FACULDADES INTEGRADAS BARROS MELO
Curso de Sistemas de Informação

SPIKE LEE FIGUEIREDO BARBOSA

SUBSTITUIÇÃO DO CRIPTOSSISTEMA RSA PARA MCELIECE COM FINALIDADE DE INCREMENTAR A SEGURANÇA DE DADOS AMEAÇADA PELA COMPUTAÇÃO QUÂNTICA

Olinda
2019

SPIKE LEE FIGUEIREDO BARBOSA

SUBSTITUIÇÃO DO CRIPTOSSISTEMA RSA PARA MCELIECE COM FINALIDADE DE INCREMENTAR A SEGURANÇA DE DADOS AMEAÇADA PELA COMPUTAÇÃO QUÂNTICA

Projeto de pesquisa apresentado ao Curso de Sistemas de Informação, das Faculdades Integradas Barros Melo, como exigência para aprovação na Disciplina de Trabalho de Conclusão de Curso I e II (TCC), sob a orientação da Profª Rafaella Matos.

Olinda
2019

SPIKE LEE FIGUEIREDO BARBOSA

SUBSTITUIÇÃO DO CRIPTOSSISTEMA RSA PARA MCELIECE COM FINALIDADE DE INCREMENTAR A SEGURANÇA DE DADOS AMEAÇADA PELA COMPUTAÇÃO QUÂNTICA

Relatório final, apresentado às Faculdades Integradas Barros Melo, como parte das exigências para a obtenção do título de Bacharel no curso de Sistemas de Informação.

Olinda, ____ de _____ de 2019.

BANCA EXAMINADORA

_____
Prof. (Rafaella Matos)
Afiliações

_____
Prof. (Nome do professor avaliador)
Afiliações

_____
Prof. (Nome do professor avaliador)
Afiliações

A comunidade científica, que corajosamente se dispõe a contribuir para um mundo melhor através do conhecimento. Também dedico esse trabalho ao meu pai, que possibilitou que eu finalizasse meu curso ao me apoiar desde o princípio.

AGRADECIMENTOS

Agradeço a todos os professores que me ensinaram nesse curso, por ter sido parte fundamental para a minha formação. Em especial, agradeço ao meu primeiro orientador, Amirton Chagas, do qual me ensinou assuntos referentes a esse trabalho, despertando interesse da minha parte para seguir em frente com esse tema. Agradeço também a minha atual orientadora, Rafaella Matos, e a professora Sandra Helena, que contribuíram com a finalização dessa pesquisa por meio de suas correções e sugestões de aprimoramento. Também menciono meus pais, que nessa jornada sempre se dedicaram para me dispor de recursos e finalizar esse curso. Agradeço a todos que fizeram parte direta e indiretamente da minha formação, meus sinceros agradecimentos.

RESUMO

Nota-se a importância que a segurança de dados representa para a comunicação via internet, manter um criptossistema imune ao bit quântico é uma direção sensata a se seguir. O qubit (bit quântico) representa o grande diferencial entre computadores clássicos e quânticos. Esse bit especial suporta a superposição de estados, característica da qual é possibilitada pela mecânica quântica, e tem como base teórica a simultaneidade de estados, onde é possível fatorar números primos em tempo polinomial. Levando em consideração que o criptossistema RSA funciona com base em fatoração de grandes números primos, sugere-se que já existe uma necessidade de substituição do mesmo à longo prazo. O criptossistema McEliece funciona de forma semelhante ao RSA, com a distinção de que ele trabalha com inserção e resolução de erros durante a troca de texto cifrado, tornando-o assim imune à processamento quântico. Essa proposta deve ser estudada junto à teoria de uso de códigos MDPC no McEliece – ao invés de códigos de Goppa - como meio de viabilizar sua aplicação e tornar sua eficácia de tempo de decriptação próxima a do RSA. Essa monografia trabalha com a hipótese de substituição do algoritmo de chave pública RSA pelo McEliece com códigos MDPC como método de prevenir futuros ataques de segurança provindos de computadores quânticos.

Palavras-chave: criptografia pós-quântica. computação quântica. segurança de dados. criptossistema McEliece.

ABSTRACT

With the importance of data security for internet communication, maintaining a quantum bit immune cryptosystem is a sensible direction to follow. The qubit (quantum bit) represents the great difference between classical and quantum computers. This special bit supports the superposition of states, characteristic of which is made possible by quantum mechanics, and is based on the simultaneity of states, where it is possible to factor prime numbers in polynomial time. Given that the RSA cryptosystem works on factoring large prime numbers, it is suggested that there is already a need for long-term replacement. The McEliece cryptosystem works similarly to RSA, with the distinction that it works with error insertion and resolution during ciphertext exchange, thus making it immune to quantum processing. This proposal should be studied together with McEliece's theory of MDPC code usage - rather than Goppa codes - as a means of making its application and its decryption time effectiveness close to that of RSA. This monograph works on the hypothesis of replacing the RSA public key algorithm to McEliece with MDPC codes as a method to prevent future security attacks from quantum computers.

Key-words: post-quantum cryptography. quantum computing.data security. cryptosystem McEliece.

LISTA DE ABREVIATURAS E SIGLAS

AES -- Advanced Encryption Standard (padrão avançado de encriptação).

AMD -- Advanced Micro Devices (micro dispositivos avançados).

GHz -- GigaHertz.

MDPC -- Medium Density Parity Check (códigos de média densidade de verificação de paridade).

NTRU -- N-Th Degree Truncated Polynomial Ring (enésimo anel polinomial truncado em grau).

QUBIT -- Bit Quântico.

RAM -- Random-Access Memory (memória de acesso aleatório).

RSA -- Rivest-Shamir-Adleman.

XOR -- Porta lógica de disjunção exclusiva.

SUMÁRIO

1 INTRODUÇÃO

Pesquisadores e teóricos que estudam sobre computação quântica passaram as ultimas décadas discutindo e analisando novas tendências de progresso dessa tecnologia a fim de garantir a eficácia da criptografia nos próximos anos. Diante desse contexto, se faz necessário reunir conhecimentos práticos e teóricos sobre esse assunto e definir possíveis alternativas a isso. Essa pesquisa tem como foco analisar a hipótese de substituição do sistema criptográfico de chave assimétrica RSA (Rivest-Shamir-Adleman) pelo criptossistema de chave pública McEliece com códigos MDPC. A importância de se estudar tal caso concentra-se no crescente desenvolvimento e popularidade que computadores quânticos estão alcançando à medida que o tempo passa.

Como explicado por (SILVA, 2005), a base de funcionamento do criptossistema RSA depende fortemente da complexidade de se calcular gigantescos números primos. Ao passo que, de acordo com a pesquisa de (BITTENCOURT, SUMMA NETTO e VIGNATTI, 2004) o algoritmo de Shor, teoricamente, se mostrou capaz de fatorar tais números em tempo polinomial. Ainda que (CHEN, JORDAN, *et al.*, 2016) constate que o criptossistema RSA 2000-bits não seja quebrável por computadores quânticos construídos até o momento de elaboração desse trabalho, existem previsões de que nas próximas décadas essa nova forma de se computar dados tornará a base de funcionamento do RSA obsoleta.

Tendo como objetivo buscar identificar algum possível método preventivo de segurança de dados disponível no momento de produção deste trabalho envolvendo um criptossistema que de acordo com (HALLGREN e VOLLMER, 2009, p. 16), é teoricamente imune à capacidade de processamento de computadores quânticos – McEliece -, e sua viabilidade de execução, a pesquisa se encaminha em uma base essencialmente teórica de análise dessa situação.

Como descrito por (DIAS, 2019), o sistema criptográfico RSA é amplamente utilizado e aceito para comunicação atualmente, sendo essa pesquisa justificada pelo desejo coletivo de manter as propriedades de segurança de dados consolidadas por (BRASIL, 2013), abordando pautas relacionadas ao risco que ataques *man-in-the-middle* poderiam causar, e como esse impasse pode ser

solucionado, mesmo considerando o avanço cada vez mais acelerado do desenvolvimento de computadores quânticos.

A metodologia aplicada a essa pesquisa é bibliográfica, pois considera a impossibilidade de se realizar testes de eficácia de criptossistemas em computadores quânticos de alta capacidade, tendo em vista que ainda não há viabilidade de se produzir tais máquinas. A essência puramente teórica desse trabalho abordará físicos e pesquisadores pioneiros no que diz respeito à mecânica quântica, como o (BOHR, 2011), assim como novos estudiosos sobre o assunto. Dissertações, monografias, artigos em periódicos e mais, foram base formuladora desse trabalho.

O roteiro dessa pesquisa compõe em conceituar criptografia e segurança de dados, explicar o que consiste computação quântica e suas respectivas capacidades de processamento, relacionar computação quântica com sistemas criptográficos amplamente usados na atualidade, estabelecer algum sistema criptográfico candidato a substituto do atual RSA para incremento na segurança de dados à longo prazo.

2 CRIPTOGRAFIA E SEGURANÇA DE DADOS

De acordo com (GUGIK, 2009), no século XX, houve uma revolução tecnológica provinda de esforços coletivos de nações que buscavam desenvolver-se durante a segunda guerra mundial. Neste tempo, a preocupação com segurança de dados estava na sua incubadora, junto da consolidação do modelo de computação clássica. Segundo (ALMEIDA e NAPP, 2012), segurança de dados era ainda um conceito abstrato, e foi preciso alguns anos para se chegar a um consenso do que realmente seria necessário para garantir uma comunicação segura utilizando computadores. Adicionalmente, foi constatado por (ALMEIDA e NAPP, 2012) que a criptografia foi a peça chave que assumiu diversas formas pré-computação até os dias atuais, consistindo na aplicação de um protocolo onde não é permitido que terceiros, ou o público, tenham acesso a mensagens confidenciais. Essa maneira de transmitir dados foi essencial para comunicação efetiva em situações onde se fazia necessário a garantia de quatro propriedades, das quais formaram a Política de Segurança da Informação estabelecida por (BRASIL, 2013):

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Autenticidade.

Confidencialidade consiste na ideia de que somente pessoas autorizadas terão acesso ao conteúdo em questão, por exemplo, quando um sistema online de um banco define que somente o usuário deverá ter acesso aos dados confidenciais de sua própria conta, nesse caso, é um requisito de segurança que o banco garanta a confidencialidade dos dados pessoais do cliente. Problemas de segurança envolvendo essa propriedade estão relacionados à quebra de sigilo de dados pessoais, como documentos, extrato bancário, histórico de compras, senhas de cartões de crédito e etc. Evitar que tais dados sejam acessados por pessoas não autorizadas fundamenta um dos requisitos de um sistema seguro.

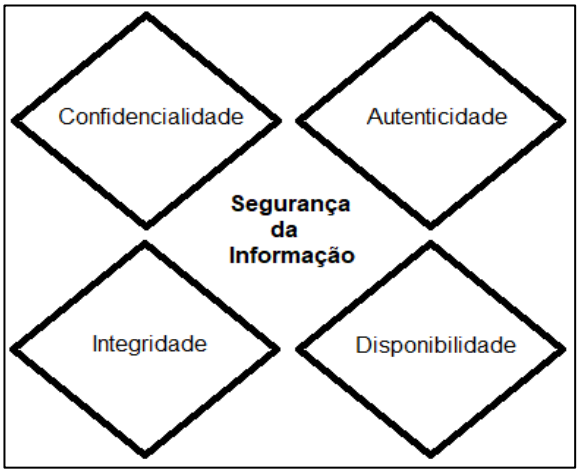
Integridade consiste em assegurar a exatidão e aspecto dos dados ao longo de todo o período de vida da informação. Temos como exemplo um caso em que o saldo de um cliente de um banco é subtraído por ele em uma transação realizada através de um cartão de débito, essa operação deverá ser exata ao valor em que o cliente deseja pagar, caso não seja, a propriedade de integridade de dados estará comprometida, pois haveria uma alteração do dado não autorizada pelo cliente.

Através dessa propriedade, a segurança de dados se corrompe quando um sistema permite processamento de dados de forma ilegítima.

Disponibilidade consiste em manter o funcionamento do sistema sempre que possível. Para garantir a efetividade dessa propriedade, o sistema deve estar à prova de falhas de software ou hardware. Exemplo, a conta de um usuário de uma rede social foi desabilitada temporariamente porque houve tentativas de autenticação com senhas inválidas por uma n quantidade de vezes, para reativar a conta, o usuário deve responder um e-mail que lhe foi enviado. Esse problema impede que o serviço esteja disponível para o cliente, além de ser considerada uma falha de segurança, pois qualquer usuário poderia realizar tentativas de autenticação a fim de desabilitar a conta do cliente em questão com objetivo de impedir o acesso dele ao serviço. A problemática da corrupção dessa propriedade de segurança deve-se principalmente ao bloqueio da tarefa programada no sistema.

Autenticidade consiste na comprovação de que um usuário é legítimo, no qual existe uma prova de que ele realmente é quem diz ser. Por exemplo, um usuário de um sistema online de uma empresa de cartão de crédito cadastrou seus dados no seu aparelho de smartphone. No entanto, posteriormente esse smartphone foi roubado. Caso alguém tente acessar os dados desse cartão a fim de efetuar uma compra, será pedida a assinatura eletrônica, que é o método de comprovação de que o usuário é o autor da conta. Problemas de segurança atrelados à autenticidade baseiam-se na hipótese de um usuário poder acessar e alterar dados de outro ao se disfarçar ilegitimamente, falsificando sua identidade. Na (Figura 01) está a representação das propriedades de segurança de dados.

Figura 01: Ilustração das propriedades da segurança da informação



Fonte: Elaborada pelo autor.

Também, segundo (ALMEIDA e NAPP, 2012), a criptografia moderna atualmente é fundamental para atestar as quatro propriedades da segurança da informação, pois esse recurso permite que:

- Os dados sejam confidenciais através de algoritmos de encriptação com senhas incapazes de serem quebradas por processadores atuais;
- Os dados sejam íntegros por meio de hashes criptográficos, que são algoritmos capazes de verificar bit a bit do dado;
- Os dados sejam autenticados mediante ao uso de assinaturas digitais, que tem como função servir de parâmetro para indicar se o usuário é legítimo ou não.

Assim sendo, percebe-se o quão preservada deve ser a capacidade de criptografia que dispomos em um mundo moderno e de tecnologias avançadas.

> Na actual Sociedade da Informação, em que cada vez mais as pessoas comunicam através da Internet, um meio de comunicação muito exposto, a importância da criptografia é enorme, só através da cifração das comunicações é que podemos garantir a confidencialidade da informação que queremos transmitir (LOPES e QUARESMA, 2008, p.7).

2.1 CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA

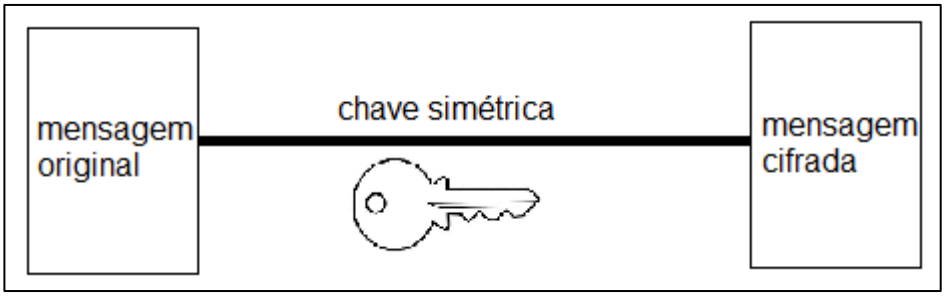
Como passo a entender os próximos tópicos abordados nessa pesquisa, é interessante saber a diferença entre algoritmos de criptografia simétrica e assimétrica. Primeiramente, considera-se o modelo tradicional da criptografia, o modelo simétrico:

> O modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente, esta chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para decodificá-la na outra (OLIVEIRA, 2012, p.12).

Basicamente, o modelo simétrico consiste em algoritmos que funcionam com apenas uma chave para criptografar e decriptografar uma determinada mensagem,

criando assim um processo linear de encriptação, tal como demostrado na (Figura 02).

Figura 02: Ilustração do modelo simétrico de criptografia



Fonte: Elaborada pelo autor.

Exemplificando esse modelo de criptografia: Valentina passa uma mensagem para Enzo de forma em que ela utilize uma chave privada para criptografar sua mensagem e Enzo utilize essa mesma chave para decriptografar a mensagem recebida. Supondo que Osíris conheça o código de criptografia, mas não tenha acesso a chave privada necessária para conhecer o conteúdo da mensagem de Valentina, Osíris não será capaz de decriptografar a mensagem, pois a segurança nesse modelo criptográfico concentra-se na chave privada, e não no algoritmo. Esse tipo de criptografia tem como desvantagem o requerimento de utilização de um canal seguro, porque a chave privada necessita de segurança ao ser utilizada pelo usuário, não devendo ser compartilhada com mais alguém além do remetente e destinatário, pois a segurança do sistema se centra nela (chave privada). Portanto, nem sempre será adequado o uso desse modelo criptográfico, especialmente em casos de dados sigilosos trafegados pela internet.

Entre os principais exemplos de criptossistemas simétricos, pode-se citar o algoritmo AES, Advanced Encryption Standard, tornando-se conhecido por ser rápido, requerer pouca memória, e ser facilmente executável. De acordo com (OLIVEIRA, 2012), o algoritmo AES possui chaves de grandeza 128, 192 e 256 bits, sendo operado em um bloco fixo de 128 bits. Também podemos citar o algoritmo RC2, do qual foi construído pelo cientista Ron Rivest (um dos criadores do algoritmo RSA). Assim como mencionado por (OLIVEIRA, 2012), RC2 é um sistema criptográfico com direcionamento para segurança de e-mails, e possui chaves variáveis de 8 a 1024 bits. Além desses algoritmos citados, existem inúmeros outros exemplos de aplicação do modelo simétrico.

Além do modelo tradicional de criptossistemas simétricos, deve-se compreender também o modelo assimétrico ou de chave pública. Inicialmente, tal modelo, de acordo com (DIFFIE e HELLMAN, M. E., 1976) definiu como um protocolo que requer utilização de uma combinação de uma chave secreta entre dois usuários, porém sem garantia de autenticidade com relação ao remetente e ao destinatário. De acordo com a interpretação da citação de (GOYA, 2006), uma modificação foi feita com finalidade de tornar esse modelo útil para segurança de dados em canais inseguros, essa modificação foi a introdução de certificados digitais:

> Com o objetivo de associar univocamente a chave pública a uma entidade, foi sugerido por (KOHNFELDER, 1978) a criação de uma mensagem assinada por uma autoridade de confiança, contendo a representação da identidade, a correspondente chave pública e um identificador temporal (período de validade). Essa mensagem que associa uma chave pública ao respectivo dono é chamada certificado, ou certificado digital (GOYA, 2006, p.11 e 12).

Percebe-se então, que os certificados digitais representam um meio de garantir que não haja intrusão de terceiros ao transferir mensagens em canais inseguros, sendo realizados a partir de instituições competentes e confiáveis para realizar a mediação da mensagem. A grande vantagem de fazer uso desse modelo criptográfico é a independência de um canal seguro para garantir autenticidade no processo de transferência de texto cifrado, situação da qual, não seria possível com algoritmos de chave simétrica.

O processo de funcionamento de algoritmos de chave pública pode ser explicado da seguinte forma. Enzo deseja receber mensagens de forma segura pela rede aberta de internet, então para isso, ele cria um certificado digital exclusivo para pessoas se comunicarem com ele. Valentina deseja enviar uma mensagem para Enzo. Ela criptografa essa mensagem com uma chave pública disponibilizada pelo certificado de Enzo, para então enviar a ele. Ao receber a mensagem cifrada através de um canal inseguro, Enzo decodifica com sua chave privada, chave essa que não é compartilhada com ninguém. Supomos que no meio do processo de transmissão Osíris deseje interceptar a mensagem, não haverá meios de decodifica-la sem uma chave privada, pois a chave pública compartilhada apenas serve para criptografar

mensagens. Esse processo garante a autenticidade através do certificado digital, pois essa ferramenta atua como documento público de identificação de uma entidade. Assim como também garante a confidencialidade, pois um terceiro agente de confiança está intermediando o envio de mensagens cifradas, que é a entidade emissora do certificado.

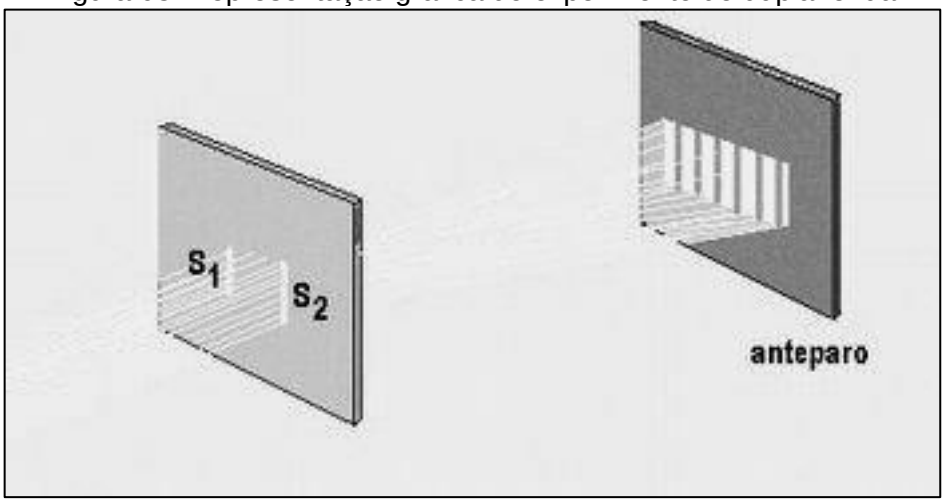
3 COMPUTAÇÃO QUÂNTICA

Computação quântica é um modelo computacional que utiliza a estrutura da mecânica quântica como base de sua lógica de processamento. Assim sendo, sua principal meta é o desenvolver o computador quântico. A importância da computação quântica deve-se à sua capacidade de computar cálculos extensos, ao passo que computadores clássicos não se mostram eficientes o suficiente para realizar tais atividades específicas. Sabendo-se da relevância dos computadores quânticos, é assumido que seu estudo apresentará mudanças significativas no que se refere à segurança de dados. Uma explicação básica sobre os conceitos de funcionamento que regem a computação quântica é descrita abaixo. (SILVA, 2018),

3.1 MECÂNICA QUÂNTICA

Para entender computação quântica, primeiramente deve-se entender mecânica quântica. De acordo com (MATTIELO, SILVA, *et al.*, 2012), mecânica quântica é uma teoria física que tem como finalidade estudar o comportamento de partículas de tamanho atômico ou molecular. Segundo (BITTENCOURT, SUMMA NETTO e VIGNATTI, 2004), essa teoria supõe que as leis da física descobertas por Newton não se aplicam a coisas menores do que átomos de hidrogênio, esses objetos são regidos pela mecânica quântica. É possível testar essa teoria através do experimento da Dupla Fenda, que consiste em pôr uma luz forte em frente a uma divisória com duas fendas. Ao realizar este procedimento, o resultado esperado é o da luz se propagar como se tivesse atravessado toda a divisória, transpassando sua essência de partícula para onda, do qual se une em consequência da interferência causada pelos feixes. Ao final desse experimento, conclui-se que a luz assume duas faces, podendo ser partícula ou onda. A imagem abaixo, na (Figura 03), simula esse experimento.

Figura 03: Representação gráfica do experimento de dupla fenda



Fonte: Elaborada por (BILLY, 2013).

3.1.2 SUPERPOSIÇÃO DE ESTADOS

Segundo o artigo de (MATTIELO, SILVA, *et al.*, 2012), os estados de um objeto subatômico variam de acordo com o princípio da incerteza, do qual cálculos de probabilidades podem ser usados como parâmetro para mensurar os movimentos de tais partículas. O conceito de inexatidão -que de acordo com (CARMICHAEL, DEVORET, *et al.*, 2019) já é ultrapassado- dos estados de uma partícula é a principal razão para a causa de superposição de estados. Dada uma partícula em um espaço limitado entre A e B, a localização dela pode estar em infinitas posições por esse universo que delimita tal distância. Acreditava-se que não era possível saber com 100% de exatidão onde essa partícula pudesse estar, apenas calcular probabilidades. Entretanto, recentemente foi descoberto por (CARMICHAEL, DEVORET, *et al.*, 2019) que é possível prever tal movimento através de um experimento que se baseava na observância da ausência de fótons de irradiação para sinalizar que um salto quântico estaria prestes a ocorrer.

3.1.3 SALTOS QUÂNTICOS E SUA PREVISIBILIDADE

De acordo com o físico-teórico (BOHR, 2011), saltos quânticos são a mudança súbita de um elétron de um estado quântico para outro dentro de um

átomo. Pesquisadores da Universidade de Yale realizaram um experimento que concluiu que, ao contrário do que se pensava sobre a imprevisibilidade de tais saltos, saltos quânticos são determinísticos e previsíveis em curto prazo. Assim como (CARMICHAEL, DEVORET, *et al.*, 2019) propôs, saltos quânticos foram analisados nessa experiência. (CARMICHAEL, DEVORET, *et al.*, 2019) realizou o experimento do qual foi obtido um sinal antecipado de que um salto iria ocorrer através do monitoramento de um átomo artificial que seria irradiado por três geradores de micro-ondas numa cavidade tridimensional de alumínio. Essa irradiação provocou saltos quânticos. No decorrer desse processo, o sinal quântico dos saltos pôde ser amplificado, tornando-o possível de ser monitorado. O átomo artificial causaria um estado auxiliar que emitiria um fóton de detecção, entretanto, haveria momentos em que esse fóton se ausentaria, e esse seria o aviso prévio do salto quântico. A conclusão desse experimento é que é possível prever esses saltos, assim como também reverte-los através de um balanceamento da coerência dos saltos. Saltos quânticos são parcialmente previsíveis depois do ponto de partida aleatório. Esse experimento foi de suma importância para se trabalhar em controle e correção de erros em computadores quânticos a fim de obter precisão de cálculos e aplicação útil.

3.2 QUBIT

Assim como descrito por (BITTENCOURT, SUMMA NETTO e VIGNATTI, 2004), na ciência da computação, usamos o bit para definir a partícula que representa a estrutura básica da computação clássica. Entretanto, a computação quântica faz uso de outra estrutura, chamada qubit. Ao contrário dos bits da computação clássica, os qubits podem ter três valores armazenáveis, são o ‘0’, o ‘1’, ou ambos simultaneamente. Esse terceiro valor é possível devido a propriedade da mecânica quântica chamada superposição. Para compreender essa propriedade, podemos usar a analogia do gato de Schroedinger explicada por (MATTIELO, SILVA, *et al.*, 2012) na seguinte citação:

> Considere um gato preso numa caixa onde há um recipiente com material radioativo que tem 50% de chance de emitir uma partícula radioativa a cada hora, e um contador Geiger. O contador Geiger é um

> aparelho utilizado para detectar radiação. Se o material liberar partículas radioativas, o contador percebe a sua presença e aciona um martelo, que, por sua vez, quebra um frasco de veneno. Evidentemente, ao se passar uma hora só terá ocorrido um dos dois casos possíveis: o átomo emitiu uma partícula radioativa ou não a emitiu (a probabilidade que ocorra um ou outro evento é a mesma). Como resultado da interação, no interior da caixa o gato estará vivo ou morto. Porém, isso não poderemos saber a menos que se abra a caixa para comprovar as hipóteses (MATTIELO, SILVA, et al, 2012, p. 35).

Pode-se observar que Schroedinger fez uma analogia em que a reação de uma partícula atômica decidiria se o frasco de veneno seria quebrado ou não, refletindo assim sobre a vida do gato, que poderia estar vivo ou morto. Adicionalmente, deve-se entender o significado do que é possível chamar de colapso de função de onda, que, segundo (MATTIELO, SILVA, *et al.*, 2012), consiste na possibilidade da superposição ser interferida por algum observador externo, que interagiria com o sistema e romperia a superposição de dois estados. De acordo com esse ponto de vista, um qubit estaria existindo em um estado contínuo entre ‘0’ e ‘1’, para que então a interferência de um observador decidisse o resultado, resultando sempre em um dos valores ‘0’ ou ‘1’. É admissível fazer uma suposição onde temos dois qubits, do qual temos também quatro resultados possíveis, 00, 01, 10 e 11. Dada a superposição teorizada por Schroedinger, existe a possibilidade de um par de qubits ocorrer em superposições desses estados, sendo conveniente a efetuação de cálculos de probabilidades usando números complexos. Por fim, conclui-se que o processamento de informações realizado por computadores quânticos é feito como se quatro estados de dois qubits existisse simultaneamente, e isso desencadearia uma capacidade de manipulação de dados bastante superior ao que disponibiliza a atual computação clássica.

4 CRIPTOSSISTEMAS E COMPUTADORES QUÂNTICOS

Importa ressaltar nesse capítulo que os criptossistemas de modelo de criptografia assimétrica são os que serão estudados e relacionados com a possibilidade de superação pelos computadores quânticos, pois esse modelo de algoritmo compromete maior parte de dados sigilosos trafegados na rede aberta de internet, sendo conveniente a priorização do mesmo para preservar a segurança no compartilhamento de informações hoje parcialmente alcançada.

De acordo com (HALLGREN e VOLLMER, 2009), algumas criptografias populares que se baseiam na dificuldade de fatoração de números gigantescos, no cálculo de logaritmo discreto, de curvas elípticas, entre outros, foram quebradas por computadores quânticos. Entretanto, alguns poucos criptossistemas foram capazes de resistir à capacidade quântica de quebra de segurança, dos quais, está excluso o popular sistema criptográfico RSA.

Tabela de (HALLGREN e VOLLMER, 2009, p. 16), que representa status de imunidade a algoritmos quânticos de sistemas criptográficos conhecidos na atualidade:

Quadro 01: Status de segurança à computação quântica para criptografias

Criptografia	**Quebrada por algoritmo quântico?**
Criptografia de chave pública RSA	Quebrada
Troca de chaves Diffie-Hellman	Quebrada
Criptografia de curvas elípticas	Quebrada
Troca de chaves Buchmann-Williams	Quebrada
Homomorfismo algébrico	Quebrada
Criptografia de chave pública McEliece	Não quebrada
Criptografia de chave pública NTRU	Não quebrada
Criptografia de chave pública sobre reticulados	Não quebrada

Fonte: Elaborada por (HALLGREN e VOLLMER, 2009, p. 16).

4.1 CONCEITOS BASE DO CRIPTOSSISTEMA RSA

Devido ao fato do sistema criptográfico RSA representar boa parte da comunicação segura na internet, tal qual mencionado por (DIAS, 2019), entende-se que há uma necessidade de medir sua eficácia em longo prazo, pondo em pauta seu cálculo base de funcionamento e o modo de processamento capaz de quebrar tal sistema.

RSA (Rivest-Shamir-Adleman) é um sistema criptográfico do qual baseia em diversos conceitos algébricos para programar sua função, tais como algoritmo de Euclides estendido, teorema de Fermat e Euler. De acordo com (SILVA, 2005), o núcleo de segurança deste sistema relaciona-se aos números primos, porque tem como base a fatoração de grandes números.

4.1.2 CIFRAGEM E DECIFRAGEM DO RSA

Para compreender o funcionamento do RSA, é necessário saber o significado dos seguintes conceitos. O primeiro deles é que um número é coprimo de outro quando seu único divisor comum é 1, (e.g.) o número 8 e 9. O segundo conceito é sobre a função $\phi(x)$, que representa a quantidade de números coprimos com x sendo menores do que o x, (e.g.) $\phi(8) = 4$, pois os números 1, 3, 5 e 7 são menores do que 8 e coprimos com ele.

De acordo com (CAMARGO, CEZARINO, *et al.*, 201-), o método RSA pode ser dividido em seguintes passos:

1. Aleatoriamente definir valores de números primos p e q, a partir de $10^{100;}$
2. Descobrir valor de p multiplicado por q, que será n;
3. Calcular $\phi(n)$, que será (p-1) multiplicado por (q-1);
4. Definir um número inteiro que seja maior que 1 e menor do que $\phi(n)$, garantindo que esse número e $\phi(n)$ sejam coprimos. Então podemos chama-lo de e;
5. Calcule d como 2 multiplicado por $\phi(n) + 1$, dividido por e.

É possível perceber que a chave pública é representada por ‘n’ e ‘e’, enquanto a chave privada é dada por ‘d’. Exemplificando o processo de cifrar e decifrar do RSA, podemos imaginar duas pessoas que estão a trocar mensagens, Maria e João. O algoritmo de envio de Maria gera dois números aleatórios p e q, p = 53 e q = 59; calcula $n = p*q$, n = 3127; calcula o ϕ(n), 3016; e escolhe um número ‘e’ que não seja impar e não compartilhe fatores com ϕ(n), sendo 3 o número escolhido para representar ‘e’. Logo o algoritmo de Maria consegue obter a chave privada da mensagem dela, que é calculado como ‘d’, do qual d = 2 * (3016)+1 / 3, resultando em 2011. No processo de envio, o algoritmo de Maria envia a João os valores de ‘n’ e ‘e’. Com esses valores, o algoritmo de João cifra a mensagem de valor 89 usando a fórmula, $c = m^e \ mod \ n$, sendo c = 89^3 mod 3127, resultando em c = 1394. O algoritmo de João retorna a mensagem cifrada ao algoritmo de Maria, que por sua vez decifra a mensagem usando a fórmula $m = c^d \ mod \ n$, resultando em 89.

Dado esse exemplo, pode-se imaginar também que exista um terceiro personagem que tenha intenção de decifrar a chave privada ‘d’ dessa mensagem apenas com as chaves públicas ‘n’, ‘e’ e a mensagem cifrada ‘c’. Isso só é possível se esse terceiro personagem puder descobrir o valor de ϕ(n), o que requer que saiba os fatores primos de ‘n’, que no exemplo, foram ‘p’ e ‘q’ definidos aleatoriamente. Se os fatores primos de ‘n’ fossem grandes o bastante, o algoritmo de força bruta operado pelo terceiro personagem levaria décadas ou séculos para descobrir tais valores. A força do RSA concentra-se nas inúmeras possibilidades de multiplicação de dois números primos resultantes de ‘n’, pois esse imenso número de probabilidades faz com que algoritmos de força bruta com propósito de quebrar essa criptografia tenham que fatorar ‘n’ até encontrar os dois primos que o multiplicam, e consequentemente chegar ao expoente ‘d’ de chave privada.

Assim como mencionado por (CHEN, JORDAN, *et al.*, 2016), a maioria dos protocolos de comunicação dependem de encriptação de chave pública, assinaturas digitais e troca de chaves. Sabendo que RSA trabalha com todas essas encriptações e é um dos sistemas mais utilizados pela rede comercial para transferência de dados, é imprescindível mensurar o nível de ameaça realizável pelo poder de processamento quântico nos próximos anos. É previsto que um computador quântico de larga escala cause impactos significativos em algoritmos criptográficos. Também por autoria de (CHEN, JORDAN, *et al.*, 2016), uma tabela foi criada para

definir a previsão de impacto de acordo com o progresso computacional quântico dos próximos anos. Nessa tabela, o sistema RSA passaria a não ser mais seria seguro, futuramente. A necessidade de adaptação de uma criptografia eficaz aos computadores quânticos é legítima, porque, a pesar de não ser previsto com exatidão quando esses tipos de computadores estarão disponíveis em larga escala comercial, pesquisadores estimam que há a possibilidade de que nos próximos 11 anos seja viável a construção de um supercomputador quântico capaz de quebrar o algoritmo RSA 2000-bits, por um orçamento de 1 bilhão de dólares americanos.

4.2 ALGORITMO DE SHOR

Assim como mencionado por (BITTENCOURT, SUMMA NETTO e VIGNATTI, 2004) o algoritmo de Shor foi descrito em 1994 como sendo capaz de fatorar números primos em tempo polinomial. Esse algoritmo foi divulgado com muita repercussão entre a comunidade científica, e foi considerado fundamental para o crescente interesse em computação quântica, pois alcançou um feito marcante para a ciência das criptografias. Apesar de toda a eficiência do tal algoritmo capaz de descobrir fatores primos de um número composto, ainda é possível afirmar que criptossistemas que dependem desse tipo de cálculo para manterem-se seguros, vão continuar a serem seguros nos próximos anos, pois de acordo com (ALEGRETTI, 2004), o algoritmo de Shor, considerado mais eficiente para esse tipo de problema, fatora números inteiros na grandeza de até 10^{200}, havendo a necessidade de se trabalhar com muitos qubits para alcançar os níveis de grandeza da criptografia RSA 2000-bits.

5 CRIPTOGRAFIA DE RESISTÊNCIA À PROCESSAMENTO QUÂNTICO

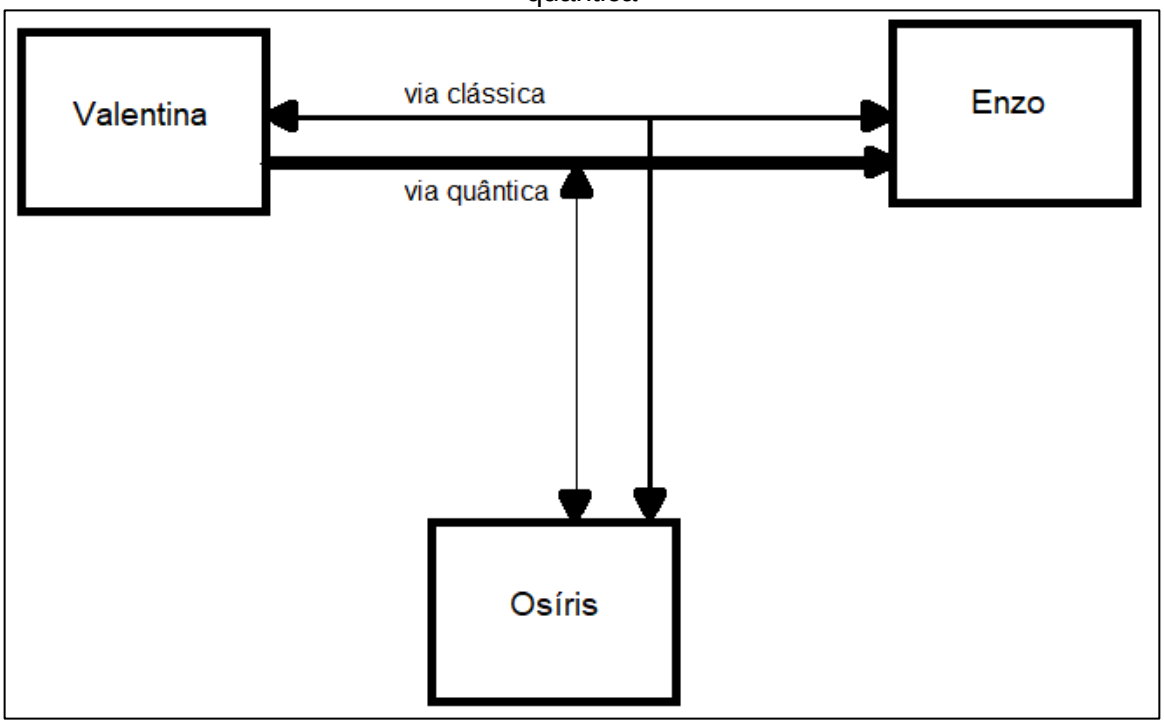
A importância de estudar criptografias resistentes ao processamento de computadores quânticos se dá pela razão de que muitas informações com alto nível de sigilo precisam ser mantidas de forma confidencial nos próximos anos. Com a evolução tecnológica, espera-se que em alguns anos seja possível construir computadores quânticos de alta capacidade. Assim como demonstrado na tabela de (HALLGREN e VOLLMER, 2009, p. 16), existem poucos criptossistemas capazes de resistir ao processamento quântico. Neste capítulo, será realizado um estudo da possibilidade teórica de aplicação de conceitos de mecânica quântica à criação de um novo sistema criptográfico. Assim como também haverá uma análise de um dos criptossistemas disposto a sustentar-se diante da capacidade de computação quântica.

5.1 COMUNICAÇÃO CRIPTOGRÁFICA BASEADA EM CONCEITOS DE MECÂNICA QUÂNTICA

O método quântico de se realizar transferência de informações por meio de chave privada tem sido amplamente teorizado por pesquisadores. Tal como constatado por (BITTENCOURT, SUMMA NETTO e VIGNATTI, 2004), os princípios da mecânica quântica podem ser utilizados para construção de um criptossistema capaz de detectar invasores de mensagens, impossibilitando a espionagem de comunicação.

Para exemplificar, é possível imaginar que existe uma via de comunicação clássica bidirecional e uma via quântica unidirecional entre Valentina e Enzo, do qual ambas as vias estão sendo interceptadas por Osíris, que tem como propósito descobrir a chave que decriptografa a mensagem passada entre Valentina e Enzo. Abaixo, na (Figura 04), se encontra a representação do exemplo:

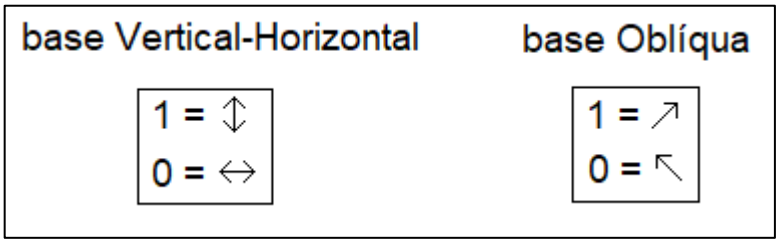
Figura 04: Ilustração do exemplo de comunicação baseada em conceitos de mecânica quântica



Fonte: Elaborada pelo autor.

A comunicação pela via quântica é realizada com uso de estados polarizados do fóton. O receptor da mensagem, nesse caso, Enzo, se encarregará de medir o estado quântico dos fótons. Essa medição é feita antecipadamente pelo intruso, nesse caso, Osíris, antes mesmo da mensagem chegar a Enzo. Entretanto, para garantir discrição no processo de espionagem, Osíris reenvia os fótons a Enzo. Dentro do processo de geração de chave secreta, está a possibilidade de escolha de Valentina sobre qual alfabeto quântico utilizar para gerar cada algarismo binário, que neste exemplo, pode ser de base Vertical-Horizontal ou de base Oblíqua, assim como se encontra na (Figura 05).

Figura 05: Mapa de indicativo dos alfabetos quânticos exemplificados



Fonte: Elaborada pelo autor.

Uma explicação detalhada sobre o passo a passo de como a comunicação entre Valentina e Enzo acontece será descrita a seguir. Transferência de informações pela via quântica unilateral:

1. A chave secreta que será compartilhada com Enzo, será estabelecida por Valentina através de uma sequência aleatória de 0’s e 1’s;
2. Valentina escolherá aleatoriamente qual alfabeto usará em cada bit dessa sequência, para então haver a transferência do fóton polarizado;
3. Para cada fóton recebido de Valentina, Enzo deve decidir aleatoriamente qual alfabeto Valentina usou, e assim realizar a medição do fóton. O resultado do bit medido por Enzo só será equivalente ao bit enviado por Valentina em 50% das vezes, pois existem apenas dois alfabetos possíveis de serem usados por Valentina. Uma sequência binária é estabelecida após o término da medição de todos os fótons recebidos.

Transferência de informações pela via clássica bilateral (canal público):

1. Ocorre o envio de Enzo para Valentina dos alfabetos usados para realizar a medição de fótons em cada bit recebido;
2. Valentina envia os acertos de Enzo –medições feitas com o alfabeto certo- como retorno;
3. Os bits que foram medidos com o alfabeto errado são deletados por Valentina e Enzo. A chave inicial é formada pelos bits restantes. A equivalência da chave inicial de Valentina e Enzo vai depender da não espionagem de Osíris, porque se Osíris espionou, a chave inicial de Valentina não mais será equivalente a de Enzo.

Uma comparação de chaves iniciais é realizada por Valentina e Enzo como uma forma de estimar os erros, para então ser possível excluir os bits que foram exibidos pelo canal aberto, assim surgindo a chave definitiva. A partir dessa explicação, pode-se observar que caso algum erro aconteça entre a transferência de informações no canal público, sabe-se que Osíris estava escutando a mensagem, e

caso não ocorra, a conclusão é de que Osíris não estava entre o processo de comunicação. O ato de Osíris interceptar e medir cada bit quântico enviado por Valentina para então enviar a Enzo com o estado já medido por ele (Osíris), causa uma taxa de erro na chave inicial de Enzo. Por essa razão que a chave de Valentina e Enzo não equivaleria.

5.2 CRIPTOGRAFIA DE CHAVE PÚBLICA MC ELIECE

Depois de constatada a quebra do algoritmo RSA por computadores quânticos, é natural que se pense em alguma solução substituta desse método que somente apresenta total resistência a algoritmos clássicos de computação. É importante ressaltar que, como mencionado na pesquisa de (CHEN, JORDAN, *et al.*, 2016), a construção de computadores quânticos capazes de quebrar os algoritmos de criptografia amplamente usados, atualmente, (e.g.) RSA 2000-bits, levará anos para tornar-se viável, e que a possibilidade de substituição de algoritmos criptográficos vulneráveis para criptossistemas imunes a computadores quânticos como método de prevenção é cogitada apenas para informações relevantes em larga escala de tempo, tempo do qual se estima a viabilidade de utilização de computadores quânticos de múltiplos qubits. Entre diversos candidatos a essa possível substituição, apresenta-se o algoritmo de chave pública McEliece, que, de acordo com a tabela de (HALLGREN e VOLLMER, 2009, p. 16), mencionada no capítulo 4 dessa pesquisa, permanece teoricamente inquebrável por algoritmos de computação quântica.

Assim como definido por (MARTINS, 2014), a criptografia de chave pública McEliece conceitua-se em um tipo de encriptação baseada em códigos, do qual, o emissor de uma determinada mensagem usa uma chave pública para criptografa-la e envia-la, acrescentando um erro aleatório, de forma que somente a chave privada do receptor seja capaz de decriptar a mensagem e remover o erro nela inserido. As evidências de que tal método criptográfico seja eficiente no que diz respeito à segurança da informação imune a algoritmos quânticos torna seu uso bastante conveniente para sistemas que armazenam informações extremamente sigilosas e sensíveis, (e.g.) informações detalhadas sobre o exército de determinado país, ou até mesmo informações privilegiadas sobre determinada corporação de cunho

estratégico comercial. Foi constatado por (MISOCZKI, TILLICH, *et al.*, 2013, p. 1) *"acredita-se que a criptografia baseada em códigos é resistente à computação quântica e, portanto, ela é considerada como uma alternativa para aplicações futuras".*

5.2.1 PROBLEMAS DO MC ELIECE E SUPOSTAS SOLUÇÕES

Sendo o McEliece tão conveniente para utilização, ainda assim existem impasses a serem superados. De acordo com (OVERBECK e SENRIER, 2009, p. 95), o tamanho das chaves públicas do criptossistema McEliece pode alcançar a grandeza de 100 kilobytes até alguns megabytes. Esse problema dificulta bastante a aplicação desse sistema nos serviços online, pois é preferível manter respostas de alta velocidade no modelo cliente-servidor, fazendo uso da quantidade mínima de dados possíveis. Outra dificuldade a ser citada diz respeito a considerável expansão de dados no processo de transformação para a codificação. (BERNSTEIN, 2009, p. 3) constata que no patamar de segurança 128 bits, o RSA atua com chaves de milhares de bits, ao passo que as chaves do McEliece alcançam o milhão de bits para este mesmo nível de segurança, que de acordo com ele, esse pode ser o motivo de estarmos utilizando o sistema criptográfico RSA ao invés do McEliece.

5.2.2 TEORIA DE SUBSTITUIÇÃO DE CÓDIGOS GOPPA POR MDPC

Sabe-se que uma parte do processo de funcionamento da criptografia McEliece se baseia em causar um erro introduzido na mensagem para poder ser decriptografado através de uma correção calculada pela chave privada. Essa chave privada é representada por códigos Goppa, que são códigos matematicamente teorizados. Segundo (CASTELLANOS, 200-), a teoria dos códigos corretores de erro foi apresentada pelo cientista Shannon (1948).

> Os códigos de Goppa fazem parte dos códigos chamados de corretores de erros, que participam da vida moderna de inúmeras formas como, por exemplo, nas comunicações via satélite, na telefonia celular e na comunicação entre computadores, etc. [...] Hoje em dia, os códigos corretores de erros são utilizados sempre que se

> deseja transmitir ou armazenar dados, garantindo sua confiabilidade (CASTELLANOS, 200-, p. 1).

O grande tamanho de chaves dos sistemas criptográficos baseados em códigos representa um considerável problema na utilização do mesmo, pois compromete sua eficiência. Pertinentemente ao assunto, de acordo com o trabalho de (GABORIT, 2005) a redução do tamanho dessas chaves pode ser feita através do uso de códigos com um grande grupo de automorfismo, sendo-os quase-cíclicos. Entretanto, assim como exposto por (FAUGÈRE, OTMANI, *et al.*, 2010), um sistema algébrico de equações pode ser desenvolvido com base na estrutura algébrica de tais códigos, (e.g.) os teorizados por (GABORIT, 2005), sendo esse sistema capaz de quebrar a segurança de criptografias baseadas em código. Isso indica que a completa exclusão de uma estrutura algébrica em um código usado como parâmetro de chave privada representa a superação dessa vulnerabilidade.

Tal como citado por (MARTINS, 2014), há a possibilidade de introduzir códigos MDPC (códigos de média densidade de verificação de paridade) com objetivo de evitar estrutura algébrica dos códigos Goppa, pois além de não possuírem estrutura algébrica, esses códigos fazem uso de matrizes de verificação de paridade esparsa no momento de decriptação. Assim como teorizado por (MISOCZKI, TILLICH, *et al.*, 2013, p. 2), a razão do uso desses códigos como corretores de erro ser conveniente é que o número de erros que podem ser corrigidos dentro de uma mensagem é numeroso o suficiente para impedir a decriptação através de algoritmos padrão de correção de erros.

Segundo (MARTINS, 2014), o processo de execução do McEliece com códigos MDPC podem corrigir n erros, e estão descritos nas seguintes etapas:

1. Geração de chaves: um vetor binário aleatório h é gerado, que é correspondente a primeira linha da matriz H, e as outras linhas são preenchidas pelos deslocamentos quase-cíclicos de h. A forma reduzida escalonada de H é o que representa a matriz G. A matriz G é a chave pública, e H é a privada;
2. Encriptação: A criação de um vetor binário aleatório pesando menos ou o mesmo que n deve ser feita. A cifra composta na mensagem m é resultado de $y \leftarrow mG + e$;

3. Decriptação: O cálculo para retornar o valor de *y* para *m* é baseado em $mG \leftarrow \Psi_H\ (mG+e)$, do qual Ψ_H atua como decodificador MDPC da matriz *H*. As primeira posições de *m*G são a mensagem recuperada.

Tempo de execução é um elemento chave para algoritmos baseados em código, pois sua necessidade se deve aos padrões já estabelecidos de eficiência, algo que ajuda a corroborar a dissertação de (MARTINS, 2014) sobre uma suposta substituição do criptossistemas RSA pelo McEliece com MDPC. Sabendo disso, o processo de decriptação deve ser encurtado o máximo possível, obtendo eficiência balanceada para somar com a segurança almejada. De acordo com (MISOCZKI, TILLICH, *et al.*, 2013), a algoritmos de decodificação de inversão de bits apresentam características de possuírem baixa complexidade, serem velozes, e iterativos. Assim como descrito na pesquisa de (MARTINS, 2014), a técnica de inversão de bits propõe que em cada iteração aconteça o calculo do conjunto de erros na mensagem que será decodificada, para então haver o calculo de equações de verificação de paridade não satisfeitas atreladas a cada parte da mensagem, de forma que seja invertido cada bit atrelado a mais que uma determinada quantidade *b* de equações não satisfeitas. Tal sequência acontece até que o conjunto de erros na mensagem seja esvaziado, ou até chegar a uma falha no processo de decriptação alcançando o limite de iterações *b.* Existem diversos decodificadores além da inversão de bits, porém, sua particularidade se deve à maneira em que é calculado o limite *b*, seja ela feita através de um cálculo antecipado de limites com base em parâmetros do código, ou feita levando em consideração a maior quantidade de equações não satisfeitas.

Considere uma execução do McEliece com código MDPC, capacidade de correção de *n* erros, e seja *C* derivado da chave pública. Nessa execução, a partir das constatações de (MISOCZKI, TILLICH, *et al.*, 2013, p. 13), os ataques mais eficientes seriam baseados em distinção de chave, recuperação de chave, e decodificação. A intenção dos araques baseados em recuperação de chave é reaver um elemento secreto do processo, o decodificador. A finalidade de ataques de distinção de chave concentra-se em apenas distinguir a chave pública de uma matriz randômica. Em ataques de decodificação, o intuito é decodificar uma mensagem dada como uma palavra código, já prevendo rastros deixados (ruídos). Encontrar a

palavra código ou computar uma decodificação de erros da mensagem é exatamente o desafio que cerca um suposto invasor *man-in-the-middle*, tais desafios que envolvem recuperação de equações de verificação de paridade, dificuldade de decodificação de erros, e peso da palavra código.

5.2.3 COMPARATIVO DO TEMPO DE DECRIPTAÇÃO DO CRIPTOSSISTEMA RSA COM MCELIECE MDPC

O tempo de decriptação do sistema criptográfico de chave pública RSA é eficaz o suficiente para intermediar comunicações de mensagens sigilosas através de canais inseguros. Entendendo isso, parte-se para a perspectiva de que a criptografia McEliece com códigos MDCP como solucionador de erros necessite de se posicionar para essa direção também. Mensurando o algoritmo de decifração RSA provido de um computador clássico de processador AMD Opteron 248, com frequência de clock de 2.2Ghz, rodando o sistema Linux Debian, (KHURANA, KOLEVA e BASNEY, 2007) obtiveram os seguintes resultados. Para o tamanho de chave de 512bits, o tempo médio de decifração ocorria em média 0,5 milissegundos. Para 1024bits, esse tempo incrementava para 2,4 milissegundos. Enquanto que para chave de 2048bits, o tempo médio era de 13,1 milissegundos. Esses tempos de decifragem também foram medidos por (BONEH e SHACHAM, 2002), do qual através de uma máquina de processador Pentium III, com 750Mhz de frequência de clock, 256 megabytes de memória RAM, rodando o sistema Linux Debian, concluiu que para chaves de 768bits, o tempo médio de decriptação era de 4,67 milissegundos. Assim como também, chaves de 1024bits apresentavam tempo de 8,38 milissegundos, e que chaves de 2048bits exibiam reprodução em tempo de 52,96 milissegundos.

Em sua dissertação, (MARTINS, 2014) reproduziu o algoritmo do criptossistema McEliece MDPC baseando-se na proposta de (MISOCZKI, TILLICH, *et al.*, 2013)**,** da qual já havia publicado testes semelhantes. Ele usou uma máquina com processador Intel Core i7-4770, com frequência de clock de 3,40GHz rodando o sistema Linux Ubuntu versão 12. Uma mesma mensagem foi utilizada para mil execuções diferentes, sendo adicionado um erro aleatório a ela (mensagem) em cada ciclo de execução. Uma versão otimizada foi utilizada para execução do teste,

a otimização consistiu em selecionar operações XOR apenas em valores não nulos das linhas da matriz. Além disso, houve também o uso de instruções vetoriais inerentes durante a multiplicação da mensagem cifrada pela matriz de paridade de forma simultânea à execução de XORs. Como o processamento de multiplicação da mensagem cifrada pela matriz de paridade é bastante custoso, foi realizado o uso de um algoritmo em que buscava substituir essa etapa por atualizações do conjunto de erros da mensagem calculados no passo introdutório da decriptação. Esse algoritmo também buscou usar valores pré-calculados baseados em parâmetros do código para diminuir a quantidade de iterações do algoritmo. Com emprego de instruções vetoriais de 256bits e 512bits, (MARTINS, 2014) teve como resultado de seus testes tempos de decriptação de, respectivamente, 0,94 milissegundos e 1,17 milissegundos, tornando assim o tempo de execução do criptossistema McEliece MDPC próximo ao do RSA.

6 CONCLUSÃO

Essa pesquisa trabalhou com argumentos teóricos sobre a aplicação do sistema criptográfico McEliece com base em códigos MDPC, e sugeriu uma possível atualização na segurança de dados que visa substituir parcialmente o algoritmo de chave assimétrica mais popular atualmente, o RSA. Foi explanada a importância da segurança de dados como garantia da ampla comunicação por canais inseguros de rede de internet aberta, dando vasão à importância de se estudar novos meios de criptografia. Propriedades como confidencialidade, autenticidade, integridade e disponibilidade foram consideradas essenciais por (BRASIL, 2013) para manter uma base de segurança de dados.

Houve também uma explicação sobre computação quântica e suas propriedades de funcionamento, tais como a mecânica quântica. O experimento de dupla fenda foi citado como forma de exemplificar o funcionamento da mecânica quântica, em que funciona com a superposição de estados, que de acordo com (CARMICHAEL, DEVORET, *et al.*, 2019) são parcialmente previsíveis através de saltos quânticos. O elemento mais importante que conceitua a computação quântica, o bit quântico (qubit), foi discutido na pesquisa. O qubit sendo o grande diferencial entre computadores clássicos e quânticos é também responsável pela capacidade exponencial de processamento em computadores quânticos, pois assim como explicou (MATTIELO, SILVA, *et al.*, 2012), além dos bits clássicos já conhecidos desde Turing, ‘0’ e ‘1’, computadores quânticos também possuem o bit que assume ambos os valores simultaneamente, isso acontece por consequência da superposição de estados referente à mecânica quântica.

Em decorrência da capacidade de computadores quânticos e seu provável crescimento de popularidade com passar dos anos, se fez necessário reavaliar a eficácia do criptossistema RSA, do qual intermedia grande parte das comunicações pela rede de internet, e que, de acordo com (SILVA, 2005) tem como base de segurança a fatoração de gigantescos números primos. Na tabela de (HALLGREN e VOLLMER, 2009, p. 16), observou-se que foi constada a quebra do sistema criptográfico RSA por algoritmos quânticos. Foi mencionado também o algoritmo de Shor, referenciado na pesquisa de (BITTENCOURT, SUMMA NETTO e VIGNATTI, 2004), esse algoritmo foi descrito em 1994 como sendo capazes de fatorar números

primos em tempo polinomial, comprometendo assim a base de segurança do RSA. No trabalho de (CHEN, JORDAN, *et al.*, 2016) notou-se que atualmente ainda não existem computadores quânticos capazes de quebrar o sistema RSA 2000-bits, mas que é algo esperado para as próximas décadas.

Essa pesquisa destacou a importância de se estudar criptografias resistentes à processamento quântico, explanando a ideia de criptografia com base em conceitos de mecânica quântica, da qual foi respaldada por (BITTENCOURT, SUMMA NETTO e VIGNATTI, 2004) no exemplo em que alfabetos quânticos de base vertical-horizontal e de base oblíqua foram citados. A hipótese de substituição do algoritmo RSA pelo McEliece foi trabalhada no quinto capítulo desse trabalho. Foi explicado o funcionamento do criptossistema de chave pública McEliece envolve a inserção de um erro na mensagem pela chave pública, para que esse erro seja corrigido pela chave privada, do qual teria o código de Goppa para realizar tais correções. Assim como analisado por (MARTINS, 2014), códigos MDPC (códigos de média densidade de verificação de paridade) poderiam ser usados no lugar dos códigos de Goppa. Em sua dissertação, (MARTINS, 2014) realizou testes de funcionamento do criptossistema McEliece baseado em códigos MDPC, e comparou com os resultados da eficiência do RSA publicados por (KHURANA, KOLEVA e BASNEY, 2007) e (BONEH e SHACHAM, 2002). O resultado dessa comparação fortaleceu a hipótese de substituição do sistema criptográfico RSA pelo McEliece, dada a necessidade de adaptar as propriedades da segurança de dados ao provável salto na acessibilidade de computadores quânticos esperado para as próximas décadas.

Os resultados dessa pesquisa puramente teórica foram suficientes para concluir que existe a necessidade de se adaptar à nova forma de computação propensa a se tornar cada vez mais poderosa no futuro, e que uma das alternativas mais acessíveis no momento de realização desse trabalho centrou-se na substituição do criptossistema de chave assimétrica RSA pelo McEliece com códigos MDPC, que provou estar muito próximo da eficiência do RSA, com o diferencial de ser teoricamente imune a computadores quânticos.

REFERÊNCIAS

ALEGRETTI, F. J. P. Computação Quântica. **Faculdade de Computação - UFMS**, 2004. Disponivel em: <http://prof.facom.ufms.br/~marco/cquantica/cquantica.pdf>. Acesso em: 14 Out. 2019.

ALMEIDA, P. J.; NAPP, D. **Criptografia e Segurança**. 1ª. ed. Aveiro: Publindústria, 2012.

BARRETO, P. S. L. M. et al. Introdução à criptografia pós-quântica. **Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**, Manaus, p. 46-100, Nov 2013.

BERNSTEIN, D. J. **Post-Quantum Cryptography**. Chicago: Springe, Berlin, Heidelberg, 2009.

BILLY, E. O desejo e a vida, jamais se esconde…. **Vibe Leve**, 2013. Disponivel em: <http://www.vibreleve.com/blog/2013/05/17/o-desejo-e-a-vida-jamais-se-esconde/>. Acesso em: 14 Nov. 2019.

BITTENCOURT, L. F.; SUMMA NETTO, F.; VIGNATTI, A. L. **Uma Introdução à Computação Quântica**. Universidade Federal do Paraná. Curitiba, p. 90. 2004.

BLUME, J. Hypescience. **www.hypescience.com**, 2019. Disponivel em: <https://hypescience.com/fisicos-conseguem-prever-os-saltos-do-gato-de-schrodinger-e-finalmente-salva-lo/>. Acesso em: 19 Out 2019.

BOHR, N. **Niels Bohr on the Application of the Quantum Theory to Atomic Structure, Part 1, The Fundamental Postulates**. 978-1-107-68158-3. ed. Cambridge: Cambridge University Press, 2011.

BONEH, D.; SHACHAM, H. Fast variants of RSA. **Cryptobytes**, San José, v. 5, n. 1, p. 1-9, 2002.

BRASIL. Política e Segurança da Informação. **Instituto Federal Farroupilha**, 27 Mar. 2013. Disponivel em: <http://www2.fw.iffarroupilha.edu.br/cti/PSI.pdf>. Acesso em: 16 Abr. 2019.

CAMARGO, L. P. F. D. et al. Criptografia: O Método RSA. **Instituto de Matemática, Estatística e Computação Científica**, 201-. Disponivel em:

<https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/Fernando_TN17M2.pdf>. Acesso em: 14 Out. 2019.

CARMICHAEL, H. J. et al. To catch and reverse a quantum jump mid-flight. **Nature 570**, 3 Jun. 2019. 200-204.

CASTELLANOS, A. S. Códigos de Goppa. **Instituto de Matemática, Estatística e Computação Científica**, 200-. Disponivel em: <https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/goppa.pdf>. Acesso em: 14 Out. 2019.

CHEN, L. et al. **Report on Post-Quantum Cryptography**. National Institute of Standards and Technology. Gaithersburg, p. 15. 2016.

DIAS, L. D. S. **Ensino de funções e criptografia RSA.** Universidade Federal de Santa Maria. Santa Maria, p. 29. 2019.

DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE Transactions on Information Theory**, Nova York, 6 Novembro 1976. 644-654.

ESPÍRITO SANTO, A. F. S. D. **SEGURANÇA DA INFORMAÇÃO**. Instituto Cuiabano de Educação. Cuiabá, p. 11. 2012.

FALEIROS, A. C.; SILVEIRA, A. S. Criptografia de chave pública - o papel da aritmética em precisão múltipla. **Instituto Tecnológico de Aeronáutica**, 2005. Disponivel em: <http://www.bibl.ita.br/xiencita/Artigos/Fund05.pdf>. Acesso em: 16 Abr. 2019.

FAUGÈRE, J.-C. et al. Algebraic cryptanalysis of McEliece variants with compact keys. **Annual International Conference on the Theory and Applications of Cryptographic Techniques.**, Springer, Berlin, Heidelberg, 2010. 279-298.

GABORIT, P. Shorter keys for code based cryptography. **Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)**, Limoges, 2005. 81-91.

GOYA, D. H. **Proposta de esquemas de criptografia e de assinatura sob modelo de criptografia de chave pública sem certificado**. Universidade de São Paulo. São Paulo, p. 132. 2006.

GRECA, I. M.; HERSCOVITZ, V. E.; MOREIRA, M. A. Uma Proposta para o Ensino de Mecânica Quântica. **Uma Proposta para o Ensino de Mecânica Quântica**, Porto Alegre, 22 Out 2001. 444-457.

GUGIK, G. Tecmundo. **www.tecmundo.com.br**, 06 Mar 2009. Disponivel em: <https://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 19 Out 2019.

HALLGREN, S.; VOLLMER, U. Quantum Computing. In: BERNSTEIN, D. J.; BUCHMANN, J.; DAHMEN, E. **Post-Quantum Cyptography**. 978-3-540-88702-7. ed. Berlim: Springer, 2009. Cap. 2, p. 15-34.

KHURANA, H.; KOLEVA, R.; BASNEY, J. Performance of cryptographic protocols for high-performance, high-bandwidth and high-latency grid systems. **Third IEEE International Conference on e-Science and Grid Computing (e-Science 2007)**, Bangalore, Dez. 2007. 431-439.

KOHNFELDER, L. A. **A Method for Certification**. University of Cambridge. Cambridge. 1978.

LOPES, E.; QUARESMA, P. Criptografia. **Gazeta de Matemática**, Coimbra, p. 7-11, mar. 2008.

MARTINS, H. D. O. **QC-MDPC MCELIECE: UMA IMPLEMENTAÇÃO OTIMIZADA DE UMA NOVA VARIANTE MCELIECE**. Universidade de Brasília. Brasília, p. 52. 2014.

MATTIELO, F. et al. DECIFRANDO A COMPUTAÇÃO QUÂNTICA. **Caderno de Física da UEFS**, Feira de Santana, 2012. 31-44.

MISOCZKI, R. et al. McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. **IEEE INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY**, Istambul, 2013. 2069-2073.

OLIVEIRA E SILVA, F. G. G. P. D. **O impacto da computação quântica na Criptografia Moderna**. Universidade do Minho. Braga, p. 126. 2013.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital**, v. 31, p. 11-15, 2012.

OVERBECK, R.; SENRIER, N. Code-Based Cryptography. In: BERNSTEIN, D. J.; BUCHMANN, J.; DAHMEN, E. **Post-Quantum Cryptography**. Berlim: Springer, 2009. Cap. 4, p. 94-145.

SHANNON, C. E. A mathematical theory of communication. **Bell system technical journal**, Nova York, 1948. 379-423.

SILVA, E. A. M. **UM ESTUDO DO SISTEMA CRIPTOGRÁFICO RSA**. Universidade Católica de Brasília. Brasília, p. 19. 2005.

SILVA, W. J. N. D. **Uma introdução à Computação Quântica**. Universidade de São Paulo. São Paulo, p. 61. 2018.

SILVEIRA, A. S. D. CRIPTOGRAFIA DE CHAVE PÚBLICA. **O PAPEL DA ARITMÉTICA EM PRECISÃO MÚLTIPLA**, São José dos Campos, 05 Out 2005. 6.