Universidade Paulista - UNIP

Otavio Augusto Mota

COMPUTAÇÃO QUÂNTICA E SEUS EFEITOS NA CRIPTOGRAFIA

Limeira

2023

Universidade Paulista - UNIP

Otavio Augusto Mota

COMPUTAÇÃO QUÂNTICA E SEUS EFEITOS NA CRIPTOGRAFIA

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da computação sob a orientação do professor Me. Antônio Mateus Locci.

Limeira

2023

Otavio Augusto Mota

COMPUTAÇÃO QUÂNTICA E SEUS EFEITOS NA CRIPTOGRAFIA

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da computação sob a orientação do professor Me. Antônio Mateus Locci.

Aprovada em XX de XXXXX de 201X.

BANCA EXAMINADORA

_____

Prof. Dr. Nome completo

_____

Prof. Me. Nome completo

_____

Prof. Esp. Nome completo

Dedicatória

Dedico este trabalho à minha família, amigos e namorada que me apoiaram para que seja possível a conclusão do curso.

“Uma mente que se abre a uma nova ideia jamais voltará ao seu tamanho original.” - Albert Einstein.

RESUMO

Seria um eufemismo dizer que a criptografia é um controle de segurança fundamental. Por milhares de anos, as comunicações militares foram criptografadas e protegidas usando algum tipo de modelo de criptografia; desde o algoritmo alternativo básico na época de Kaiser, até a famosa máquina enigma usada pelo exército alemão na segunda guerra mundial, e ainda conhecida hoje como criptografia de nível militar. Levando isso em consideração, faz-se muito tempo desde que a proteção de dados não era mais um tópico limitado aos militares. Empresas e até indivíduos deveriam usar criptografia para proteger suas informações, inclusive de redes Wi-Fi, de dados pessoais regulamentados pelo GDPR (General Data Protection Regulation), para transações financeiras que exigem confidencialidade, integridade e não repúdio. Este trabalho tem como objetivo geral, discursar sobre a criptografia quântica e a partir disso, apresentar de que maneira ela interfere na segurança das informações em meio a era digital.

Palavras-chaves: Criptografia. Quântica. Segurança da Informação.

ABSTRACT

It would be an understatement to say that encryption is a fundamental security control. For thousands of years, military communications have been encrypted and secured using some type of encryption model. From the basic Alternate Algorithm in Kaiser's time to the famous Enigma machine used by the German Army in WWII, and still known today as military grade cryptography. Of course, it's been a long time since data protection was no longer a topic limited to the military, companies and even individuals should use encryption to protect their information, including from Wi-Fi networks, from personal data regulated by the GDPR (General Data Protection Regulation), to financial transactions. that require confidentiality, integrity and non-repudiation. This work has the general objective of discussing quantum cryptography and based on that, to present how it interferes with the security of information in the digital age.

Keywords: Encryption. Quantum. Information security.

Sumário

1 INTRODUÇÃO

1.1 Contextualização

A criptografia é um estudo associado à segurança de dados, que tem modelos matemáticos para garantir a privacidade e originalidade das informações entre as partes. A transposição e substituição são dois principais métodos da criptografia, que utilizam modelos matemáticos denominados algoritmos: simétricos e assimétricos. Eles são utilizados para criptografar e descriptografar mensagens por meio de chaves ou cifras. A criptografia simétrica utiliza uma única chave para tornar texto simples em texto cifrado e também para tornar texto cifrado em texto simples, enquanto a criptografia assimétrica usa cifras diferentes para isso. Esses dois algoritmos são feitos por meio da geração de chaves, as quais demandam considerável tempo para serem quebradas nos computadores atuais. No entanto, ao “reunir” processadores, há um aumento na chance de comprometer um sistema criptográfico, proporcional ao número de equipamentos executando a mesma operação. Na computação clássica, as informações são codificadas em bits, os quais podem existir exclusivamente em um dos dois estados binários possíveis (0 ou 1). Em um computador quântico, os análogos aos bits podem coexistir em uma superposição de estados (representando simultaneamente 0 e 1), formando um qubit (quantum bit), que, por sua vez, podem assumir uma superposição de todas as suas potenciais condições (FORD, 1997).

Criptografia quântica se fundamenta no princípio de que a informação quântica não pode ser clonada. Na verdade, é um pré-requisito para a distribuição segura de chaves privadas e não obrigatoriamente compartilha processos e metas idênticas aos da computação quântica. A ideia central implica a transmissão de “fótons” ao invés de focar no modo como são processados, sugerindo que não há uma conexão direta entre elas, apenas que ambas têm suas bases na física quântica (BENNETT, 1984).

Os sistemas de criptografia quântica garantem segurança absoluta contra tentativas de interceptação sem o consentimento do remetente ou destinatário,

pois não é viável realizar a medição do estado quântico de qualquer sistema sem interferir nele (SHOR, 1994).

1.2 Objetivo geral

Este trabalho tem como objetivo geral abordar a criptografia baseada em princípios quânticos e, a partir disso, explorar sua influência na proteção das informações na era digital.

1.3 Objetivo específico

A fim de viabilizar a consecução do objetivo geral de estudo, foram formulados objetivos específicos, como forma de restringir logicamente o raciocínio descritivo apresentado neste estudo. Neste tema abordarei a relevância da criptografia baseada em princípios quânticos e seus impactos na área de proteção de dados, além de analisar as vantagens e desvantagens desse tipo de criptografia.

1.4 Justificativa

Há uma enorme necessidade de usar criptografia para proteger as identidades e os dados dos usuários. No caso de tentativa de invasão, o sistema de criptografia protege todas as informações importantes: dados pessoais dos usuários e conteúdo de arquivos, bem como mensagens trocadas. Considerando os recentes casos de violação de dados que causaram verdadeiros escândalos na internet e a entrada em vigor da LGPD (Lei Geral de Proteção de Dados) em setembro de 2020, torna-se claro a relevância da aplicação de técnicas

criptográficas como medida de segurança para as empresas. No entanto, os usuários também estão expostos em seu ambiente doméstico. Todos nós estamos procurando ou compartilhando informações online hoje em dia, então nossos dados são armazenados em algum lugar. Em muitos casos, é impossível determinar se o ambiente de armazenamento é seguro. Por isso, é importante se proteger com criptografia, e aumentar a segurança e a privacidade ao usá-la em casa.

2 REFERENCIAL TEÓRICO

2.1 Aspectos gerais da criptografia

Quando informações ou dados são compartilhados pela Internet, eles passam por uma variedade de dispositivos em rede em todo o mundo que fazem parte da Internet pública. À medida que trafegam pela Internet pública, os dados correm o risco de serem comprometidos ou roubados por crackers. Para evitar isso, os usuários podem instalar software ou hardware específico para garantir a transmissão segura de dados ou informações. Esses processos são conhecidos na segurança cibernética como criptografia (BENNETT, 1992).

A criptografia envolve a conversão de texto simples legível por humanos em texto incompreensível, conhecido como texto cifrado. Essencialmente, isso significa pegar dados legíveis e transformá-los de maneira a parecerem aleatórios. A criptografia envolve a utilização de uma chave composta por um conjunto de valores matemáticos com os quais o remetente e o destinatário concordam. O destinatário usa a chave para descriptografar os dados, restaurando-os em texto simples legível (BENNETT, 1984).

Quanto mais complexa a chave, mais segura a criptografia, pois é menos provável que um terceiro consiga descriptografá-la por meio de um ataque de força bruta (ou seja, tentar combinações de valores aleatórios até que a combinação correta seja adivinhada). A criptografia também é usada para proteger senhas. Os métodos de criptografia de senha embaralham suas senhas para que não possam ser lidas por hackers (HAAS, 2005).

Os dois métodos mais comuns são criptografia simétrica e assimétrica. Esses nomes referem-se à chave que é usada para criptografia e descriptografia (HEISENBERG, 1958).

Chave de criptografia simétrica: também conhecida como criptografia de chave privada. A chave usada para criptografia é a mesma chave usada para a descriptografia, que é a melhor escolha para usuários individuais e sistemas fechados. Caso contrário, a chave deve ser enviada ao destinatário. Isso aumenta o risco de comprometimento se for interceptado por terceiros, como um

hacker. Este método é mais rápido que o método assimétrico (SCHARA FRANCESE, 2008).

Chave de criptografia assimétrica: esse tipo usa duas chaves diferentes, uma chave pública e uma chave privada, que são relacionadas matematicamente. Essencialmente, as chaves são apenas números grandes que combinam entre si, mas não são idênticos, daí o nome assimétrico. A chave privada é mantida em segredo pelo usuário, enquanto a chave pública é compartilhada entre destinatários autorizados ou disponibilizada ao público. Os dados criptografados com a chave pública do destinatário só podem ser descriptografados com a chave privada correspondente (EKERT, 1991).

Um sistema de segurança deve fornecer garantias como confidencialidade, integridade e disponibilidade dos dados. Quando usada corretamente, a criptografia ajuda a fornecer essas proteções. A criptografia assegura a privacidade e a integridade dos dados em trânsito e em repouso. Ele também pode autenticar mutuamente o remetente e o destinatário. Um sistema de software geralmente possui vários terminais, geralmente vários clientes e um ou mais servidores de back-end (HEISENBERG, 1958).

Essas comunicações cliente-servidor ocorrem em uma rede não confiável. As comunicações podem ocorrer em redes públicas abertas, como a internet, ou em redes privadas suscetíveis a serem comprometidas por estranhos ou internos mal-intencionados (SINGH, 2001).

A proteção de confidencialidade e integridade fornecida por protocolos de criptografia, como SSL/TLS, pode proteger as comunicações contra interceptação maliciosa e adulteração (SCHARA FRANCESE, 2008).

Também pode ser usado para proteger dados em repouso. Os dados em discos ou bancos de dados removíveis podem ser criptografados para evitar a confidencialidade se a mídia física for perdida ou roubada (FORD, 1997).

Além disso, ele pode fornecer proteção de integridade de dados em repouso para detectar adulteração maliciosa, alterando o conteúdo para que possa ser manipulado (STIX, 2005).

2.2 Sobre a criptografia quântica

Devido aos fenômenos distintos observados em escalas subatômicas, surgiu um novo ramo científico conhecido como mecânica quântica. Essa área aborda o processo de como os átomos emitem ou absorvem luz em comprimentos de ondas específicos, à medida que os elétrons transacionam entre diferentes níveis de energia em suas órbitas. A palavra em latim “quantum”, traduzida para o português como “quantidade”, é usada nos dias de hoje para representar a menor fração mensurável de uma característica física, como energia ou matéria (HEISENBERG, 1958).

De acordo com o princípio da incerteza de Werner Heisenberg, essa teoria sugere que não é possível medir com precisão tanto o trajeto quanto a velocidade de uma partícula ao mesmo tempo. Isso ocorre porque não podemos ter certeza do seu posicionamento e, ao localizá-la, não podemos medir sua velocidade a partir da posição; quando tentamos observá-las, notamos múltiplos valores no mesmo tempo (em um estado de superposição), ao invés de um único valor definido. No entanto, ao observá-los, ocorrem perturbações que alteram o sistema, resultando na quebra dessa superposição. Isso provoca a transição para um dos possíveis estados de maneira aleatória. Duas das características mais significativas desse campo abrangem os conceitos de superposição e entrelaçamento. Em oposição aos fundamentos da física clássica, esse campo segue a incerteza e a probabilidade, confirmando a natureza ondulatória de todas as partículas. Além disso, a energia liberada é quantizada com valores definidos, fixos e não divisíveis. (STIX, 2005). Isso ocorre porque as partículas não ocupam posições específicas. Eles existem simultaneamente em múltiplos locais, cada um com diferentes probabilidades de ser observado. Portanto, é impossível determinar simultaneamente tanto a posição quanto a velocidade da partícula. No mundo da física quântica, essa incerteza fundamental é inevitável, impactando a segurança do sistema (PACHECO, 2003).

Na matemática, esse princípio transcende a teoria e é expresso de forma mais abrangente como: $\Delta xi\, \Delta pix \geq h/2\pi$, implicando que quanto menor o erro na medição da posição da partícula, maior será o erro associado ao momento linear, e vice-versa. No entanto, na física quântica, a aleatoriedade prevalece,

respeitando a possibilidade de cada estado possível. Essa definição desafia o princípio da causalidade absoluta na física clássica, sugerindo a aplicação da mecânica quântica na descrição de sistemas criptográficos (PACHECO, 2003).

O nascimento da criptografia quântica teve origem em um trabalho não publicado oficialmente pelo físico Stephen Wiesner, da Universidade de Columbia, em 1960, intitulado “Quantum Currency”, onde foi proposta a concepção de papel-moeda resistente a fraudes. Porém, essa ideia vanguardista foi inicialmente desacreditada. Posteriormente, Wiesner compartilhou sua proposta com seu colega e pesquisador da IBM, Charles H. Bennett, em 1980. Bennett se interessou pelo conceito e discutiu-o com seu outro colega e pesquisador, Gilles Brassard, gerando diversas ideias e percebendo potenciais aplicações na criptografia quântica (BENNETT, 1984).

A robustez da criptografia quântica se fundamenta na intrínseca incerteza presente no microcosmo, refletida pelo princípio da incerteza. Explorando a instabilidade inerente das partículas em sistemas de processamento quântico, é viável transmitir dados, como códigos ASCII, de modo seguro através de canais ópticos denominados mídia quântica. Nestes canais, conhecidos como meio quântico, a interceptação de partículas de luz (fótons) resulta em perturbações que afetam drasticamente o sinal, tornando impossível para um invasor capturar a informação binária contida. Essa incerteza intrínseca é aproveitada para gerar chaves, pois os fótons exibem vibrações angulares específicas enquanto atravessam o meio óptico, conferindo aos bits clássicos suas representações distintas (BENNETT, 1992).

Ao contrário da computação clássica, os dados quânticos ao serem lidos resultam em suas alterações. Essa é uma barreira impossível de passar no mundo quântico, já que não pode ser superada, mesmo com equipamentos sofisticados, devido à própria natureza da medição ou interações simples com os qubits causam erros, conhecido como decoerência (SINGH, 2001).

Dessa forma, o conceito central de criptografia quântica implica a transmissão de feixes de fótons com polarização provenientes de lasers por meio de um caminho óptico, ao invés de proteger o texto com métodos criptográficos convencionais. Refere-se ao procedimento de garantir a distribuição segura e inquebrável de chaves, empregando técnicas de comunicação e conceitos da física quântica para a troca de chaves entre remetente e destinatário, sem a

necessidade de conhecimento prévio do canal compartilhado. Considerando a natureza intrínseca de incerteza no mundo quântico, é possível reduzir a eficácia de ataques de interceptação conhecidos na segurança da informação, como os “man-in-the-Middle” (homem no meio). Isso permite que as partes envolvidas troquem chaves de forma segura através de canais públicos (PACHECO, 2003).

Essa chave de criptografia consiste em um conjunto de qubits que são representados pela polarização de um fóton ou até mesmo por múltiplos fótons. Seu comprimento pode variar diretamente dependendo do tipo de implementação do algoritmo a ser aplicado.

No entanto, uma regra básica da criptografia é que “o número de bits usados para criar uma chave é proporcional à sua inviolabilidade", então quanto mais bits usados em uma chave, mais segura ela é (EKERT, 1991).

Esses fótons passam por um “filtro de polarização”, o qual pode ser avaliado com base em diferentes orientações: retilínea (Å) - horizontal (90º, ↔), vertical (0º, ↕); ou diagonal (Ä) - esquerda (135º, ↖) , direita (45º, ↗). Esse esquema é caracterizado pela rotação no sentido horário ou anti-horário. Em ambos os casos, essas polarizações são interpretadas como representações de 0s (zeros) e 1s (uns) no sistema binário (EKERT, 1991).

2.3 Segurança da informação

A internet corresponde a uma grande parte de uma rede de computadores, e é nesse ambiente onde acontecem os maiores ataques cibernéticos que se tem conhecimento. No contexto que corresponde a rede de computadores a segurança entra com um significado de táticas que diminuam os riscos corridos naturalmente no meio online. Dessa forma, de maneira mais objetiva o autor Moraes (2010) coloca a segurança como a parte da rede de computadores que fica responsável por analisar, prever e estabelecer metodologias que inviabilizam possíveis invasões e ataques a mesma.

Além disso, Moraes (2010), enfatiza também que a segurança de uma rede de computadores deve estar apta para identificar e eliminar qualquer defeito que possa ser utilizado por terceiros para invadir, modificar, deletar, coletar ou

inserir informações sem autorização prévia do detentor desta rede. A importância dessas medidas de segurança é exemplificada por executar as medidas de proteção para as informações contidas nessa rede de computadores, alterações, vazamentos e mudanças na finalidade dos processos executados por esses computadores. Muitas das atividades criminosas executadas após a consolidação dos computadores e da internet na realidade de boa parte das pessoas do mundo, contam com a invasão da rede de computadores da vítima. Os dados contidos nessas redes são extremamente valiosos para os seus usuários, não apenas no caso de grandes empresas, mas também quando se trata de pessoas comuns. Dessa forma, estes são usados por criminosos como objetos de ameaça em busca de quantias de dinheiro ou apenas para que esses dados sejam divulgados e passem a ser de conhecimento público.

Segundo Mitshashi (2011), usar a internet não pode mais ser tão associado a algo pessoal, isso porque o grande crescimento da busca por aplicativos e formas de compartilhamento tirará essa característica do ponto central desse meio. A demanda por ferramentas que possibilitem a transferência de informações, imagens, arquivos, documentos, mensagens e vídeos para uma quantidade cada vez maior de pessoas em um espaço de tempo cada vez menor, tornou a internet um espaço muito mais social do que individual. Esse cenário tem suas vantagens baseadas no fortalecimento das relações interpessoais entre pessoas independente da distância em que elas estejam uma das outras. Por outro lado, favorece as invasões e o roubo desses dados que são compartilhados diariamente.

O sucateamento do cabeamento de maneira geral e a substituição do mesmo pela nova tecnologia que torna as redes de internet sem fio, também foi um dos fatores que mais contribuiu para o aumento desses crimes ocorrido em ambiente virtual. Devido ao fato de que os cuidados e as políticas de segurança de uma rede sem fio (via Wi-Fi) são muito mais complexos e extensos do que a rede quando passada através de cabos. Tendo a sua disposição uma máquina com uma placa de rede sem fio e um ponto de conexão para sustentar essa conexão, o usuário pode navegar livremente na internet. Entretanto, aqueles que acessam essas redes têm mais facilidade para conseguir captar os dados dos quais desejam (MITSHASHI, 2011).

Logo, como afirma o autor, as redes sem fio são comprovadamente menos seguras do que as redes que utilizam cabos, em sua natureza. Dessa forma, muitas foram as políticas de segurança desenvolvidas, implantadas nas redes de computadores domésticas e profissionais, para que houvesse a resolução das brechas criadas por essa nova tecnologia. Entretanto, esses sistemas de invasão estão sempre sendo atualizados e se desenvolvendo para conseguirem criar brechas naquelas redes que não as possuem, de modo que essas políticas de segurança devem se atualizar nessa mesma velocidade. A criptografia é uma das formas de segurança mais comuns nas redes de computadores. Através da formulação de códigos indecifráveis, apenas os usuários que possuem autorização para acesso a estas informações são capazes de tomar conhecimento delas. O sistema desenvolvido é capaz de identificar e criar chaves que codificam as palavras contidas de modo que elas passem a estar codificadas de maneira completa. A criptografia é muito antiga e é considerada uma área da matemática e não está relacionada a computadores em sua essência (STALLINGS, 2008).

Os vírus para computadores, celulares e outras ferramentas tecnológicas representam um grande problema para o século XXI. Esses são programas desenvolvidos unicamente para adentrar nos sistemas sem serem notados pelo usuário e impedir o bom funcionamento dos mesmos, roubar, editar e excluir dados que nele estejam contidos (NAKAMURA, 2010).

O autor ainda enfatiza que o desenvolvimento dos programas conhecidos como “Antivírus” ameniza o caos cibernético que havia se instalado no cenário atual que se encontrava totalmente conectado e era comumente invadido e furtado por tais programas que entram sorrateiramente em suas redes de computadores. Ao longo do tempo e com o aumento da demanda devido à necessidade de segurança dos arquivos mantidos nas redes de computadores, muitos foram os programas criados para fechar as brechas deixadas por alguns dos sistemas contidos nessas redes. De modo que esse mercado precisa se reinventar em um período muito curto, para continuar atendendo as necessidades do mercado (NAKAMURA, 2010).

3 DESENVOLVIMENTO

3.1 Material e Métodos

Este estudo caracteriza-se mediante a uma revisão da literatura com abordagem qualitativa. Com isso, torna-se possível coletar diversas informações atualizadas sobre um determinado contexto, permitindo aos pesquisadores atualizarem-se e realizarem inferências pertinentes para a comunidade científica (GONÇALVES, 2019).

Nesse processo tratou-se da busca de pesquisas relacionadas à temática, ademais, essa ação foi realizada por meio de plataformas científicas, bibliotecas e bases de dados diversas, como por exemplo: Scientific Electronic Library Online (SCIELO), Google Scholar, Scopus Elsevier, Cochrane Library, Web of Science, dentre outros.

3.2 Metodologia

De acordo com Lakatos (1998), a pesquisa foi desenvolvida e classificada com o propósito de atingir o objetivo da pesquisa de forma mais eficiente. Para mais, a revisão bibliográfica originou-se a partir da necessidade que pesquisadores encontraram para desenvolver métodos lineares de pesquisa, com rigor metodológico claramente definido e, acima de tudo, com descrição de etapas que pudessem ser seguidas por outros pesquisadores, ou seja, que seus métodos fossem de fácil replicação ou adaptação ao contexto mais próximo àquele que pesquisa (GONÇALVES, 2019).

A revisão de literatura contribui para que os pesquisadores identifiquem como o campo de pesquisa tem se posicionado acerca de determinada temática, possibilitando que a partir do levantamento dos resultados apontados em diversos estudos, convergem em um ponto de singularidade englobando a visão

de todos os estudiosos, formulando conceitos, sentidos e contextos amplos sobre diversos temas (CARVALHO, 2020).

Visto isso, ela segue a premissa de uma abordagem qualitativa dos estudos selecionados, pois, detém-se a qualidade das informações retratadas, independente da metodologia utilizada por esses estudos, pois, estudos qualitativos, contribuem para que os pesquisadores analisem o contexto que se detém e, assim, concretizem seu posicionamento sobre a temática pesquisada (GALVÃO; RICARTE, 2019).

3.3 A importância da criptografia quântica na segurança

O foco na relação entre computação quântica e segurança da informação não é acidental. Isso porque criptografia e segurança cibernética são dois campos que terão um grande impacto nos computadores quânticos. Transações com cartão de crédito, bancos de dados das empresas e outras informações confidenciais são notoriamente criptografadas. A propósito, o mundo "depende da criptografia para proteger tudo", conforme mencionado em um artigo feito pelo MIT Technology Review (FORD, 1997).

Conforme explicado no artigo, um novo relatório publicado pelas Academias Nacionais de Ciências, Engenharia e Medicina destaca a importância da "preparação acelerada para uma era em que computadores quânticos superpoderosos quebram as defesas criptográficas tradicionais" (BENNETT, 1992).

Segundo o artigo, é possível ter máquinas quânticas de alto desempenho. E, "se os hackers colocarem as mãos nele, o resultado pode ser um pesadelo de segurança e privacidade", observam os autores (BRASSARD, 1984).

Isso significa que, se os computadores quânticos caírem em mãos erradas, eles teoricamente seriam capazes de usá-los para comprometer sistemas seguros que são considerados imunes a ataques de computação clássicos. Portanto, o acesso a dados previamente protegidos é permitido (DEUTSCH, 1985).

Apesar dos riscos, "a computação quântica também pode ajudar a melhorar nossa capacidade de proteger dados críticos e pessoais, principalmente no que diz respeito ao aprendizado de máquina quântica e à geração de números aleatórios quânticos", disse Chris Hockings, diretor de tecnologia da IBM Security Austrália e Nova Zelândia (HEISENBERG, 1958).

Anomalias comportamentais podem ser detectadas por meio de aprendizado de máquina e, portanto, será possível prever ameaças, explicou. Outro artigo publicado pelo Financial Times analisou que as ameaças quânticas surgem em um momento em que a Internet das Coisas e o 5G estão se aproximando e os requisitos de segurança são maiores do que nunca. De acordo com o texto, existem duas abordagens gerais para formar um futuro quântico seguro (SCHNEIDER, 2005).

A primeira opção constitui-se na criação de novos algoritmos que, na visão de muitos matemáticos e cientistas da computação, não devem ser violados nem mesmo pelos computadores quânticos mais poderosos. A segunda opção é construir uma solução física baseada na mecânica quântica. Ao contrário dos algoritmos, os computadores quânticos podem gerar números verdadeiramente aleatórios sem padrões. Apenas estes são resistentes a hackers por outros computadores quânticos. Muito se discute sobre computação quântica e segurança da informação. Além disso, várias empresas têm trabalhado no desenvolvimento de produtos quânticos cada vez mais seguros (SCHNEIDER, 2005).

3.4 A computação quântica e seus efeitos na criptografia

No ano de 1982, Richard Feynman propôs propriedades quânticas para a geração de computadores. Ao contrário da computação clássica, na qual a informação é codificada em bits, os computadores quânticos permitem que esses bits existam em superposição. Um bit pode estar apenas em apenas um estado voltaico representativo, enquanto um qubit pode assumir uma superposição de todos os estados possíveis (HAAS, 2005).

Uma vez que os registradores estão no estado sobreposto do estado desejado, as operações de todos os números 2x podem ser executadas simultaneamente, enquanto os computadores convencionais requerem velocidade de processamento de dados em um computador quântico, pois basta um certo número de qubits estar no estado 2x ao mesmo tempo, o que significa que a possibilidade real de quebrar uma chave rapidamente é faturar números muito grandes e consiste em vários termos de um polinômio algébrico, para grande tristeza dos criptoanalistas. Outras opções para o uso da técnica são: simulação de teoria física, realização de análises estatísticas, problemas astrofísicos, e tratamento de problemas que envolvem uma grande quantidade de termos e variáveis (STIX, 2005).

Matematicamente falando, um computador quântico é um equipamento que utiliza diretamente a peculiaridade da mecânica quântica, que é a superposição e interferência, para realizar cálculos, a manipulação da superposição do clássico zero e um, que pode ser expressa como : |qubit> = p |zero > + q |um>, onde “|zero>” significa o bit “0” e |um> significa o bit “1”; p e q são valores numéricos, escritos na forma z = p + qi. Entretanto, se “p” e “q” forem números reais, a probabilidade medida de um resultado 0 é “p^2” e um resultado 1 é “q^2”. Esta notação permite visualizar o estado do qubit como um ponto na superfície de uma esfera, denominada esfera de Bloch, onde |0> pode ser o polo norte da esfera e |1> pode ser o polo sul (STIX, 2005).

Nesse emaranhamento, cada qubit empregado pode existir 0s e 1s simultaneamente, permitindo que um computador quântico execute 2x cálculos simultâneos, onde x representa o número de qubits necessários. Se o computador consistir em 1.000 qubits, isso implica que um processo pode realizar 21.000 cálculos. Sua capacidade cresce exponencialmente à medida que mais qubits são adicionados. Esta configuração atualmente não tem limite virtual (PACHECO, 2003).

Para entender melhor, vamos pegar o exemplo de uma chave cuja raiz é um produto entre 2000, como 7412 x 6547, para resolver essa questão bastam alguns nanossegundos. No entanto, para obter o produto de X vezes Y, 48.526.364, levará muito mais tempo porque não temos um processo de fatoração rápido o suficiente. Se o desfecho resultar da multiplicação de números primos, a situação se complica ainda mais. Usar números de vários dígitos para

decompor significa um extenso tempo e processamento de computação, tornando o processo de decifração comercialmente inviável, porque agora as informações criptografadas expiram quando suas chaves criptográficas são quebradas, já que os números primos são escolhidos para criar essas chaves. São centenas de casas, por isso, torna-se muito complexa a destruição delas por meio de computadores eletrônicos (BENNETT, 1992).

No entanto, esse cenário de segurança muda a partir da utilização de computadores quânticos, que podem partir grandes chaves em um curto espaço de tempo. Com o algoritmo de Shor(criado por Peter Shor, da AT & T Bell Laboratories, em 1994, para computação de modelo formal), é possível testar e calcular inúmeras soluções de maneira simultânea. Ele é muito eficiente quando o assunto é a decomposição de valores primos complexos por divisores não triviais da razão não em O ($\log^3 n$). Em 1996, Lov Grover, da Bell Labs, projetou um método de busca ultrarrápida na lista de chaves para decifrar a cifra DES, explorando todas as combinações possíveis de chaves e obteve sucesso. Se esses métodos forem implementados, eles avançam os modelos tradicionais da computação voltados à confidencialidade da informação (PACHECO, 2003).

O maior desafio na construção de uma máquina quântica está diretamente relacionado a evitar perturbações nesse sistema, as quais interferiram nas informações. Essa interferência, ao interagir com o ambiente, torna o comportamento imprevisível e excessivamente complexo, dificultando a correlação entre os quantum bits. O desafio atual está na impossibilidade de armazenar subpartículas que estejam emaranhadas ou polarizadas, devido à instabilidade da forma física do qubit em períodos prolongados. Isso exigirá a criação de dispositivos herméticos, tais como memórias quânticas, capazes de reter qubits sem provocar alterações neles (WIESNER, 1970).

Foi somente quando a pesquisa passou a priorizar a transmissão de fótons, em vez de seu armazenamento, que obteve-se sucesso, transformando a criptografia quântica em uma ciência prática e viável, com amplas aplicações em segurança (WIESNER, 1970).

3.5 Vantagens e desvantagens da criptografia quântica

Como qualquer tecnologia, a criptografia quântica tem suas vantagens e desvantagens. Suas vantagens inspiraram vários estudos nessa área por décadas, incluindo garantias de confiabilidade e segurança baseadas nos princípios físicos e não em suposições de computabilidade. Por outro lado, dificuldades severas de implementação, combinadas com o alto custo para construir computadores quânticos confiáveis, dificultam a adoção em massa da computação quântica e da segurança associada à mesma (FORD, 1997).

Graças ao princípio da incerteza de Heisenberg, um espião que está monitorando as comunicações em uma troca de chaves pode ser detectado porque a medição dos qubits enviados altera o valor desses dados. Ao perceber a presença de um intruso, a transmissão é abortada para garantir o sigilo das informações (FORD, 1997).

Apesar da segurança oferecida pela distribuição de chaves quânticas, não é possível evitar todos os tipos de ataques. A característica probabilística da mecânica quântica não assegura a eliminação total de todas as oportunidades de intrusão (PACHECO, 2003).

A segurança absoluta é proporcionada pela criptografia quântica quando um intruso pode apenas ouvir passivamente a comunicação. No entanto, se ele tiver a capacidade de interceptar os dados transmitidos e reenviá-los, é possível selecionar os dados corretos, obter dados confidenciais e enganar sem que as partes percebam (PACHECO, 2003).

Por razões práticas, é difícil seguir estritamente o modelo teórico e enviar um único fóton com polarização de luz. Isso possibilita que o espião dívida o feixe e leia as informações interceptadas sem modificar a polarização (apenas a intensidade) do feixe recebido pelo destinatário, permitindo ao espião descobrir a chave de transmissão, a base adequada para medir e tornar as informações úteis (SCHARA FRANCESE, 2008).

Mesmo sem bugs passivos, a passagem de fótons seria perturbada por ruídos no ambiente, e tais perturbações seriam indistinguíveis umas das outras. Portanto, o transmissor e o receptor devem aceitar algum nível de perturbação na transmissão, independentemente de estar contaminada ou não. Dessa forma,

o espião, embora não consiga obter os dados, pode interromper a transmissão introduzindo interferência até que ela falhe, frustrando assim o objetivo do remetente (SCHARA FRANCESE, 2008).

Apesar de todas as pesquisas teóricas e experimentos práticos sobre o tema, a aplicação em larga escala da computação e criptografia quânticas ainda não está disponível (STIX, 2005).

Existem sérias dificuldades físicas em construir um computador quântico com poder de processamento suficiente para ser útil a um custo igualmente alto. Por exemplo, fatorar um número de 200 dígitos usando o algoritmo de Shor requer 3.500 qubits estáveis – no entanto, além de tornar esses qubits difíceis de emaranhar, eles gradualmente sofrem de um efeito chamado decoerência, caso em que se emaranham com o ambiente e perdem o contato um com o outro. Mesmo em uma caixa isolada, a decoerência pode ocorrer após dezenas de nanossegundos (PACHECO, 2003).

A transmissão de fótons também é muito sensível a erros, com a taxa de erro aumentando com a velocidade de transmissão ou a distância entre os pontos finais. A correção quântica de erros (QEC) é uma saída possível, pois a pesquisa mostra que ela é mais eficaz do que as técnicas de correção de erros usadas nas comunicações tradicionais (SCHARA FRANCESE, 2008).

4 CONSIDERAÇÕES FINAIS

Em breve, a presença de computadores quânticos poderá ser mais real do que se imagina, comprometendo a utilização dos valores criptográficos clássicos assimétricos. A segurança da informação pode ser grandemente fortalecida pela criptografia quântica, pois a distribuição de chaves quânticas oferece uma alternativa altamente segura em comparação com o uso da criptografia assimétrica clássica. Isso permite que dois pares troquem mensagens de forma segura, sem o receio de comprometer suas informações, eliminando a necessidade de esquemas complexos de servidores e validadores centrais para chaves e autenticação.

Também é uma vantagem sobre outros métodos de criptografia, visto que é possível a identificação de intrusos passivos, sendo condicionalmente seguro, embora paradoxalmente, mesmo para alto poder de computação, sua segurança continha intrinsecamente relacionada à extensão da chave utilizada.

A criptografia de chave pública, conhecida como criptografia assimétrica, conta com uma série de algoritmos matemáticos considerados complexos demais para serem quebrados, principalmente quando se utilizam chaves de criptografia de comprimento aceitável, como por exemplo: RSA-2048 e ECDSA-256. Da mesma forma, mesmo com altas quantidades de poder de computação tradicional, em alguns casos levaria a idade de nosso universo para garantir que a criptografia fosse quebrada.

Na computação quântica, tudo muda. Algo como o algoritmo de Shor pode ser usado, pois explora os fenômenos quânticos para simplificar a decomposição dos números em seus componentes principais (números primos), o que é basicamente inviável para computadores comuns quando os números são muito grandes. Muitos algoritmos de criptografia assimétrica, como o RSA, são baseados na suposição de que a fatoração de números inteiros grandes é computacionalmente inviável. Até agora, essa suposição é verdadeira para computadores clássicos, mas uma máquina quântica hipotética, com capacidade suficiente de Qubit (qubit), poderia quebrar o RSA e outros algoritmos semelhantes, formando a criptografia de chave pública essencialmente em um controle de medidas de segurança desnecessárias.

5 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. NBR 6023: Informação e documentação: referências: elaboração. VERSÃO CORRIGIDA ATUALIZADA: ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Rio de Janeiro, 2002.

ABNT. NBR 6028: resumo: elaboração. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Rio de Janeiro, 2002.

BENNETT, C. H., BESSETTE, F., BRASSARD, G., SALVAIL, L., SMOLIN, J., “Experimental Quantum Cryptography”, Journal of Cryptology, 1992. BRASSARD, G., “Bibliograph of Quantum Criptography”, 1984.

BENNETT, C. H., BRASSARD, G., “Quantum cryptography: Public-key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing”, 1984.

BENNETT, C. H., BRASSARD, G., EKER, A.K., “Quantum Criptography”, Scientific American, n. 267, 1992.

BRASSARD, G., CRÉPEAU, C., JOZSA, R., LANGLOIS, D., “A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties”, 1993.

BRASSARD, G., CRÉPEAU, C., MAYERS, D., SALVAIL, L., “A brief review on the impossibility of quantum bit commitment”, 1984.

DEUTSCH, D., “Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer”, 1985.

EKERT, A., “Introduction to Quantum Cryptography”, 1991.

FORD, J. C., “Quantum Cryptography”, Tutorial, 1997.

FORD, J., “Quantum Cryptography. Tutorial”, 1997.

HAAS, F., “Computação Quântica – Desafios para o século XXI”. 2005

HEISENBERG, W. “Physics and Philosophy: the Revolution in Modern Science. New York, Harper and Brothers.”, 1958.

MITSHASHI, R. Segurança de Redes. Monografia apresentada à Faculdade de Tecnologia de São Paulo – FATEC – para a obtenção do Grau de Tecnólogo em Processamento de Dados. São Paulo, 2011.

MONTEIRO, R. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil. Artigo estratégico, v. 39, p. 1-14, 2018.

MORAES, A.. Segurança em Redes – Fundamentos, Primeira Edição, São Paulo, Editora Érica 2010.

NAKAMURA, E. Tissato & Geus Paulo Lício de, Segurança de Redes – em ambientes cooperativos, Segunda Edição, São Paulo, Novatec Editora, 2010.

PACHECO, J. M. P., Criptografia Quântica, 2003.

SCHARA FRANCESE, J.P., “Criptografia Quântica”, Trabalho Final de Redes I – UFRJ, 2008.

SCHNEIDER, G.G., “Arquitetura de Computadores Quânticos”, Universidade Federal de RS, 2005.

SHOR, P. W., “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, 1994.

SINGH, S., O Livro dos Códigos: A Ciência do Sigilo – do Antigo Egito à Criptografia Quântica. RJ, Record, 2001.

STIX, G., “Os segredos mais bem guardados”, Scientific American Brasil, n. 33, 2005.

THING, L, “Dicionário de Técnologia”, Futura, 2003.

WIESNER, S., “Conjugate Coding”, Artigo, Sigact One News, 1970.