GPUs), Field Programmable Gate Arrays (FPGA) e Circuitos Integrados de Aplicação Específica (ASICs), os invasores podem levar séculos de processamento computacional para testar todos os possíveis valores de chave. Ataques de força bruta permanecem uma tarefa desafiadora [4][6].

No entanto, a computação quântica introduz uma abordagem radicalmente diferente para as técnicas criptográficas, reconfigurando problemas da teoria dos números em desafios que podem ser resolvidos com notável eficiência por um computador quântico. Isso implica a transformação de problemas que, em contextos clássicos, demandariam milênios de processamento computacional em tarefas gerenciáveis em períodos muito mais curtos, como dias ou semanas. Recentemente, pesquisadores também demonstraram a capacidade da computação quântica de desvendar sistemas criptográficos robustos [Figura 3].

CRIPTOSSISTEMAS MODERNOS E SUAS VULNERABILIDADES AOS ALGORITMOS QUÂNTICOS

Criptossistema	Impacto	Observação
RSA Diffie-Hellman Curva Elíptica	Quebrado Quebrado Quebrado	O algoritmo de Shor descreve uma aceleração exponencial para resolver problemas classicamente difíceis de teoria dos números, como fatorar grandes números primos e resolver logaritmos discretos.
Baseado em código Baseado em hash	Ainda não quebrado Ainda não quebrado	Esses criptossistemas foram introduzidos no final da década de 1970 e sua segurança foi bem estudada. Eles não são conhecidos por serem vulneráveis aos avanços da computação quântica.
Baseado no método Lattice Multivariado	Ainda não quebrado Ainda não quebrado	Esses criptossistemas foram introduzidos no final da década de 1990 e acredita-se que sejam seguros contra os avanços da computação quântica.
One-time pad (OTP)	Comprovadamente inquebrável	Claude Shannon provou que o OTP tem sigilo perfeito, o que significa que não é vulnerável aos avanços na computação quântica. Embora imunes à criptoanálise, os requisitos de codificação rigorosa limitam a implementação do OTP.

Figura 3. Relação de criptossistemas vulneráveis

Teoricamente, é possível monitorar qualquer canal de comunicação moderna sem que o remetente ou o destinatário tenham conhecimento da interceptação. Isso ocorre porque informações semelhantes a chaves criptográficas são codificadas em características físicas mensuráveis de um objeto ou sinal. Assim, a criptografia clássica deixa em aberto a possibilidade de escuta passiva.

Padronização de Criptografia do NIST

Em 2016, competidores de várias partes do mundo apresentaram um total de 69 esquemas criptográficos, com o objetivo de possível padronização junto ao NIST (Instituto Nacional de Padrões e Tecnologia dos Estados Unidos) [5]. Posteriormente, o Instituto conduziu uma série de três fases para gradualmente reduzir o grupo de candidatos, culminando na seleção de sete finalistas, abrangendo quatro para criptografia de chave pública e três para assinaturas digitais.

Após um processo de seis anos, três dos quatro padrões selecionados emergiram por meio de uma colaboração entre indústria e acadêmicos. Neste contexto, a criptografia de chave pública **CRYSTALS-Kyber** e os algoritmos de assinatura digital **CRYSTALS-Dilithium** foram designados como padrões principais.

Simultaneamente, o algoritmo de assinatura digital **Falcon** foi adotado como padrão para situações em que a implementação do Dilithium estaria limitada por considerações de espaço. Kyber “é um mecanismo de encapsulamento de chave (KEM) cuja segurança é baseada na dificuldade de resolver o problema de aprendizagem com erros em redes de módulos, e faz parte do conjunto de algoritmos CRYSTALS (suíte criptográfica para redes algébricas).” Dilithium, também um algoritmo CRYSTALS, “é um esquema de assinatura digital que tem sua segurança baseada de forma semelhante na dureza dos problemas de rede em redes de módulos”. Falcon é outro algoritmo de assinatura digital fundamentado na complexidade de encontrar vetores curtos em redes NTRU (um sistema de criptografia de chave pública de código aberto, que se vale da criptografia baseada em rede para codificar e decodificar informações). Embora Dilithium e Falcon sejam algoritmos de assinatura digital enraizados em conceitos de rede, eles atuam de maneira complementar em suas aplicações - o Falcon apresenta parâmetros mais compactos, enquanto o Dilithium se destaca por ser mais simples de implementar e utilizar [6].

A Accenture identifica **duas fases cruciais na evolução da criptografia**, no curto e longo prazo [1]. Enquanto aguardam a eventual adoção de um novo padrão de segurança quântica previsto pelo NIST entre 2022-2024, as organizações devem priorizar sua migração tecnológica com máxima urgência. Isso envolverá a implementação de medidas de mitigação de curto prazo para aprimorar a segurança dos métodos de criptografia existentes.

A primeira fase refere-se a evitar antecipadamente que computadores quânticos possam efetivamente comprometer a criptografia clássica.

Nesse sentido, é necessário que os especialistas em criptografia atualizem os algoritmos tradicionais com métodos resistentes à computação quântica, como a criptografia baseada em redes e em funções hash. Isso visa aprimorar a capacidade de resistência desses sistemas contra potenciais ataques de criptoanálise provenientes da computação quântica.

A computação quântica também poderia expor dados estratégicos importantes, causando grandes instabilidades na segurança cibernética. **Protocolos como HTTPS e S/MIME correm o risco de vazamento de dados em casos de má configuração**. Dados transferidos por meio de métodos de VPN, seja de cliente remoto ou site a site, também podem ficar vulneráveis.

A falta de integridade dos sistemas e dos dados na era pós-quântica teria um impacto severo na utilização prática de infraestruturas críticas e sistemas financeiros digitais. A autenticação em muitos desses sistemas também depende da criptografia de chave pública RSA para identificação e autorização do usuário, o que a tornaria vulnerável. Os profissionais de segurança também precisariam revisar muitos sistemas de autenticação multifatorial para garantir a resistência quântica, caso os atores de ameaça comecem a aproveitar os computadores quânticos.

Além disso, especialistas teriam que avaliar inúmeros sistemas governamentais e empresariais críticos para determinar o potencial impacto na integridade devido a um evento quântico.

Para colocar esta ameaça em perspectiva, a Forbes estimou que “**um único ataque quântico causaria um fracasso financeiro em cascata que custaria entre 730 bilhões de dólares e 1,95 trilhões de dólares**” [11]. Se essa ameaça se concretizar, muitos serviços que utilizam túneis criptográficos pela Internet, como VPNs site-to-site, túneis SSH, VPNs SSL ou VPNs IPSec, perderiam completamente a integridade do sistema e exporiam potenciais vulnerabilidades à exploração por parte de atores de ameaça.

Criptografia e Espionagem

Um estudo recente da Accenture Cyber Threat Intelligence em parceria com a Accenture Emerging Technology Security sugere que **grupos patrocinados por estados podem já estar coletando dados criptografados com o objetivo de descriptografá-los posteriormente com o uso de computadores quânticos**. Países conhecidos por suas extensas atividades cibernéticas voltadas para a coleta de informações, espionagem e ganhos financeiros incluem a China, Rússia, Coreia do Norte e Irã. Essa tendência reforça a importância de se preparar para os desafios da criptografia pós-quântica.

Atividades relacionadas a atores vinculados à Coreia do Norte, como o grupo **NEEDLEFISH**, são notórias por envolverem roubos de criptomoedas, uso de ransomware e várias ferramentas de hacking para atingir setores críticos, incluindo o da saúde, principalmente com o objetivo de obter ganhos financeiros.

Da mesma forma, grupos iranianos, como o **Corpo da Guarda Revolucionária Islâmica**, são conhecidos por mirar o setor financeiro, construção e serviços de alta tecnologia, além de conduzirem atividades ilegais, como contrabando, mineração de criptomoedas, lavagem de dinheiro e operações de ransomware para financiar suas operações.

Devido à avançada capacidade dos atores de ameaças originários da China e ao forte respaldo do governo chinês para o desenvolvimento de tecnologias quânticas, foi concluído que os **atores provenientes da China representam a principal ameaça global no cenário pós-quântico**.

A Accenture avalia ainda que a China, que tem investido fortemente em tecnologias quânticas e na expansão econômica, se tornará cada vez mais bem-sucedida em suas campanhas e vitimologia. Os atores de ameaças chineses são conhecidos por suas constantes atividades de espionagem cibernética em diversos setores, incluindo os críticos.

Nos últimos anos, as capacidades de computação quântica chinesas aumentaram com os seguintes desenvolvimentos:

- Em 2018, a China revelou uma rede experimental de distribuição de chaves quânticas por satélite abrangendo 2 continentes, conectando Xinglong, China, e Graz, Áustria;
- Em 2020, a China incluiu tecnologia quântica e de gestão de chaves nas novas leis de controle de exportações;
- Em janeiro de 2021, cientistas chineses revelaram uma rede híbrida de comunicações quânticas conectando Pequim, Jinan, Hefei e Xangai;
- Em fevereiro de 2021, a Origin Tech, com sede na China, lançou o Origin Pilot, o primeiro sistema operacional desenvolvido na China para computadores quânticos;
- Em abril de 2022, a China anunciou um investimento de US$ 15,3 bilhões destinado ao desenvolvimento da computação quântica.

4 VULNERABILIDADES

Embora a mídia ocasionalmente alegue que a criptografia quântica fornece segurança "garantida" com base nas leis da física, em março de 2023 **foram divulgadas as primeiras vulnerabilidades dessa tecnologia** [9].

Essas vulnerabilidades estão relacionadas aos componentes de niobato de lítio disponíveis no mercado e que estão sendo utilizados nos primeiros dispositivos comerciais de criptografia quântica. A primeira vulnerabilidade foi encontrada na área de transição de avalanche do dispositivo de detecção: o "efeito avalanche" começa com um único fóton e desencadeia uma série de outros fótons, garantindo uma conexão óptica eficaz. Para realizar esse ataque, apenas um feixe de laser com 3 nanoWatts (nW) é necessário.

A segunda vulnerabilidade foi detectada no transmissor. Os pesquisadores conseguiram executar o ataque utilizando um transmissor adaptado para sistemas QKD independentes do dispositivo de medição. Ao medir simultaneamente todos os estados quânticos enviados pelo remetente e ao induzir a fotorrefração no modulador de niobato de lítio por meio do feixe de irradiação inserido, o invasor é capaz de efetivamente esconder as perturbações causadas no sistema quântico devido às suas ações de medição.

O experimento de ataque demonstrou a **possibilidade real de o invasor obter praticamente todas as chaves criptográficas**. Essas descobertas recentes são um lembrete incontestável de que a segurança na esfera da criptografia quântica não pode ser considerada garantida sem análise e controle rigorosos e constantes.

À medida que as pesquisas avançam, é essencial que a comunidade permaneça vigilante, abraçando a inovação e adaptando continuamente as abordagens de segurança. Isso é fundamental para garantir que a promessa da criptografia quântica seja respaldada por medidas de defesa sólidas, a fim de aproveitar todo o seu potencial com segurança.

5 FUTURO

Estamos em uma época marcada pela rápida evolução da segurança cibernética, em parte devido à ascensão da computação quântica. Esta inovação, considerada revolucionária, pode remodelar completamente os padrões de criptografia, desafiando organizações a se adaptarem de imediato.

A pesquisa realizada pela Accenture destaca duas fases essenciais na progressão da criptografia. No curto prazo, enquanto se espera pela adoção de padrões de segurança quântica previstos pelo NIST entre 2022-2024, é crucial que as organizações acelerem sua transição tecnológica. Este período envolve melhorar a robustez dos métodos de criptografia atuais. Especialistas estão focados em adaptar algoritmos clássicos para torná-los mais resistentes a ataques quânticos.

A segunda fase promete ser ainda mais impactante: a integração da mecânica quântica na criptografia. Essa abordagem, ao contrário da criptografia clássica, depende da física quântica para oferecer uma segurança inédita e robusta.

Em 2022, o governo dos EUA emitiu diretrizes para avaliar sistemas vulneráveis a ataques quânticos. Além disso, o investimento global em startups de computação quântica aumentou, refletindo o interesse crescente nesse campo.À medida que nos aproximamos dessa nova era, as decisões atuais desenharão o futuro da segurança cibernética. O impacto da computação quântica nos negócios é inegável. Nosso ecossistema digital depende da confiabilidade dos métodos criptográficos para garantir a segurança dos dados. Ameaças quânticas são, portanto, uma ameaça direta ao funcionamento desse ecossistema.

No Brasil, em setembro de 2022, a Agência Brasileira de Inteligência (ABIN) lançou a libharpia, uma biblioteca criptográfica com suporte a algoritmos pós-quânticos [12]. Este anúncio ocorreu durante o XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, onde a ABIN apresentou a libharpia com o intuito de aprimorar a transparência e auditabilidade do código utilizado nas eleições de outubro. Essa iniciativa alinhou-se com a crescente necessidade de reforçar a segurança e a confiabilidade do processo eleitoral, fornecendo base para garantir a integridade das eleições no Brasil.

A Accenture prevê que, dentro de oito anos, a capacidade dos processadores quânticos poderá comprometer a criptografia atual. **Assim como a mudança para o ano 2000 exigiu ações específicas, a iminente era quântica demanda adaptações profundas na infraestrutura tecnológica.**

O NIST, recentemente, destacou a seleção de algoritmos resistentes à computação quântica, um marco crucial nessa transição. A meta é atingir a "agilidade criptográfica", adaptando-se rapidamente a ameaças emergentes e cumprindo novos padrões de conformidade.

Em conclusão, a ascensão da computação quântica apresenta desafios e oportunidades singulares para a criptografia. As organizações estão se antecipando, atualizando padrões e preparando-se para ameaças futuras. O futuro requer uma reavaliação de nossos sistemas e uma transição estratégica para garantir a segurança em uma nova era tecnológica.

4 REFERÊNCIAS

[1] Accenture, “Cryptography in a Post-Quantum World”, Outubro de 2018. [Online]. Disponível em: https://www.accenture.com/us-en/insights/technology/quantum-cryptography

[2] NSA, “Quantum Key Distribution (QKD) and Quantum Cryptography (QC)”. [Online]. Disponível em: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[3] NIST, “NIST Announces First Four Quantum-Resistant Cryptographic Algorithms”, Julho de 2022. [Online]. Disponível em: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[4] NIST, “Update on the NIST Post-Quantum Cryptography Project”. [Online]. Disponível em: https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2_post-quantum_dmoody.pdf

[5] IBM, “IBM scientists help develop NIST’s quantum-safe standards”, Julho de 2022. [Online]. Disponível em: https://research.ibm.com/blog/nist-quantum-safe-protocols

[6] IBM, “Expanding the quantum-safe cryptography toolbox”, Julho de 2023. [Online]. Disponível em: https://research.ibm.com/blog/new-quantum-safe-standards-NIST

[7] White House, “M-23-02”, Novembro de 2022. [Online]. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

[8] McKinsey & Company, “The Rise of Quantum Computing”, Abril de 2023. [Online]. Disponível em: https://www.mckinsey.com/featured-insights/the-rise-of-quantum-computing

[9] Physical Review APPLIED, “Induced-photorefractive attack against Quantum Key Distribution”, Março de 2023. [Online]. Disponível em: https://arxiv.org/abs/2303.10885

[10] University of California, “Lattice-based Cryptography”. [Online]. Disponível em: https://cseweb.ucsd.edu/~daniele/papers/PostQuantum.pdf

[11] Forbes, “Assessing The Quantum Threat By The Numbers-Finally”, Maio de 2023. Disponível em: https://www.forbes.com/sites/arthurherman/2023/05/17/assessing-the-quantum-threat-by----------the-numbers-finally/?sh=25721c051615

[12] GOV BR, “ABIN lança criptografia com algoritmos pós-quânticos para as eleições”, setembro de 2022. [Online]. Disponível em: https://www.gov.br/abin/pt-br/assuntos/noticias/abin-lanca-criptografia-com-algoritmos-pos-quanticos-para-as-eleicoes

LABORATÓRIO DE SEGURANÇA CIBERNÉTICA

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS