MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM SISTEMAS E COMPUTAÇÃO

RAFAEL DA SILVA OLIVEIRA

AVALIAÇÃO DE DESEMPENHO DE ALGORITMOS DE CRIPTOGRAFIA PÓS-QUÂNTICA EM SISTEMAS DE VOTAÇÃO PELA INTERNET

RIO DE JANEIRO
2025

RAFAEL DA SILVA OLIVEIRA

AVALIAÇÃO DE DESEMPENHO DE ALGORITMOS DE CRIPTOGRAFIA PÓS-QUÂNTICA EM SISTEMAS DE VOTAÇÃO PELA INTERNET

Dissertação apresentada ao Programa de Pós-graduação em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Mestre em Ciências em Sistemas e Computação.

Orientador(es): José Antonio Moreira Xexéo, D.Sc
Renato Hidaka Torres Torres, D.Sc

Rio de Janeiro

2025

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80 – Praia Vermelha
Rio de Janeiro – RJ CEP: 22290-270

Oliveira, Rafael da Silva.
Avaliação de desempenho de algoritmos de criptografia pós-quântica em sistemas de votação pela internet / Rafael da Silva Oliveira. – Rio de Janeiro, 2025.
70 f.

Orientador(es): José Antonio Moreira Xexéo e Renato Hidaka Torres Torres.

Dissertação (mestrado) – Instituto Militar de Engenharia, Sistemas e Computação, 2025.

1. Votação eletrônica. 2. Criptografia pós-quântica. 3. Segurança da informação. 4. Votação online. i. Xexéo, José Antonio Moreira (orient.) ii. Torres, Renato Hidaka Torres (orient.) iii. Título

RAFAEL DA SILVA OLIVEIRA

Avaliação de desempenho de algoritmos de criptografia pós-quântica em sistemas de votação pela internet

Dissertação apresentada ao Programa de Pós-graduação em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Mestre em Ciências em Sistemas e Computação.

Orientador(es): José Antonio Moreira Xexéo e Renato Hidaka Torres Torres.

Aprovado em Rio de Janeiro, 27 de fevereiro 2025, pela seguinte banca examinadora:

Prof. **José Antônio Moreira Xexéo** - D.Sc. do do IME - Presidente

Prof. **Anderson Fernandes Pereira dos Santos** - D.Sc. do do IME

Prof. **Renato Hidaka Torres** - D.Sc. da UFPA

Prof. **Roberto Samarone dos Santos Araújo** - D.Sc. da UFPA

Prof. **Jorge de Abreu Soares** - D.Sc. do CEFET-RJ

Rio de Janeiro
2025

Este trabalho é dedicado à Deus, minha família e todos que acreditaram em mim.

AGRADECIMENTOS

Agradeço aos meus orientadores, José Antônio Moreira Xexéo e Renato Hidaka Torres, pelos ensinamentos, paciência, dedicação e contribuição para a concretização deste projeto.

À minha família, em especial à minha esposa Ivyanne, sou imensamente grato por sempre estar ao meu lado, especialmente nos momentos de maior dificuldade, oferecendo palavras de apoio e motivação.

Aos professores do Programa de Pós-Graduação em Sistemas e Computação, agradeço pelos conhecimentos compartilhados, pelas experiências vivenciadas e pela dedicação à arte de ensinar.

Aos meus colegas de curso, expresso minha gratidão pelo apoio ao longo dessa jornada desafiadora, pela troca de conhecimentos e pelas discussões técnicas enriquecedoras.

Aos militares da Marinha do Brasil que, de alguma forma, contribuíram para a realização deste trabalho, registro aqui meus mais sinceros agradecimentos.

RESUMO

A evolução das tecnologias da informação e comunicação tem impactado significativamente os processos eleitorais, impulsionando a adoção de sistemas eletrônicos de votação. A proteção dos dados nesse contexto depende amplamente do uso da criptografia. No entanto, a segurança desses sistemas é uma preocupação crescente, especialmente diante do avanço da computação quântica, que ameaça os algoritmos criptográficos clássicos. Nesse cenário, este trabalho propõe utilizar algoritmos resilientes a ataques quânticos para garantir os requisitos de autenticidade, confidencialidade, integridade e anonimato durante as fases de votação e apuração de um sistema de votação online. Para verificar a viabilidade dessa proposta, são analisadas diferentes abordagens criptográficas, incluindo esquemas de criptografia homomórfica, funções de hash e assinaturas digitais. Além disso, é realizada uma simulação computacional para avaliar o desempenho dos algoritmos utilizados e sua aplicabilidade em eleições de grande escala. Os resultados obtidos demonstram que a solução proposta pode atender as demandas de segurança pós-quântica, preservando a confiabilidade e a transparência do processo eleitoral. Dessa forma, este estudo contribui para o avanço de novas abordagens criptográficas que garantam a segurança do voto eletrônico diante da iminente evolução dos computadores quânticos.

Palavras-chave: Votação eletrônica. Criptografia pós-quântica. Segurança da informação. Votação online.

ABSTRACT

The evolution of information and communication technologies has significantly impacted electoral processes, driving the adoption of electronic voting systems. The protection of data in this context largely depends on the use of cryptography. However, the security of these systems is a growing concern, especially in the face of advancements in quantum computing, which threatens classical cryptographic algorithms. In this scenario, this work proposes the use of quantum-resilient algorithms to ensure the requirements of authenticity, confidentiality, integrity, and anonymity during the voting and tallying phases of an online voting system. To assess the feasibility of this proposal, different cryptographic approaches are analyzed, including homomorphic encryption schemes, hash functions, and digital signatures. Furthermore, a computational simulation is performed to evaluate the performance of the algorithms used and their applicability in large-scale elections. The results obtained show that the proposed solution can meet the demands of post-quantum security, preserving the reliability and transparency of the electoral process. Thus, this study contributes to the advancement of new cryptographic approaches that ensure the security of electronic voting in light of the imminent evolution of quantum computers.

Keywords: Electronic voting. Post-quantum cryptography. Information security. Online voting.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BFV Brakerski-Fan-Vercauteren

CKKS Cheon-Kim-Kim-Song

CVP Closest Vector Problem

ECDSA Elliptic Curve Digital Signature Algorithm

ECiber Estratégia Nacional de Segurança Cibernética

LWE Learning With Errors

NIST National Institute of Standards and Technology

NIZK Non-interactive zero-knowledge proofs

NSA National Security Agency

PQCS Post-Quantum Cryptography Standardization

RLWE Ring Learning With Errors

RSA Rivest-Shamir-Adleman

SVP Shortest Vector Problem

TIC Tecnologias da Informação e Comunicação

ZKPs Zero-knowledge proofs

LISTA DE SÍMBOLOS

$\mathbb{R}$	Conjunto dos números reais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathcal{L}$	Reticulado
B	Base de um reticulado

SUMÁRIO

1 INTRODUÇÃO

O uso das Tecnologias da Informação e Comunicação (TIC) tem exercido um impacto profundo e transformador na vida cotidiana de bilhões de pessoas ao redor do mundo nos últimos anos. Uma das aplicações mais relevantes dessas tecnologias ocorre no campo da democracia, onde elas têm desempenhado um papel crucial no suporte à tomada de decisões, especialmente por meio de sistemas eletrônicos de votação.

A votação eletrônica (*e-voting*) é definida como um sistema que possibilita aos eleitores registrarem suas escolhas ou votarem em candidatos durante uma eleição. A adoção desses sistemas no processo eleitoral pode oferecer diversas vantagens em relação ao modelo tradicional de votação em papel. Entre essas vantagens, destacam-se a maior precisão nos resultados, a rapidez na contagem dos votos, a redução de erros humanos, a maior acessibilidade para pessoas com deficiência, além de recursos como a contagem automática dos votos (4).

Os sistemas eletrônicos de votação podem ser classificados em dois tipos principais: a votação eletrônica supervisionada fisicamente e a votação eletrônica remota via internet, também conhecida como *i-voting*. No modelo supervisionado, os eleitores comparecem a seções eleitorais específicas e utilizam equipamentos eletrônicos configurados para a votação. Esse modelo é amplamente adotado em diversos países, incluindo o Brasil (5). Já no modelo *i-voting*, os eleitores podem registrar suas escolhas online, de qualquer local, utilizando computadores pessoais ou dispositivos móveis, por meio de aplicativos ou páginas web. Apesar de seu potencial, essa modalidade ainda é pouco utilizada em eleições políticas de grande escala, sendo a Estônia (6) e a Suíça (7) os principais exemplos de sua implementação bem-sucedida.

De maneira geral, o processo eleitoral é dividido em três fases: pré-votação, votação e apuração (8). Para garantir a segurança das informações durante essas etapas em sistemas de votação eletrônica, a literatura apresenta uma variedade de algoritmos de criptografia (9). No entanto, essas propostas não estão imunes a tentativas de ataque, que podem comprometer a integridade e a legitimidade do processo eleitoral, além de potencialmente alterar os resultados. Em resposta a esses riscos, diversos estudos têm sido desenvolvidos nos últimos anos com o objetivo de aprimorar a segurança do processo eleitoral e promover maior transparência em todas as fases da votação (10).

A segurança dos sistemas de votação contra ataques quânticos tem sido uma preocupação constante de diversos autores. Vários trabalhos têm sido propostos na literatura. O trabalho (11) propõe um modelo de votação baseado em reticulados, enquanto (12) propõe um modelo baseado na contagem homomórfica de votos. Além disso, tem sido

observada uma constante evolução em trabalhos relacionados à criptografia pós-quântica e à votação eletrônica.

Entretanto, trabalhos como (13), (14), (15) e (16) não cobrem, individualmente, os requisitos de segurança necessários a cada uma das fases do processo de votação. Esta proposta visa contribuir no desenvolvimento desses estudos, mostrando a viabilidade de implementar recursos computacionais pós-quânticos nas etapas de votação e apuração, de forma a garantir os requisitos de segurança necessários a cada uma delas.

1.1 Motivação

O voto eletrônico possibilita o uso de tecnologias como urnas eletrônicas e internet para auxiliar os procedimentos de votação em um cenário de tomada de decisão. A segurança dos sistemas empregados nesse processo é uma questão de séria preocupação, considerando a necessidade de garantir requisitos de segurança, de modo a assegurar a lisura do processo de votação.

Para garantir o cumprimento desses requisitos, vários esquemas de votação eletrônica têm sido propostos na literatura, destacando-se entre os mais utilizados: votação eletrônica baseada em *mix-net*, votação eletrônica homomórfica, votação eletrônica baseada em assinatura cega, votação eletrônica baseada em *blockchain*, votação eletrônica pós-quântica e implementações híbridas (4).

A criptografia de chave pública empregada na maioria dessas abordagens tem sua segurança garantida pela dificuldade de resolver problemas matemáticos, como a fatoração de inteiros e o cálculo de logaritmos discretos, que demandam tempo subexponencial para serem solucionados em computadores convencionais (17). Esse cenário pode mudar com o advento do computador quântico, que, ao empregar algoritmos como o de Shor, possui a capacidade de resolver esses problemas em tempo polinomial (18). Dessa forma, o surgimento do computador quântico pode comprometer a criptografia utilizada e, consequentemente, a segurança desses sistemas (19).

Diante desse cenário, nos últimos anos tem-se observado um aumento no número de estudos voltados para a implementação de criptografia pós-quântica em sistemas eletrônicos de votação (4). Os algoritmos criptográficos pós-quânticos são aqueles que permanecem seguros em computadores clássicos e são resistentes a ataques quânticos. O estudo e a aplicação da criptografia pós-quântica revela-se como uma ferramenta importante para manter os aspectos de segurança contra ameaças atuais e futuras, especialmente considerando que o desenvolvimento de computadores quânticos está avançando cada vez mais (20).

Destaca-se ainda o crescente interesse de diversos países no desenvolvimento de

soluções em TIC que empregam a criptografia pós-quântica. Nesse contexto, são notáveis as ações dos Estados Unidos, que, desde 2016, por meio do *National Institute of Standards and Technology* (NIST), realizam o concurso *Post-Quantum Cryptography Standardization* (PQCS) para a avaliação de propostas de algoritmos de criptografia pós-quântica para futuras padronizações (21). Dessa forma, espera-se que o uso da criptografia pós-quântica se torne cada vez mais presente e relevante em diversas aplicações cotidianas.

Além disso, de acordo com a Estratégia Nacional de Segurança Cibernética (E-Ciber), que orienta o Governo Federal sobre os principais objetivos e ações na área de segurança cibernética, tanto em termos nacionais quanto internacionais, destacam-se entre as ações estratégicas: o fortalecimento da governança cibernética por meio da adoção de soluções nacionais de criptografia e o incentivo à concepção de soluções inovadoras em segurança cibernética. Ao avaliar as diretrizes propostas por esse documento, pode-se observar a relevância do desenvolvimento e emprego de soluções criptográficas nacionais para contribuir com o fortalecimento da segurança nacional.

Assim, a principal motivação deste trabalho é contribuir para tornar a votação eletrônica mais segura e resistente a computadores quânticos, por meio da utilização de técnicas de criptografia pós-quântica nas fases de votação e apuração.

1.2 Caracterização do Problema

A segurança do voto eletrônico é um elemento crucial para o processo democrático, especialmente em um contexto em que países adotam, de forma crescente, soluções tecnológicas com o objetivo de alcançar maior confiabilidade, agilidade na votação, totalização e divulgação dos resultados eleitorais. Nesse cenário, aprimorar a segurança dos processos eleitorais torna-se altamente relevante, sobretudo diante do avanço dos computadores quânticos (22).

Conforme observado em (23), diferentes cenários de votação demandam distintas propriedades de segurança. A partir da revisão da literatura, conforme explanado na Tabela 3, foi possível identificar lacunas no atendimento a requisitos de segurança nas fases de votação e apuração do processo eleitoral online, principalmente autenticidade, confidencialidade, integridade e anonimato, especialmente no contexto da segurança pós-quântica. Além disso, as assinaturas digitais, as funções de hash e as operações homomórficas ganharam destaque nos trabalhos mais recentes porque proporcionam a oportunidade de atender a esses requisitos.

1.3 Objetivo

- Objetivo geral: Implementar e avaliar algoritmos pós-quânticos que garantam os requisitos de segurança selecionados (anonimato, autenticidade, confidencialidade, integridade) durante as fases de votação e apuração de um processo eleitoral online.
- Objetivos específicos:

  (i) Realizar revisão de literatura para selecionar algoritmos que têm como objetivo garantir os requisitos de autenticidade, integridade, confidencialidade e anonimato nos procedimentos de votação e apuração de um processo eleitoral online.

  (ii) Avaliar o desempenho de algoritmos de criptografia clássica e criptografia pós-quântica selecionados, a fim de verificar a aplicabilidade dos mesmos nos procedimentos do processo de votação e apuração de votação online.

  (iii) Avaliar a viabilidade da proposta, quando consideradas diferentes escalas de eleitores e candidatos.

1.4 Contribuições

As contribuições esperadas para este trabalho são:

(i) Condução de revisão de literatura para selecionar algoritmos que têm como objetivo garantir os requisitos de de autenticidade, integridade, confidencialidade e anonimato nos procedimentos de votação e apuração de um processo eleitoral online.

(ii) Avaliação do desempenho de algoritmos de criptografia clássica e algoritmos criptografia pós-quântica selecionados, a fim de verificar a aplicabilidade dos mesmos nos procedimentos do processo de votação e apuração de votação online.

(iii) Avaliação da viabilidade da proposta, quando consideradas diferentes escalas de eleitores e candidatos.

1.5 Organização da Dissertação

Este trabalho foi segmentado em mais cinco capítulos.

No Capítulo 2 (Fundamentação teórica) é apresentada a teoria que fundamenta o trabalho proposto.

No Capítulo 3 (Revisão da literatura) são apresentados os principais trabalhos relacionados encontrados, os quais constituem o estado da arte do tema de pesquisa, além de um quadro comparativo entre esses trabalhos.

No Capítulo 4 (Cenário proposto) a proposta será apresentada da seguinte forma: inicialmente, será fornecida uma visão geral do processo eleitoral online considerado, seguida pelo detalhamento dos principais componentes. Isso permitirá compreender como cada parte contribui para que a solução proposta alcance os objetivos estabelecidos.

No Capítulo 5 (Experimentos e resultados) será apresentada uma descrição dos cenários de experimentos, seguidos pela realização de testes para avaliar a viabilidade da solução proposta.

No Capítulo 6 (Conclusão e trabalhos futuros) será apresentada uma síntese das conclusões extraídas do trabalho realizado, além da perspectiva de futuros trabalhos sugeridos por esta dissertação.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta uma revisão dos principais conceitos fundamentais para o desenvolvimento deste trabalho. Inicialmente, são abordadas as definições gerais sobre sistemas eletrônicos de votação (Seção 2.1), seguidas pela apresentação dos principais esquemas de votação eletrônica descritos na literatura (Seção 2.2). Em seguida, são discutidos os conceitos de criptografia pós-quântica (Seção 2.3), a definição de função hash e os algoritmos utilizados neste trabalho (Seção 2.4), além da definição de assinatura digital e dos algoritmos empregados (Seção 2.5). Por fim, são apresentados os algoritmos de criptografia homomórfica utilizados (Seção 2.6) e uma breve conclusão (Seção 2.7).

2.1 Conceitos básicos

Esta seção descreve uma estrutura genérica de um sistema eletrônico de votação, que pode servir como um modelo para implementações futuras, considerando os ajustes necessários. Inicialmente, são apresentadas as principais entidades envolvidas no modelo e suas funções. Em seguida, são abordadas as fases do processo eleitoral. Por fim, são discutidas as propriedades de segurança esperadas desses sistemas.

2.1.1 Entidades de um sistema e-voting

As seguintes entidades constituem o sistema eletrônico de votação de acordo com (23):

- Eleitor: indivíduos elegíveis para votar nos candidatos;
- Candidato: indivíduos elegíveis a serem votados na eleição;
- Autenticador: são responsáveis por autenticar os eleitores;
- Autoridade: pessoas encarregadas de conduzir a eleição;
- Auditor: pessoas autorizadas a verificar e revisar os resultados das eleições; e
- Adversário: neste trabalho o adversário considerado será o computador quântico.

2.1.2 Estrutura do sistema eletrônico de votação

Conforme observados em diversos trabalhos na literatura utilizam o modelo descrito em (8) para definir o modelo do sistema de votação, de acordo com esse modelo os sistemas eletrônicos de votação pode ser divididos em três fases: pré-votação, votação e apuração.

O processo na fase de pré-votação inclui a definição da lista de candidatos, o registro dos eleitores aptos e a geração de chaves criptográficas.

Na fase de votação, os eleitores fazem sua escolha, criptografam seu voto, assinam digitalmente e o enviam ao Centro de Controle.

A fase de apuração trata principalmente das atividades de verificação da validade dos votos, da contagem e da divulgação dos resultados das eleições.

A Figura 1 mostra a estrutura da votação eletrônica divididas nas fases citadas.

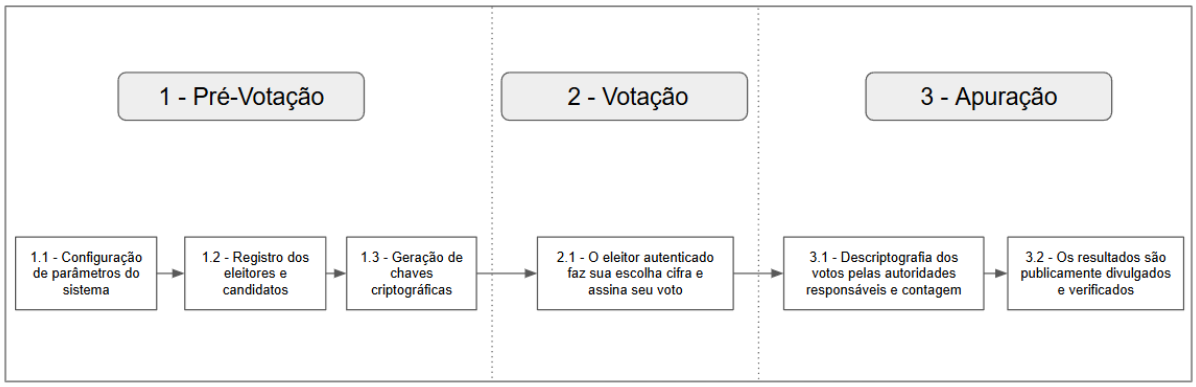

Figura 1 – Estrutura genérica de um sistema eletrônico de votação.

2.1.3 Propriedades de segurança dos sistemas e-voting abordadas na proposta

Com base na revisão da literatura, foi possível identificar uma ampla gama de propriedades de segurança. De acordo com (24), algumas dessas propriedades são equivalentes, embora sejam apresentadas com termos diferentes. A maioria das propostas de modelos de votação eletrônica não consegue atender a todos os requisitos de segurança devido a contradições entre algumas dessas propriedades. Por exemplo, o compromisso com a segurança muitas vezes pode impactar o desempenho dos sistemas, e a busca por maior transparência pode comprometer a confidencialidade (23). Dessa forma, o cumprimento de determinadas propriedades de segurança pode variar dependendo da situação de votação e dos requisitos a serem estabelecidos.

Para selecionar os algoritmos pós-quânticos, serão considerados somente os requisitos de segurança que abordam a integridade, autenticidade, confidencialidade e anonimato, conforme definido na revisão sistemática de (4). Os demais requisitos de segurança e os requisitos funcionais não estão no escopo deste trabalho. A justificativa para considerar somente os requisitos de integridade, autenticidade, confidencialidade e anonimato se deu pela análise dos artigos selecionados na revisão de literatura apresentada no Capítulo 3. A leitura da Tabela 3 demonstra que os trabalhos selecionados para a revisão não abordam esses requisitos em sua totalidade.

Os seguintes requisitos de segurança serão observados neste trabalho:

- Confidencialidade: garantia do sigilo das informações processadas durante o processo eleitoral. A confidencialidade é assegurada por meio da utilização de algoritmos de criptografia, garantindo que dados sensíveis, como votos e informações dos eleitores, permaneçam protegidos.

- Anonimato: garantia do sigilo do eleitor, de modo que não seja possível vincular o eleitor ao candidato escolhido. Durante o processo eleitoral, esse requisito pode ser alcançado por meio do emprego de criptografia homomórfica, que permite realizar operações sobre dados cifrados sem a necessidade de descriptografá-los, garantindo a privacidade durante a apuração dos votos.

- Autenticidade: garantia da verificação de autoria do voto dos eleitores aptos, assegurando que o voto foi realmente emitido por um eleitor legítimo. Esse requisito é alcançado por meio do uso de assinaturas digitais, que permitem verificar a autenticidade do voto. Com a assinatura digital, é possível confirmar que o voto foi de fato enviado pelo eleitor autorizado, sem comprometer a segurança do processo eleitoral.

- Integridade: garantia de que os dados de votação não foram alterados durante as fases do processo. Esse requisito é alcançado por meio do uso de funções de hash, que geram um valor único para cada dado de votação. Ao comparar o hash dos dados originais com o hash dos dados após o processamento, é possível garantir que nenhuma alteração foi feita, assegurando a integridade das informações durante todo o processo eleitoral.

2.2 Principais esquemas de votação eletrônica

Nesta seção, é realizada uma breve revisão dos esquemas de votação eletrônica consolidados na literatura, considerando que a maioria dos modelos propostos utiliza esses esquemas ou combinações deles.

2.2.1 Mix-net

As redes mistas (*mix-nets*), introduzidas em (25), consistem em um conjunto de servidores denominados embaralhadores (*mix servers*) que aceitam um lote de mensagens de entrada e as enviam em uma ordem permutada aleatoriamente, de forma que as mensagens de entrada e saída não sejam vinculáveis. Embora originalmente propostas para comunicação anônima por e-mail entre entidades, as redes mistas em eleições têm o objetivo de esconder a origem de uma cédula de votação.

Os responsáveis pela contagem permutam e randomizam as cédulas criptografadas a fim de garantir que o vínculo entre a identidade do eleitor e o voto seja rompido. Esse

processo é essencial para preservar o anonimato dos eleitores, impedindo que a associação entre quem votou e a escolha feita seja detectada, mesmo após a totalização dos votos.

Na Figura 2 é apresentado um modelo genérico de uma *mix-nets* no qual os votos criptografados passam por servidores responsáveis pelo embaralhamento dos votos. Como resultado desse processo, obtém-se a desvinculação entre os eleitores e seus votos, garantindo o anonimato do eleitor.

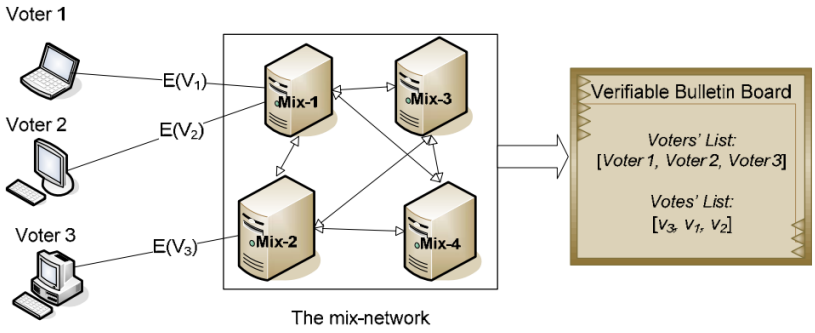

Figura 2 – Votação com mix-net (caso geral) (1).

Apesar de garantir o anonimato do eleitor e a confidencialidade do voto, o esquema em sua concepção original não assegura a autenticidade e a integridade dos dados. Além disso, as duas categorias de *mix-nets* propostas na literatura utilizam os algoritmos RSA e ElGamal (4), que são vulneráveis a ataques de computadores quânticos.

2.2.2 Esquema Homomórfico

De acordo com este modelo, introduzido em (26) cada eleitor cifra seu voto, e a partir do voto cifrado são realizadas operações matemáticas empregando conceitos de homomorfismo.

O homomorfismo permite que o sistema opere no texto cifrado sem decifrá-lo. Por exemplo, supondo que existam os votos cifrados $E_k(V1)$ e $E_k(V2)$, então a operação $E_k(V1 \odot V2)$ pode ser realizada de duas maneiras: a primeira seria a adição modular $E_k(V1 \oplus V2)$ no qual o resultado dessa operação será um texto cifrado que representa a soma dos votos, a segunda operação possível seria a multiplicação modular $E_k(V1 \otimes V2)$ que terá como resultado um texto cifrado com a multiplicação dos votos.

Existem dois tipos de esquemas homomórficos: parcialmente homomórficos (Partially homomorphic encryption (PHE)) e totalmente homomórficos (Fully homomorphic encryption (FHE)).

Os esquemas parcialmente homomórficos são baseados nas propriedades algébricas homomórficas de diversos criptossistemas probabilísticos de chave pública, como RSA e ElGamal. Este tipo de criptografia permite que apenas um tipo específico de operação (como soma ou multiplicação) seja realizada sobre dados criptografados. Dependendo do

sistema, é possível realizar apenas um tipo de operação, mas não ambos simultaneamente. Além disso, os algoritmos empregados são vulneráveis a ataques quânticos (27).

Na Figura 3 é apresentado um esquema de votação parcialmente homomórfico de uma votação binária (sim/não), no qual os votos criptografados são somados como 1 (sim) e -1 (não), através da soma homomórfica é obtido o resultado sem que se conheça os votos individuais.

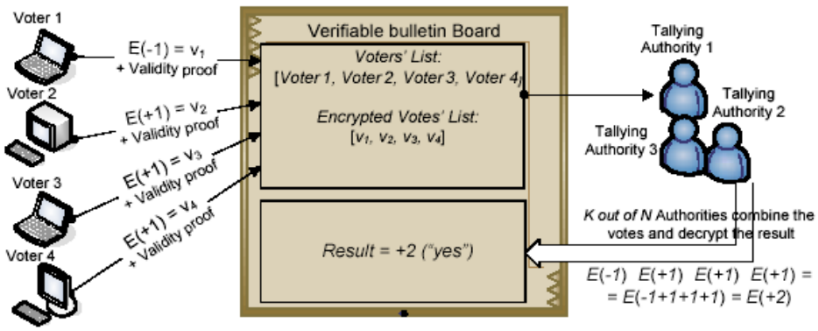

Figura 3 – Votação eletrônica homomórfica (2).

Os esquemas totalmente homomórficos, além de permitirem a soma, possibilitam realizar operações de multiplicação sobre textos cifrados (28). Em sua maioria, esses esquemas empregam criptografia pós-quântica em suas construções, garantindo assim resistência a ataques de computadores quânticos (4).

A principal vantagem dos esquemas homomórficos é que eles não requerem a descriptografia dos votos durante o processo de apuração dos resultados da eleição, garantindo assim o anonimato do eleitor. Além disso, como todas as informações transmitidas são criptografadas, a confidencialidade do sistema também é mantida (14).

2.2.3 Assinatura cega

A assinatura cega é um esquema criptográfico que permite a um usuário assinar uma mensagem de forma que o conteúdo da mensagem permaneça oculto para o assinante durante o processo de assinatura. A proposta original é de (29) e é projetado para garantir que a assinatura de uma mensagem seja realizada sem que o assinante tenha conhecimento do conteúdo dessa mensagem, mesmo que o processo de assinatura seja realizado de forma externa e sem a necessidade de confiar no usuário solicitante.

Esse modelo, quando usado em um protocolo de votação eletrônica, em que um eleitor deseja enviar seu voto a uma autoridade certificadora de maneira simplificada, segue a seguinte sequência:

- O eleitor tem a mensagem original M que ele deseja que a autoridade assine. Supo-

nhamos que a mensagem seja: "Voto para o candidato X".

- Aplicação do cegamento: o eleitor aplica um valor de cegamento r (um número aleatório) à mensagem original para gerar uma nova mensagem cegada M'. Essa operação pode ser feita, por exemplo, multiplicando a mensagem M por r em um espaço criptográfico adequado (como em um esquema baseado em cifras de chave pública). Assim, a mensagem cegada M' é uma versão da mensagem original M, mas "embutida"com um fator de cegamento r, de modo que a autoridade não tenha acesso ao conteúdo real da mensagem.

- O eleitor envia a mensagem cegada M' para a autoridade que sem saber o conteúdo original da mensagem, assina a mensagem cegada M'. Ele gera uma assinatura S' sobre M' utilizando sua chave privada.

- A autoridade cria uma assinatura S' = Sign(Autoridade, M') sobre a mensagem cegada.

- Remoção do cegamento: Após Autoridade assinar a mensagem cegada, Eleitor recebe a assinatura S'. Ela então "remove"o fator de cegamento r da assinatura, de forma que ele tenha uma assinatura válida S sobre a mensagem original M.

- O Eleitor aplica um processo para "descegar"a assinatura, resultando na assinatura final S = Descegar(S'), que agora é válida para a mensagem original "Voto para o candidato X".

Assim, o eleitor obteve uma assinatura válida sobre a sua mensagem original sem que a Autoridade soubesse qual era o conteúdo da mensagem no momento em que a assinou. Isso garante que a privacidade do eleitor seja preservada, ao mesmo tempo em que a assinatura da autoridade valida a autenticidade da mensagem.

O objetivo desse processo é assegurar tanto o sigilo do voto quanto a autenticidade do eleitor, uma vez que a autoridade eleitoral não pode associar a assinatura ao conteúdo específico do voto. Dessa forma, o eleitor tem a garantia de que seu voto permanece anônimo, enquanto o sistema pode verificar a autenticidade da assinatura. No entanto, a concepção original deste esquema não garante o requisito de integridade e não oferece resistência a ataques de computadores quânticos.

2.2.4 Blockchain

Esse novo esquema tem surgido nos últimos anos em trabalhos como (30), com a principal característica sendo o uso de blockchain para armazenar cédulas de votação. O emprego dessa tecnologia visa oferecer aos sistemas de votação maior transparência, segurança e resistência a adulterações (31).

A blockchain armazena periodicamente informações de transações em lotes chamados blocos. Cada bloco recebe um hash, que funciona como uma impressão digital, e aponta para o hash do bloco anterior, formando uma cadeia contínua. Esse modelo torna extremamente difícil a alteração do conteúdo dos blocos devido à combinação de funções hash, que vinculam os blocos de maneira criptográfica, e à necessidade de consenso da maioria da rede descentralizada para validar qualquer alteração, tornando praticamente impossível modificar dados sem ser detectado (32).

No contexto da votação eletrônica, cada voto é criptografado e registrado em um bloco dentro da blockchain, formando um histórico de votos que pode ser verificado por todos os participantes do sistema. Além disso, uma vez que um voto é registrado na blockchain, ele se torna imutável, tornando virtualmente impossível alterar os resultados sem o consenso da maioria dos participantes da rede, garantindo assim a integridade dos votos (33).

Apesar de existirem algumas propostas baseadas nessa tecnologia, o voto eletrônico baseado em blockchain ainda está em estágio inicial. As propostas existentes ainda não possibilitam a aplicação em eleições de grande escala, principalmente devido à complexidade envolvida na operação de um grande volume de dados (34).

2.2.5 Esquema baseado em Criptografia Pós-Quântica

A utilização da criptografia pós-quântica em esquemas de votação eletrônica é uma área emergente de pesquisa, com poucas implementações práticas até o momento. A segurança desses sistemas é garantida pelo uso de algoritmos criptográficos pós-quânticos, que são seguros em computadores clássicos e resistentes a ataques quânticos. Como parte da proposta deste trabalho, a criptografia pós-quântica será detalhada na seção 2.3

2.2.6 Esquemas híbridos

Um esquema híbrido refere-se a um modelo construído pela integração de dois ou mais esquemas criptográficos. Esse tipo de esquema combina as vantagens e propriedades de segurança das ferramentas criptográficas envolvidas, enquanto minimiza as fraquezas que podem existir quando cada ferramenta é utilizada isoladamente. Exemplos desses esquemas incluem:

- O esquema que combina votação eletrônica baseada em mix-net e homomórfica aproveita as vantagens de ambos os métodos: a votação homomórfica proporciona um processo de contagem simples, enquanto a *mix-net* não requer a verificação de validade dos votos e é adequada para eleições complexas (35).

- O esquema que combina votação eletrônica homomórfica e assinatura cega aproveita a propriedade homomórfica aditiva, permitindo a obtenção dos resultados sem a necessidade de descriptografar as cédulas. Ao mesmo tempo, a assinatura cega garante o anonimato da identidade do eleitor e dos votos (36).

A maioria dos sistemas que utilizam criptografia pós-quântica adota uma abordagem híbrida, geralmente combinando modelos já consolidados e substituindo a criptografia tradicional por algoritmos pós-quânticos (4).

A proposta deste trabalho apresenta um modelo híbrido que utiliza criptografia pós-quântica totalmente homomórfica para garantir os requisitos de confidencialidade e anonimato. Além disso, serão utilizadas duas funções criptográficas: função hash e assinatura digital adicionais para assegurar os requisitos de integridade e autenticidade, que serão descritas nas próximas seções.

2.3 Criptografia pós-quântica

A criptografia pós-quântica é um campo da criptografia dedicado ao desenvolvimento de sistemas que são seguros contra ataques de computadores quânticos. Seu objetivo é garantir a proteção de informações sensíveis, mesmo em um cenário futuro onde os computadores quânticos se tornem amplamente disponíveis e eficientes.

2.3.1 Principais abordagens de criptografia pós-quântica

Existem na literatura várias propostas de criptografia segura contra computadores quânticos, em (3) estes modelos são classificados 4 tipos básicos de algoritmos criptográficos, conforme observado na Figura 4.

- Assinaturas baseadas em hash: esquema criptográfico que usa funções de hash como seu bloco de construção central. A segurança desses esquemas é baseada na resistência à colisão e na resistência à inversão da função de hash utilizada (37). O objetivo da função de hash é garantir a integridade dos dados, gerando um valor fixo para uma entrada, de forma que qualquer alteração mínima nos dados resulte em um hash completamente diferente.
- Criptografia baseada em sistemas multivariados: esquema criptográfico em que a segurança está relacionada a dificuldade de resolver estruturas de equações não lineares sobre corpos finitos é a base de esquemas de criptografia multivariada (3).
- Criptografia baseada em teoria dos códigos: esquema criptográfico em que a mensagem criptografada é enviada adicionada a um vetor erro, sendo usado pelo receptor um código de correção de erros para decriptar a mensagem (38).

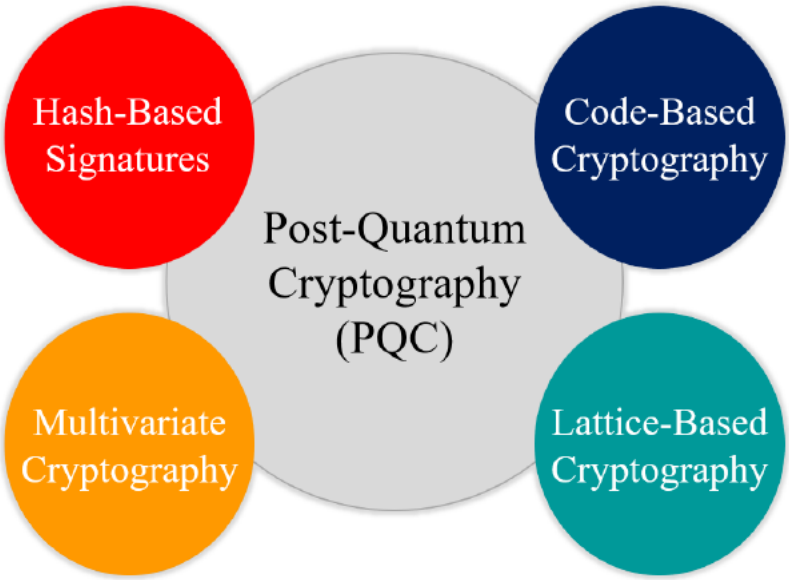

Figura 4 – Tipos básicos de criptografia pós-quântica. (3).

- Criptografia baseada em reticulados: esquema criptográfico que utiliza propriedades matemáticas de reticulados, que são estruturas algébricas discretas. Essa abordagem busca explorar a dificuldade de resolver problemas relacionados a reticulados, como o problema do vetor mais curto (*Shortest Vector Problem* - SVP) e o problema do vetor mais próximo (*Closest Vector Problem* - CVP), para garantir a segurança das informações (3).

Apesar de todas as abordagens possuírem segurança em nível pós-quântico, a criptografia baseada em reticulados tem se destacado como uma solução promissora devido à sua flexibilidade, desempenho e aplicabilidade em diversos problemas de segurança, como criptografia de chave pública, assinatura digital e criptografia homomórfica (3). Além disso, é importante destacar que os dois principais algoritmos recomendados pelo NIST para o emprego em criptografia de chave pública e assinatura digital são baseados em reticulados (39) (40).

2.3.2 Reticulado

Um reticulado é um conjunto de pontos no espaço n-dimensional com uma estrutura periódica (41). De maneira mais formal, dados n vetores linearmente independentes, temos que B é a base do reticulado definida como:

$$B = \{b_1, b_2, b_3, \ldots, b_n\}, \quad b_k \in \mathbb{R}^n \tag{2.1}$$

O reticulado gerado por eles é o conjunto de vetores dado por:

$$\mathcal{L}(B) = \mathcal{L}(b_1, b_2, b_3, \ldots, b_n) = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z} \right\} \tag{2.2}$$

Um reticulado pode ser gerado a partir de diferentes bases. Essas bases podem ser consideradas boas ou ruins, dependendo do tamanho e da ortogonalidade dos vetores que as compõem. Um conjunto de vetores pequenos e relativamente ortogonais constitui uma base considerada boa. Em contraste, vetores grandes e não ortogonais geralmente compõem bases ruins, pois exigem combinações complexas para gerar o mesmo reticulado. Sistemas de chave pública baseados em reticulados utilizam boas bases para gerar chaves privadas e bases ruins para as chaves pública (41).

A Figura 5 a apresenta um reticulado em $\mathbb{R}^2$ e duas bases distintas .

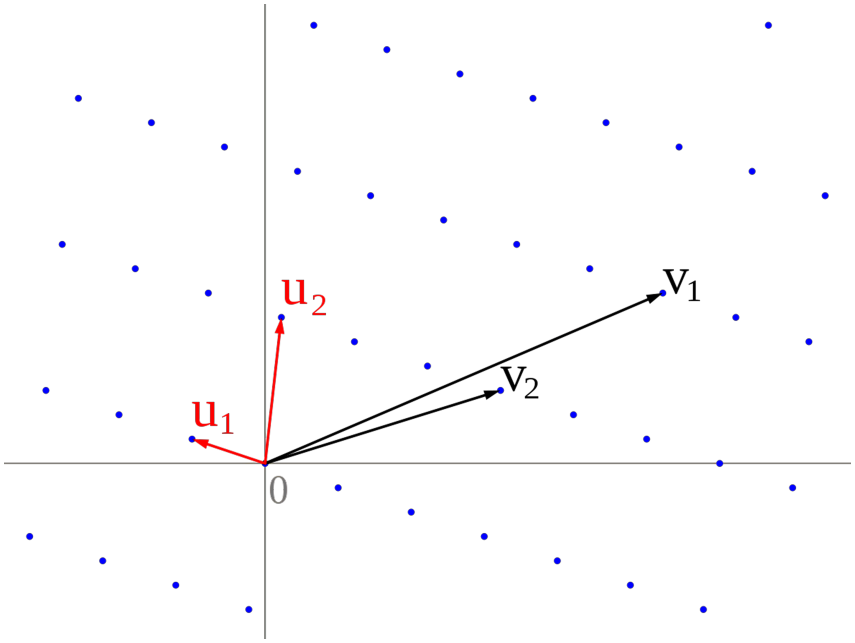

Figura 5 – Reticulado em $\mathbb{R}^2$ e duas bases distintas.

O desenvolvimento dos estudos sobre reticulados no contexto da criptografia ganhou relevância a partir dos resultados obtidos em (42), que propôs que os reticulados poderiam ser usados não apenas como uma ferramenta para a criptoanálise, mas também para construir primitivas criptográficas.

2.3.3 Problema do Vetor Mais Curto (SVP)

O problema do vetor mais curto consiste em encontrar o vetor não nulo de menor norma dentro de um reticulado dado. Formalmente, dado um reticulado $\mathcal{L}$ gerado por uma base B, o objetivo é encontrar um vetor $\mathbf{v} \in \mathcal{L} \setminus \{0\}$ tal que:

$$\|\mathbf{v}\| = \min_{\mathbf{w} \in \mathcal{L} \setminus \{0\}} \|\mathbf{w}\|. \tag{2.3}$$

Esse problema é fundamental na teoria dos reticulados e está intimamente relacionado à segurança de muitos sistemas criptográficos baseados em reticulados. A dificuldade de resolver o SVP é uma das razões pelas quais esses sistemas são considerados seguros, pois a busca por um vetor de norma mínima em um reticulado é um problema de complexidade computacional elevada (42).

2.3.4 Problema do Vetor Mais Próximo (CVP)

O problema do vetor mais próximo consiste em, dado um reticulado $\mathcal{L}$ e um ponto arbitrário $\mathbf{t} \in \mathbb{R}^n$, encontrar o vetor $\mathbf{v} \in \mathcal{L}$ mais próximo de $\mathbf{t}$. Formalmente, o objetivo é minimizar a distância Euclidiana entre o ponto $\mathbf{t}$ e os vetores do reticulado, ou seja, resolver a seguinte equação:

$$\mathbf{v} = \arg\min_{\mathbf{w} \in \mathcal{L}} \|\mathbf{w} - \mathbf{t}\|. \tag{2.4}$$

Esse problema é essencialmente uma versão do problema do vetor mais curto (SVP), mas no caso do CVP, o objetivo não é encontrar o vetor de menor norma dentro do reticulado, mas sim o vetor que é mais próximo de um ponto arbitrário $\mathbf{t}$ fora do reticulado (42).

A dificuldade do CVP está no fato de que, dado um ponto $\mathbf{t}$, encontrar o vetor $\mathbf{v}$ no reticulado $\mathcal{L}$ que minimiza essa distância não é uma tarefa simples, especialmente em espaços de alta dimensão (43).

2.3.5 Learning With Errors (LWE)

O LWE é um problema fundamental na criptografia baseada em reticulados, que consiste em encontrar um segredo $s \in \mathbb{Z}_q^n$ de uma sequência de equações lineares aproximadas em s (44).

De forma geral, o problema pode ser definido dado: a é um polinômio com coeficientes aleatoriamente amostrados em $\mathbb{Z}_q^n$, onde n e q são o grau e o módulo do reticulado, respectivamente, e e é um vetor de erros pequenos também aleatórios. Dada a equação abaixo, temos o par (a, b) como chave pública, e s como chave privada.

$$(s, a_i) + e_i = b_i \quad | \quad 1 \leq i \leq n \tag{2.5}$$

A segurança do LWE é baseada na dificuldade de resolver esse sistema de equações para o vetor secreto s quando o erro e é pequeno, ou seja, as perturbações nos resultados tornam o sistema de equações difícil de resolver, mesmo com o conhecimento da chave pública a e dos valores de b. Em outras palavras, mesmo com acesso a várias instâncias do

problema, a tarefa de recuperar o vetor secreto s é considerada difícil para um adversário, especialmente quando n e q são suficientemente grandes (44).

2.4 Funções hash

A função hash é um algoritmo matemático que transforma um dado (como um arquivo, senha ou informações) em um conjunto hexadecimal de tamanho fixo, conhecido como resumo (45).

A função hash é amplamente utilizada para gerar um resumo de tamanho estabelecido a partir de dados de tamanho variável, garantindo que, até mesmo pequenas mudanças nos dados, resultem em um resumo completamente diferente. Essa propriedade é fundamental para garantir a integridade dos dados, pois qualquer alteração no conteúdo de um arquivo ou mensagem é detectada imediatamente pela diferença no hash.

Na verificação de integridade, a função hash é aplicada diretamente sobre o dado, gerando e salvando o resumo correspondente. Após o dado ser transmitido ao receptor, a função hash é aplicada novamente sobre o dado recebido para gerar um novo resumo. Se os resumos coincidirem, presume-se que o dado não foi alterado. Caso os resumos sejam diferentes, recomenda-se realizar um novo download do arquivo. Esse processo é ilustrado de forma resumida na Figura 6.

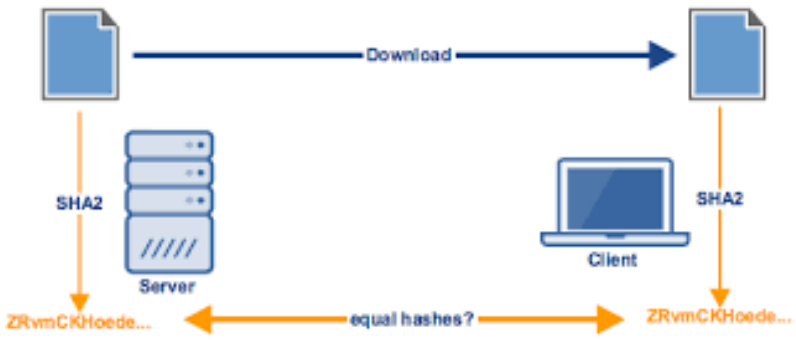

Figura 6 – Verificação da integridade, com função de hash.

No contexto da votação eletrônica, as funções de hash podem ser usadas para garantir a integridade das cédulas de votação, assegurando que o voto não foi alterado durante a transmissão do eleitor para o centro de controle dos votos (14).

2.4.1 SHA-2

O SHA-2 é uma família de funções hash desenvolvida pela (*National Security Agency*) NSA e padronizada pelo NIST em 2001 (46). Ele inclui variantes como SHA-224, SHA-256, SHA-384 e SHA-512, que possuem diferentes tamanhos de saída e níveis de segurança. Sua estrutura baseia-se na função de compressão Merkle–Damgård (47) e utiliza

operações *bitwise*, como rotações, adições modulares e expansões de mensagens. A adoção massiva do SHA-2 ocorreu após a descontinuação do SHA-1, que se tornou vulnerável a colisões (48).

Embora o NIST tenha selecionado o algoritmo SHA-3 como o padrão para funções hash em futuras aplicações (49), o SHA-2 continua sendo amplamente utilizado, principalmente devido à sua presença em sistemas legados, como assinaturas digitais, blockchain, certificados SSL/TLS e proteção de senhas (50).

2.4.2 SHA-3

O SHA-3 foi desenvolvido após uma competição pública organizada pelo NIST para criar uma nova função hash que pudesse servir como alternativa ao SHA-2, sendo padronizado em 2015. Após a competição, o algoritmo Keccak foi escolhido (49).

Diferente do SHA-2, que utiliza a função Merkle–Damgård, o SHA-3 adota a construção sponge, que processa a entrada por meio de uma permutação iterativa, tornando-o mais resistente a ataques como colisões, ataques de extensão de comprimento e pré-imagem. Ele suporta diferentes tamanhos de saída, incluindo SHA3-224, SHA3-256, SHA3-384 e SHA3-512, além das variantes SHAKE128 e SHAKE256, que permitem gerar saídas de tamanho variável (49).

Embora o SHA-3 ofereça vantagens em termos de segurança, ele não substituiu completamente o SHA-2. O SHA-2 continua a ser amplamente utilizado, especialmente porque é eficiente contra as ameaças atuais e está bem estabelecido em várias aplicações. Por outro lado, o SHA-3 foi projetado para ser uma alternativa de segurança mais robusta, com maior resistência a certos tipos de ataques e maior flexibilidade. Ele é especialmente importante em contextos onde a segurança adicional é necessária, como sistemas pós-quânticos (50).

2.4.3 BLAKE2

O BLAKE2 é um algoritmo de hash projetado como uma alternativa mais rápida e segura ao SHA-2 e SHA-3, tendo sido padronizado em 2012. Ele é baseado no BLAKE, um dos finalistas da competição do NIST para o SHA-3, mas que não foi escolhido como vencedor. BLAKE2 foi desenvolvido para ser mais eficiente que SHA-2 e SHA-3, mantendo um nível de segurança comparável ao SHA-3 (51).

Ele possui duas principais variantes: BLAKE2b, otimizado para arquiteturas de 64 bits, e BLAKE2s, projetado para 32 bits.

O algoritmo é amplamente utilizado em aplicações como criptografia de arquivos, autenticação de mensagens (HMAC), proteção de senhas (como no Argon2) e integridade de software. Diferentemente dos algoritmos baseados em Merkle-Damgård, BLAKE2

usa um esquema de compressão inspirado no cifrador ChaCha20, eliminando algumas vulnerabilidades conhecidas (52).

No estágio atual, o BLAKE2 embora mais rápido, tem resistência a ataques quânticos ainda em avaliação (53). Dessa forma, a recomendação atual do NIST para função hash pós-quântica segue sendo o SHA-3 (49).

2.5 Assinatura digital

A assinatura digital desempenha um papel crucial em sistemas de votação eletrônica, garantindo a autenticidade do voto de cada eleitor. Em um sistema de votação eletrônica, cada eleitor possui uma chave privada associada a uma chave pública. Quando o eleitor emite seu voto, o voto é assinado com sua chave privada, criando uma assinatura digital única. Essa assinatura digital serve como uma prova de que o voto foi feito de forma legítima por um eleitor autenticado (54).

A assinatura digital é criada por meio de um algoritmo de criptografia assimétrica. A Figura 7 apresenta uma representação do emprego de assinatura digital em um processo eleitoral, no qual o voto do eleitor é criptografado com sua chave privada, gerando uma assinatura que é enviada a um Centro de Controle. Quando o voto é recebido, os autenticadores podem verificar a assinatura utilizando a chave pública do eleitor, garantindo que o voto foi de fato emitido pelo eleitor legítimo.

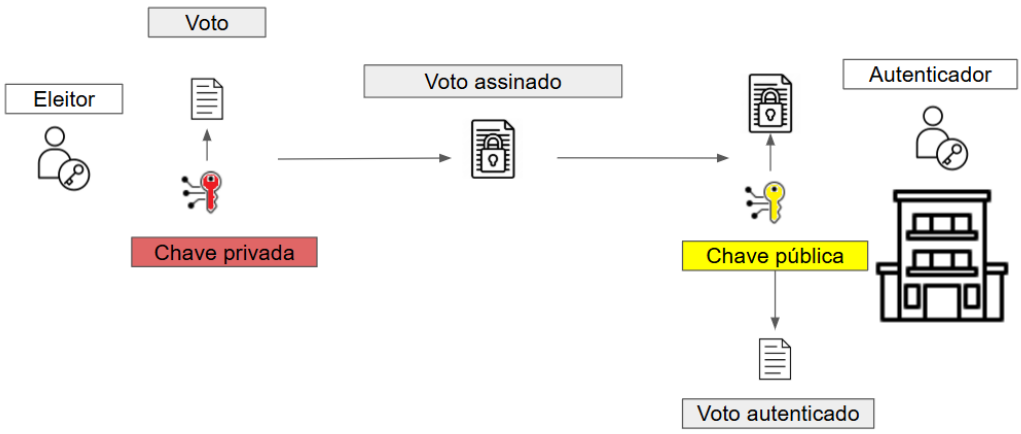

Figura 7 – Assinatura digital em sistemas de votação eletrônica

A utilização de assinaturas digitais também facilita a transparência e a auditoria dos resultados da eleição, já que a verificação da autenticidade dos votos pode ser feita de forma independente por qualquer parte autorizada. (55).

2.5.1 CRYSTALS-Dilithium

CRYSTALS-Dilithium é um algoritmo de assinatura digital baseado em reticulados e foi uma das principais escolhas do NIST no processo de padronização de criptografia pós-quântica. Sua segurança baseia-se no problema matemático do LWE (Learning With Errors) em reticulados e é considerado resistente a ataques de computadores quânticos (56).

O algoritmo foi projetado para ser eficiente, oferecendo assinaturas de tamanho moderado e verificações rápidas, o que o torna adequado para sistemas de alto desempenho. Além disso, o CRYSTALS-Dilithium é altamente resistente a ataques de colisão, tornando-o uma opção segura para assinaturas digitais em sistemas de longa duração. Ele também foi desenvolvido com foco na eficiência de recursos, permitindo sua implementação em dispositivos com capacidade de processamento limitada (57).

Como resultado do processo de padronização de assinaturas digitais pós-quânticas realizado pelo NIST, o CRYSTALS-Dilithium foi escolhido como o principal padrão para assinaturas digitais (40). Assim, ele é o algoritmo recomendado para substituir os tradicionais algoritmos de assinatura digital RSA e ECDSA em um cenário pós-quântico.

2.5.2 ECDSA

A assinatura digital baseada em curvas elípticas (ECDSA - Elliptic Curve Digital Signature Algorithm) tem se destacado no campo da criptografia devido à sua eficiência e segurança. O uso de curvas elípticas permite a geração de chaves mais curtas com o mesmo nível de segurança de algoritmos tradicionais, como RSA (58).

Além disso, as curvas elípticas são altamente eficientes em termos de processamento computacional, o que torna a assinatura digital mais rápida e com menor consumo de recursos. Estudos demonstram que a criptografia baseada em curvas elípticas é uma alternativa robusta e escalável para a assinatura digital em ambientes de alta performance (58).

Embora o algoritmo ECDSA seja considerado seguro contra ataques realizados por computadores clássicos, ele pode ser vulnerável a ataques de computadores quânticos, especialmente com o uso do algoritmo de Shor (18), que pode comprometer a segurança das curvas elípticas. Em um cenário pós-quântico, é provável que o ECDSA seja substituído por algoritmos de assinatura digital baseados em criptografia resistente a ataques quânticos.

2.5.3 SPHINCS+

O SPHINCS+ é um algoritmo de assinatura digital baseado em árvores de hash, que oferece segurança por meio da dificuldade de pré-imagem e colisão das funções hash, o que

o torna resistente a ataques quânticos. Uma das principais vantagens do SPHINCS+ é sua independência de problemas estruturados específicos, como LWE ou SVP, conferindo-lhe uma robustez adicional contra avanços na criptanálise (59).

No entanto, a desvantagem do SPHINCS+ está no tamanho das assinaturas, que são significativamente maiores do que as de outros algoritmos, como CRYSTALS-Dilithium, o que pode torná-lo menos eficiente para algumas aplicações. Além disso, o tempo de verificação também é mais longo, o que o torna menos atraente para sistemas de alto desempenho (59).

Apesar dessas desvantagens, o SPHINCS+ oferece uma solução sólida e segura, especialmente em contextos onde a segurança à prova de colisões é crucial e a eficiência de tempo não é a principal preocupação. Sua resistência comprovada contra ataques quânticos, combinada com a independência de problemas de reticulado, faz do SPHINCS+ uma das opções mais promissoras para o futuro da criptografia pós-quântica. Como resultado do processo de padronização realizado pelo NIST, o SPHINCS+ foi selecionado como uma opção alternativa para padronização como algoritmo de assinatura digital seguro em um cenário pós-quântico (60).

2.6 Criptografia homomórfica

A criptografia homomórfica é um método de criptografia que permite realizar operações sobre dados cifrados sem a necessidade de descriptografá-los. Isso significa que é possível processar informações protegidas sem expô-las, garantindo a privacidade durante o processamento. A principal vantagem dessa técnica é a capacidade de realizar cálculos diretamente sobre dados sensíveis, o que é particularmente útil em cenários de votação eletrônica, onde dados privados precisam ser analisados sem comprometer a segurança. Assim, a criptografia homomórfica assegura os requisitos de segurança, como a confidencialidade por meio da criptografia dos dados trafegados, e o anonimato, garantido pela soma homomórfica, que possibilita desvincular o eleitor de sua escolha no processo eleitoral.

2.6.1 Paillier

Paillier é um algoritmo de criptografia homomórfica baseado em teoria dos números e na dificuldade de fatoração. Ele permite operações de soma sobre dados cifrados, ou seja, é homomórfico aditivo (61).

O Paillier é amplamente utilizado em sistemas de votação eletrônica e em aplicações financeiras, onde a privacidade dos valores é essencial, mas ainda é necessário realizar cálculos sobre os dados.

A principal vantagem do Paillier é sua segurança robusta, que se baseia na dificuldade de fatorar números grandes, mas sua principal limitação está no fato de ser um esquema apenas aditivo, não suportando multiplicação diretamente (61).

Embora o algoritmo Paillier seja considerado seguro contra ataques realizados por computadores clássicos atualmente, ele pode ser vulnerável a ataques de computadores quânticos, especialmente com o uso do algoritmo de Shor (18). A capacidade de fatorar números grandes de maneira eficiente com algoritmos quânticos coloca em risco a segurança de sistemas que dependem da dificuldade de fatoração, como o Paillier. Em um cenário pós-quântico, é possível que o algoritmo Paillier seja substituído por alternativas mais resistentes a esses tipos de ataques.

2.6.2 CKKS

O CKKS (Cheon-Kim-Kim-Song) é um esquema de criptografia homomórfica pós-quântico, desenvolvido para operações com dados numéricos aproximados, como cálculos aritméticos em números de ponto flutuante. Este algoritmo foi projetado como uma adaptação mais eficiente da criptografia totalmente homomórfica (FHE), com foco na melhoria do desempenho em ambientes de computação prática (62). Sua principal vantagem é a capacidade de realizar operações sobre grandes volumes de dados, mantendo a privacidade sem comprometer a eficiência operacional.

O CKKS permite realizar multiplicações e somas sobre dados cifrados, facilitando o processamento de dados em formato aproximado. O algoritmo utiliza o conceito de *approximate homomorphism*, que minimiza o aumento exponencial do erro de aproximação durante as operações, um desafio comum nos esquemas de criptografia homomórfica tradicionais (63). Essa abordagem é particularmente útil em contextos onde a precisão exata pode ser sacrificada em favor de maior velocidade e menor consumo de recursos computacionais, como na realização da soma de um grande número de votos.

Em termos de segurança, o CKKS mantém as propriedades essenciais da criptografia homomórfica, incluindo a proteção contra ataques de adversários com poder computacional quântico. O avanço significativo trazido pelo CKKS é permitir o processamento eficiente de dados aproximados sem revelar os dados privados.

2.6.3 BFV

O BFV (Brakerski-Fan-Vercauteren) é um esquema de criptografia homomórfica pós-quântico que permite a realização de operações aritméticas sobre dados criptografados, garantindo a privacidade em aplicações como computação segura na nuvem e votação eletrônica. Ele suporta operações de soma e multiplicação diretamente no domínio cifrado, tornando-o adequado para cenários que exigem processamento eficiente de dados sensíveis

(64).

A segurança do esquema BFV baseia-se no problema do ruído em redes ideais (RLWE - *Ring Learning With Errors*), considerado resistente a ataques quânticos. O esquema utiliza modulação polinomial para realizar operações de criptografia, o que permite representar grandes números de forma compacta e eficiente. Em vez de utilizar números grandes diretamente, como ocorre em esquemas tradicionais, a modulação polinomial possibilita que os números sejam representados por polinômios com coeficientes menores, o que resulta em uma redução no espaço de armazenamento necessário. No entanto, o crescimento do ruído a cada operação limita a profundidade dos cálculos que podem ser realizados antes que a descriptografação se torne imprecisa (64).

Para reduzir o impacto do crescimento do ruído e melhorar o desempenho do esquema, são utilizadas técnicas como relinearização e *bootstrapping*. Essas abordagens ajudam a manter o processo seguro e viável na prática. O BFV tem sido amplamente utilizado em áreas como segurança da informação, análise de dados sensíveis e sistemas de votação eletrônica, devido à sua combinação de segurança robusta e bom desempenho (65). No entanto, para funcionar bem, o algoritmo precisa de ajustes nos parâmetros, como o tamanho dos números e o grau do polinômio, o que exige encontrar um equilíbrio entre segurança e eficiência (64).

2.7 Conclusão

Este capítulo abordou os principais conceitos relacionados aos sistemas de votação eletrônica e à criptografia que serão empregados neste trabalho. Foram apresentadas definições gerais, os requisitos de segurança considerados, os principais esquemas de votação eletrônica descritos na literatura, além dos conceitos de criptografia pós-quântica. Por fim, foi feita uma descrição de todos os algoritmos criptográficos utilizados na proposta, que serão aplicados nas simulações detalhadas no Capítulo 5.

3 REVISÃO DA LITERATURA

Este capítulo apresenta a revisão da literatura, abordando os principais conceitos, teorias dos trabalhos relacionados ao tema em estudo. Inicialmente, será apresentada a metodologia de pesquisa empregada para a seleção dos trabalhos relacionados (Seção 3.1). Em seguida, será feita uma descrição dos trabalhos selecionados (Seção 3.2), finalizando com um quadro comparativo que aponta os esquemas utilizados em cada proposta e os requisitos de segurança abordados em cada trabalho, permitindo, assim, identificar lacunas e áreas de estudo a serem exploradas (Seção 3.3).

3.1 Metodologia de pesquisa

Visando analisar o estado da arte, foi realizado um mapeamento sistemático com o objetivo principal de responder à pergunta: "Como a criptografia pós-quântica tem sido empregada em sistemas de votação eletrônica?".

Conforme observado na Figura 8 Foi estabelecido a seguinte metodologia para a revisão da literatura.

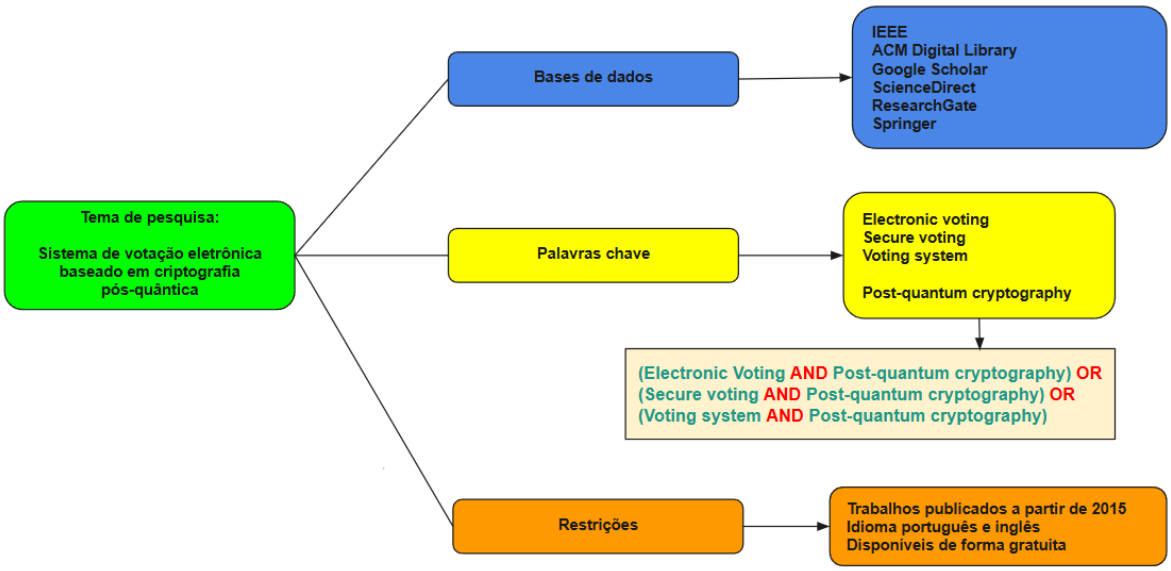

Figura 8 – Dados da pesquisa bibliográfica

As seguintes bases de dados foram empregadas:

- IEEE
- ACM Digital Library

- Google Scholar
- ScienceDirect
- ResearchGate
- Springer

As seguintes strings de buscas foram empregadas: (Electronic Voting AND Post-quantum cryptography) OR (Secure voting AND Post-quantum cryptography) OR (Voting system AND Post-quantum cryptography).

Com as seguintes restrições:

- Critérios de inclusão
  - (i) Trabalhos publicados a partir de 2015 até dezembro de 2023
  - (ii) Idioma português e inglês
  - (iii) Disponíveis de forma gratuita

- Critérios de exclusão
  - (i) Os trabalhos não relacionavam o emprego de criptografia pós-quântica e clássica aos sistemas de votação eletrônica.
  - (ii) Artigos duplicados.

De todos os artigos selecionados foram lidos o título, resumo e palavras-chave e aplicados os critérios de inclusão e exclusão. Os resultados são apresentados na Tabela 1.

Tabela 1 – Resultado da revisão da literatura

Bases de Dados	Resultados	Aplicação de CE e CI
IEEE	122	10
ACM Digital Library		
Google Scholar		
ScienceDirect		
ResearchGate		
Springer		

Vale ressaltar que os estudos de (66) e (67), embora utilizem criptografia pós-quântica, adotam abordagens fora do escopo deste estudo. Dessa forma, foram excluídos da seleção final de trabalhos relacionados.

Os principais dados extraídos desses trabalhos foram: o objetivo de cada estudo, os métodos abordados para a solução dos problemas, as limitações dos métodos propostos e as principais lacunas existentes nessa área de estudo.

3.2 Estado da arte

Os trabalhos relacionados apresentados nesta seção, resumem-se nas principais propostas encontradas que empregam a criptografia pós-quântica na garantia dos requisitos de segurança dos sistemas eletrônicos de votação.

3.2.1 Kaim et al.(2021)

Este trabalho tem como objetivo uma proposta de votação online pós-quântico que emprega uma abordagem híbrida, utilizando como base o esquema original de assinatura cega apresentado em (68) e, para a garantia da proteção pós-quântica, um esquema de criptografia de chave pública baseado em reticulados.

A proposta permite o emprego de sistemas de votação no formato *"vote and go"*, no qual os votantes não precisam esperar o fim da votação para validar seus votos. Além disso, o esquema também evita a obtenção de resultados parciais antes do final da eleição, sendo que essas limitações existem no esquema original de assinatura cega (11).

O autor apresenta solução para os requisitos de anonimato, autenticidade e confidencialidade do voto. Entretanto, a proposta não apresenta soluções para a garantia da integridade dos votos. Além disso, o trabalho apresenta provas teóricas e não apresenta uma implementação prática.

3.2.2 Chillotti et al.(2016)

O objetivo deste trabalho é alterar uma proposta de votação eletrônica já existente, o Helios (69), que é baseado na propriedade homomórfica aditiva de ElGamal (inseguro contra computadores quânticos), para uma proposta de votação pós-quântica empregando um protocolo criptográfico baseado em uma construção criptográfica totalmente homomórfica.

O autor aponta que as principais vantagens da proposta são a sua simplicidade e transparência, e que além disso, o uso de primitivas criptográficas simplifica as provas de confidencialidade e anonimato (13). Ressalta-se que o trabalho apresenta provas teóricas, não havendo, uma implementação prática.

3.2.3 Aziz et al.(2018)

Este trabalho apresenta uma proposta de votação eletrônica pós-quântica que emprega criptografia totalmente homomórfica nas operações de soma sobre os votos criptografados (14). O modelo é implementado utilizando a biblioteca de criptografia homomórfica HELib (70) que é um framework código aberto empregado em diversas aplicações de criptografia homomórfica.

A proposta também garante a utilização de Provas não interativas de conhecimento zero (*Non-interactive zero-knowledge proofs* - NIZK) que consiste em uma condição em que uma parte (o provador P) pode provar para outra parte (o verificador V) sobre a verdade de uma declaração sem revelar nada além desta verdade (71). Este conceito é muito importante nos sistemas de votação eletrônica, uma vez que o eleitor pode validar seu voto, sem que seja necessário revelar seu conteúdo.

Cabe ressaltar que o uso de provas de conhecimento zero (*Zero-knowledge proofs* - ZKPs) na criptografia baseada em reticulados exige a consideração de desafios significativos, como a complexidade computacional e o tamanho das provas. As ZKPs tradicionais, quando adaptadas para a criptografia de reticulados, podem resultar em provas de tamanho significativo, frequentemente na ordem de megabytes. Isso ocorre devido à necessidade de múltiplas iterações para alcançar um erro de solidez negligenciável, o que aumenta tanto o tamanho total da prova quanto o custo computacional associado (72).

O trabalho atende os requisitos se anonimato, confidencialidade e integridade, além disso, o trabalho apresenta uma implementação prática onde é possível verificar a eficiência do modelo em eleições de até 10 milhões de eleitores. Entretanto, o trabalho não apresenta uma solução que garanta o requisito de autenticidade em um nível pós-quântico.

3.2.4 Pinilla(2018)

O autor utiliza de criptografia baseada em reticulados, em conjunto com uma *mix-net*, e assegura os requisitos de anonimato e confidencialidade (73). No entanto, aspectos relacionados aos requisitos de integridade e autenticidade não são discutidos no trabalho. Além disso, a verificação da validade do modelo é realizada de maneira teórica.

3.2.5 Ronne et al.(2020)

O autor combina a criptografia totalmente homomórfica com funções de hash, baseando-se no protocolo de votação resistente à coerção JCJ (74). A proposta garante os requisitos de integridade e anonimato, mas não aborda os requisitos de autenticidade e confidencialidade. Além disso, este trabalho foca exclusivamente na etapa de apuração dos votos, sem apresentar soluções para outras fases do processo de votação (75).

3.2.6 Boyen et al.(2020)

Este trabalho apresenta uma abordagem híbrida, na qual uma *mix-net* é empregada em conjunto com um protocolo baseado em reticulados, com o objetivo de propor um sistema de votação eletrônica pós-quântico que garanta o anonimato e que os servidores de mixagem possam ser auditáveis (76).

Considerando a principal característica das *mix-net*, que é criar um canal de comunicação anônimo entre o eleitor e a central de contagem de votos por meio de servidores de mixagem, a ideia central do trabalho é desenvolver servidores de mixagem que possam ser auditáveis e verificáveis contra possíveis alterações. Dessa forma, torna-se possível identificar eventuais tentativas de fraude e localizar qual servidor deu origem ao problema, por meio de um ou mais auditores. Esse objetivo é alcançado empregando uma característica presente na criptografia baseada em reticulados, conhecida como indistinguibilidade contra ataques adaptativos de texto cifrado escolhido (IND-CCA2) (77).

Embora o requisito de anonimato esteja presente neste trabalho, os requisitos de autenticidade, confidencialidade e integridade não são o foco do estudo. Dessa forma, o modelo tem como foco principal a auditabilidade dos servidores da *mix-net*.

3.2.7 Liao(2020)

A pesquisa apresenta uma proposta de votação eletrônica para vários candidatos, baseada em criptografia totalmente homomórfica e assinatura digital, com o principal objetivo de criptografar votos de forma eficiente e reduzir a dependência de diferentes entidades no sistema de votação (12).

A contagem dos votos é realizada por meio de uma criptografia totalmente homomórfica baseada em reticulados, garantindo, assim, o anonimato do eleitor. Para resolver o problema da autenticação de identidade na votação eletrônica, o Algoritmo de Assinatura Digital ECDSA é utilizado.

A proposta garante os requisitos de anonimato, autenticidade e confidencialidade. Entretanto, não discute soluções para o requisito de integridade. Além disso, o algoritmo de assinatura digital ECDSA não é pós-quântico, sendo, portanto, suscetível a eventuais ataques de computadores quânticos.

3.2.8 Farzaliyev et al.(2021)

O estudo apresenta uma implementação híbrida entre *mix-net* e criptografia baseada em reticulados, com o objetivo de propor um sistema de votação eletrônica pós-quântico. A abordagem combina a principal característica das *mix-net*, que é manter o anonimato

dos eleitores, com a segurança pós-quântica garantida pelos reticulados (15).

A proposta garante os requisitos de anonimato e confidencialidade. No entanto, os requisitos de autenticidade e integridade não são abordados na pesquisa. Além disso, uma das limitações do modelo é que ele pode ser empregado apenas em escalas de até 100.000 votos, tornando necessárias futuras otimizações para votações em grande escala.

3.2.9 Gao et al.(2019)

Este trabalho apresenta uma proposta de votação eletrônica baseada em blockchain que utiliza um esquema de criptografia pós-quântico baseado em teoria dos códigos com o objetivo de fornecer transparência no processo de votação e a integridade dos votos que serão salvos na blockchain (15).

A combinação entre blockchain e criptografia pós-quântica garante ao modelo proposto os seguintes requisitos de segurança: anonimato e integridade dos dados. Uma das limitações da utilização da blockchain, se da pela ineficiência em eleições de grande escala, isso se deve principalmente à complexividade em operar um grande volume de dados na blockchain e da necessidade de esquemas de criptografia mais robustos. Desta forma o modelo proposto se mostra eficiente somente em eleições de pequena escala.

3.2.10 Kho et al.(2019)

Este trabalho, apesar de não apresentar uma nova proposta, realiza uma revisão sistemática abrangente sobre as soluções criptográficas aplicadas aos sistemas de votação eletrônica. Ele explora diferentes esquemas criptográficos, como criptografia homomórfica, assinatura cega, blockchain, *mix-net* e criptografia pós-quântica, comparando suas estruturas, vantagens e desvantagens.

Além disso, o estudo lista diversas propostas existentes na literatura, destacando suas principais características, propriedades de segurança, ferramentas criptográficas empregadas e potenciais fragilidades.

A revisão aborda desafios enfrentados pelos sistemas de votação, como autenticação de identidade e resistência a fraudes. Também são discutidas as limitações das soluções existentes e as dificuldades associadas à implementação de sistemas de votação eletrônica em grande escala. Adicionalmente, destaca-se a importância da adoção de técnicas pós-quânticas para garantir a segurança a longo prazo.

Por fim, o estudo aponta para a necessidade de otimizações e novos algoritmos que melhorem a eficiência e a escalabilidade dos sistemas de votação criptografada.

3.3 Comparação dos trabalhos relacionados

A análise dos trabalhos relacionados permitiu identificar diferentes abordagens para a implementação de criptografia pós-quântica em sistemas de votação eletrônica. Observou-se que a maioria das propostas segue um modelo híbrido, combinando técnicas consolidadas na literatura com criptografia pós-quântica.

Destaca-se que os esquemas mais adotados são baseados em criptografia totalmente homomórfica e em reticulados. No entanto, os principais desafios dessas abordagens estão na complexidade das operações homomórficas e no tamanho das chaves utilizadas nos algoritmos baseados em reticulados (4).

A Tabela 2 apresenta os trabalhos analisados e os respectivos esquemas criptográficos empregados. Vale ressaltar que o estudo de (4), embora descrito nos trabalhos relacionados, não está incluído no comparativo por se tratar de uma revisão sistemática.

Tabela 2 – Relação entre as referências e os esquemas criptográficos utilizados

Referências	Criptografia Homomórfica	Reticulados	Mix-net	Assinatura Digital	Blockchain	Função hash
Kaim et al.(2021)		**X**		**X**		
Chillotti et al.(2016)	**X**					
Aziz et al.(2018)	**X**					**X**
Pinilla(2018)		**X**	**X**			
Ronne et al.(2020)	**X**					**X**
Boyen et al.(2020)		**X**	**X**			
Liao(2020)	**X**			**X**		
Farzaliyev et al.(2021)		**X**	**X**			
Gao et al.(2019)					**X**	

A Tabela 3 sintetiza a avaliação dos trabalhos quanto aos principais requisitos de segurança: anonimato, autenticidade, confidencialidade, integridade e verificabilidade. Entre esses requisitos, anonimato, confidencialidade e verificabilidade do voto se mostram as principais preocupações nos modelos analisados. No entanto, todos os trabalhos apresentam limitações em relação aos requisitos de autenticidade, confidencialidade e integridade, e alguns ainda dependem de algoritmos clássicos em parte do modelo, tornando-se vulneráveis a futuros ataques quânticos.

Referente ao requisito de verificabilidade, para garantir o cumprimento desse requisito, poderia ter sido utilizada prova de conhecimento zero, conforme destacado anteriormente. O uso desse protocolo criptográfico em algoritmos baseados em reticulados é uma tarefa relativamente complexa (72), levando em conta que os algoritmos utilizados neste trabalho são baseados em reticulados. Dada a necessidade de estudos mais detalhados sobre a verificabilidade, optou-se por não abordar esse requisito neste trabalho, deixando-o como possibilidade para trabalhos futuros.

A partir das tabelas comparativas, foi verificado que abordagens híbridas se mostram mais promissoras para alcançar múltiplos requisitos de segurança e garantir proteção

contra ataques quânticos. Dessa forma, este trabalho apresenta um cenário com uma combinação de algoritmos criptográficos pós-quânticos para atender aos requisitos de anonimato, autenticidade, confidencialidade e integridade, os quais serão descritos no próximo capítulo.

Tabela 3 – Relação entre as referências e requisitos de segurança

Referências	Anonimato	Autenticidade	Confidencialidade	Integridade	Verificabilidade
Kaim et al.(2021)	**X**	**X**	**X**		
Chillotti et al.(2016)	**X**		**X**		**X**
Aziz et al.(2018)	**X**		**X**	**X**	**X**
Pinilla(2018)	**X**		**X**		**X**
Ronne et al.(2020)	**X**			**X**	
Boyen et al.(2020)	**X**				**X**
Liao(2020)	**X**	**X**	**X**		
Farzaliyev et al.(2021)	**X**		**X**		**X**
Gao et al.(2019)	**X**			**X**	

4 CENÁRIO PROPOSTO

Este capítulo apresenta o cenário proposto para a avaliação do desempenho dos algoritmos criptográficos. A revisão da literatura revelou que as propostas existentes não atendem simultaneamente a todos os requisitos avaliados (integridade, confidencialidade, anonimato e autenticidade) em um nível de segurança adequado para um cenário pós-quântico.

Diante dessa limitação, propõe-se uma configuração que combina funções criptográficas pós-quânticas, incluindo assinatura digital, funções de hash e criptografia totalmente homomórfica. Considerando que cada uma dessas funções, quando utilizada isoladamente, é resistente a ataques de computadores quânticos e atende a requisitos específicos de segurança, a hipótese deste trabalho é que a combinação dessas técnicas pode viabilizar um protocolo de votação online seguro em um ambiente pós-quântico.

As funções criptográficas empregadas e os respectivos requisitos de segurança que garantem são:

- Função de hash: integridade (Seção 2.4)
- Assinatura digital: autenticidade (Seção 2.5)
- Criptografia totalmente homomórfica: confidencialidade e anonimato (Seção 2.6)

Inicialmente, serão apresentadas as condições iniciais para a validação do cenário proposto. Em seguida, será descrito o modelo da cédula de votação e detalhadas as etapas do processo de votação em que os algoritmos serão empregados.

4.1 Método

A metodologia para o desenvolvimento do ambiente de teste do sistema de votação online pós-quântico será estruturada em duas fases principais do processo eleitoral: a fase de votação e a fase de apuração.

Considerando que a fase de pré-votação envolve aspectos como o registro de eleitores e candidatos, a geração e distribuição de chaves, além da complexidade e necessidade de outras soluções de segurança, optou-se por não implementar essa fase neste trabalho. Assim, as seguintes considerações serão assumidas:

- Todos os eleitores e candidatos já estão cadastrados no sistema, sendo que cada eleitor possui login e senha para acessar o sistema de votação pela internet.

- Durante a fase de pré-votação serão geradas o par de chaves para criptografar homomorficamente os votos, sendo que essas chaves serão derivadas do par de chaves do Centro de Controle, além disso, também serão geradas o par de chaves para assinatura digital.

- No momento em que usuário realiza seu login será enviado um par de chaves para assinatura e outro para criptografar os votos. Essas chaves serão de enviadas de forma criptografada com as senhas dos usuários cadastradas no sistema, utilizando um algoritmo de criptografia simétrico resistente a ataques quânticos.

4.1.1 Modelo da cédula de votação

Com o objetivo de simplificar as operações de soma homomórfica durante o processo de contagem de votos, foi proposto um modelo de representação em formato numérico, no qual cada voto é representado por um número inteiro. Esse modelo facilita a soma homomórfica, permitindo que os votos sejam somados de maneira mais eficiente, reduzindo o custo computacional e o tempo necessário para a realização da contagem dos votos.

O esquema consiste na criação de um número em que diferentes intervalos representam os votos atribuídos a cada candidato dentro de um grupo específico. O início do número é sempre precedido por um algarismo "1", garantindo a contabilização única e individual do voto de cada eleitor.

A Figura 9 ilustra um exemplo prático, considerando uma eleição fictícia com 4 candidatos e até 999 eleitores. Esse modelo não apenas otimiza o processo de contagem, mas também assegura que o sistema permaneça eficiente, mesmo em cenários com grandes volumes de dados.

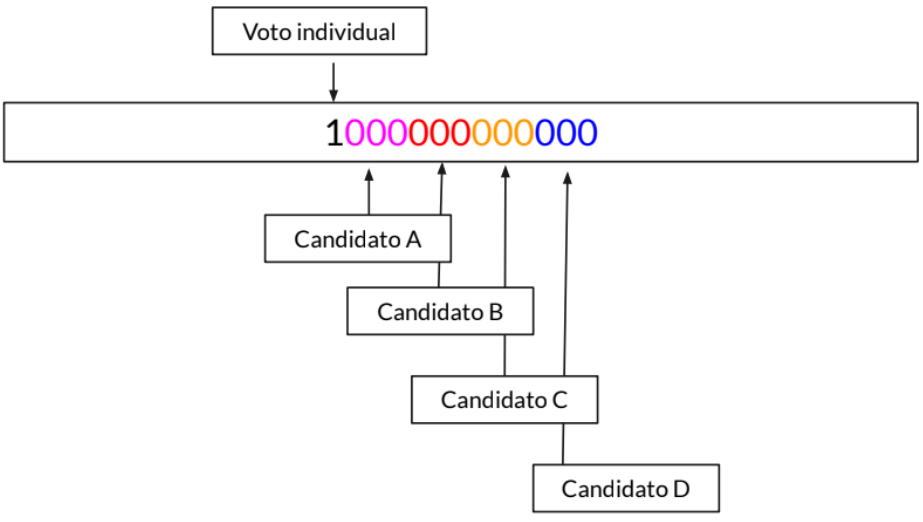

Figura 9 – Representação do voto

Caso um eleitor X escolha o candidato B o voto seria representado com descrito na Figura 10.

Figura 10 – Representação da escolha

Se, ao final de uma eleição com 100 eleitores, os candidatos A, B, C e D tivessem respectivamente os seguintes números de votos: 20, 35, 15 e 30, a soma final dos votos seria representada de acordo com a Figura 11.

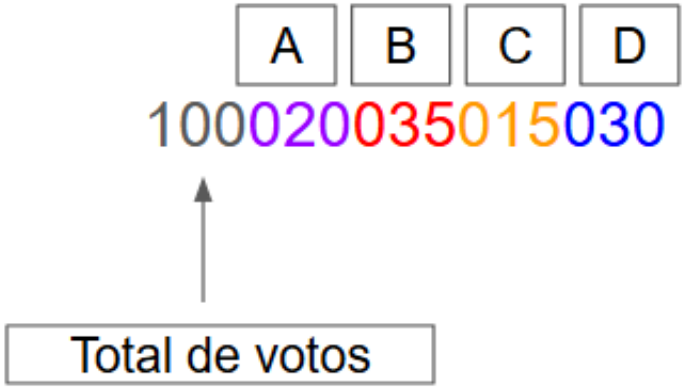

Figura 11 – Contagem final dos votos

Caso o número de candidatos seja ampliado, o modelo pode ser facilmente ajustado com a inserção de intervalos adicionais de valores para acomodar as novas opções. De maneira similar, um aumento no número de eleitores pode ser refletido por meio da expansão do número de algarismos utilizados para representar cada eleitor.

Esse modelo apresenta a vantagem de permitir a contagem da soma total de votos e, simultaneamente, a soma individual de cada candidato. Além disso, tal abordagem garante que os votos individuais de cada eleitor permaneçam confidenciais, assegurando a privacidade no processo de apuração.

4.1.2 Configuração proposta

A Figura 12 apresenta o cenário proposto na fase de votação. Nesta fase, os eleitores previamente cadastrados utilizarão seus dispositivos eletrônicos para acessar o site de votação.

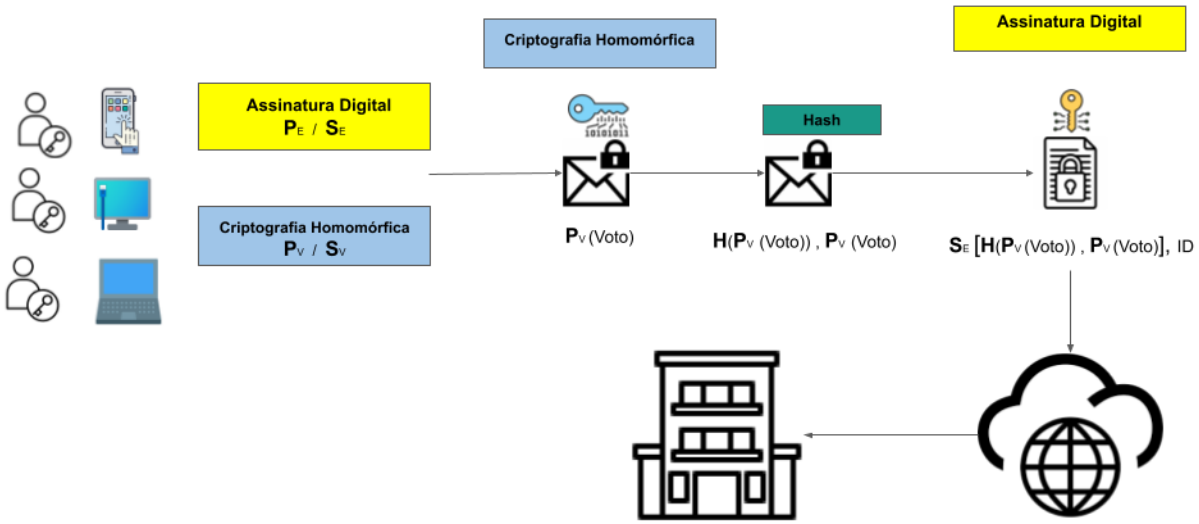

Figura 12 – Visão geral do modelo proposto na fase de votação

Após receberem o acesso para a votação, os eleitores farão sua escolha e o voto será criptografado com a chave pública do voto, utilizando uma criptografia totalmente homomórfica pós-quântica. Os votos criptografados, posteriormente, serão somados. Este procedimento tem como intuito garantir o anonimato do eleitor, pois a soma será realizada sem que haja o conhecimento de quem efetuou o voto em um determinado candidato.

Em seguida, será gerado um hash do voto criptografado utilizando uma função hash com segurança pós-quântica. O principal objetivo dessa função é garantir a integridade do voto, uma vez que, caso haja alguma alteração nos dados durante a transmissão, o hash será alterado, invalidando assim o voto do eleitor.

Após a geração do hash, o eleitor utilizará sua chave privada de assinatura digital pós-quântica para assinar o voto criptografado e o hash gerado. Além disso, será acrescentado um ID do eleitor, de forma que seja possível verificar a assinatura no centro de controle. Após esse procedimento, o sistema enviará o voto para o centro de controle por um canal público (internet). O processo de assinatura digital garante a autenticidade do eleitor, uma vez que somente o votante pode assinar seu voto utilizando sua chave privada.

Levando em consideração as funções criptográficas empregadas durante a fase de votação, o modelo propõe que, mesmo que um adversário com um computador quântico consiga interceptar o voto durante a transmissão, ele não terá acesso ao seu conteúdo, nem poderá alterar as informações da cédula eleitoral ou se passar pelo eleitor.

A Figura 13 apresenta o processo de verificação da assinatura e do hash durante a fase de apuração. O processo de validação do voto ocorrerá pela ordem inversa das etapas realizadas pelo eleitor.

Inicialmente, a assinatura do eleitor será verificada utilizando a chave pública

referente ao ID do eleitor, garantindo a autenticidade do voto.

Após a validação da assinatura, será realizada a verificação da integridade do voto. Um novo hash do voto criptografado será gerado e comparado com o hash enviado pelo eleitor. Caso os valores sejam iguais, terá a garantia de que o conteúdo do voto não foi alterado durante a transmissão. Após essa verificação, o voto estará validado e seguirá para a etapa de contagem dos votos.

Figura 13 – Validação do voto na fase de apuração

A Figura 14 apresenta o processo de soma homomórfica dos votos na fase de apuração

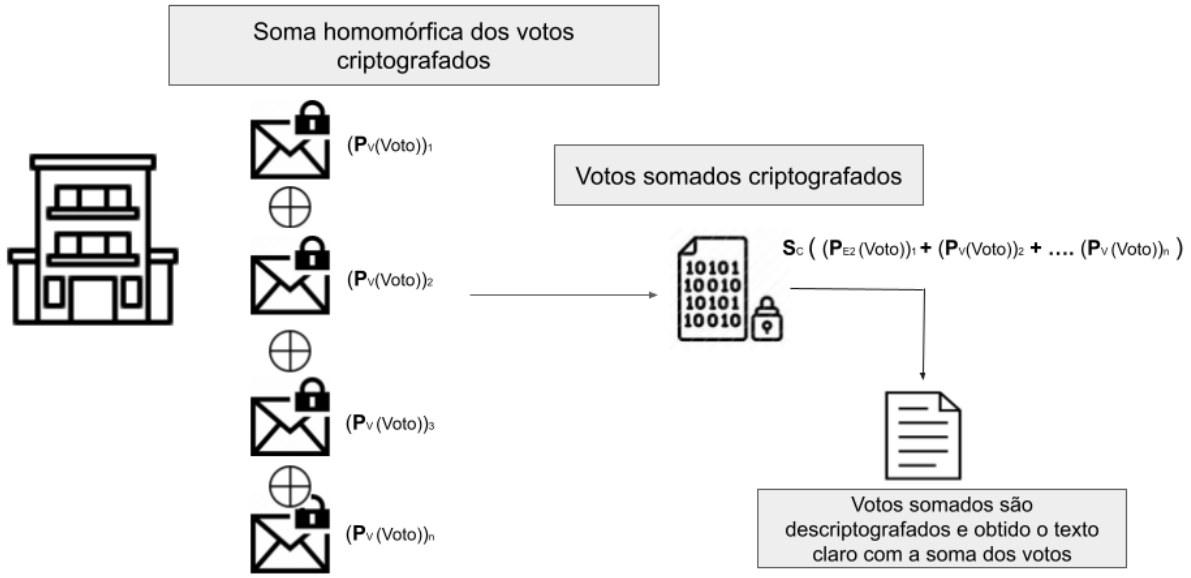

Figura 14 – Contagem dos votos na fase de apuração

Os votos individuais criptografados são somados utilizando funções homomórficas, sem a necessidade de descriptografá-los. Dessa forma, o anonimato dos eleitores é

preservado.

Após a soma homomórfica, a chave privada do centro de controle será utilizada para descriptografar a soma dos votos. Assim, será possível obter o texto claro com o resultado das eleições, sem que se revele a escolha individual de cada eleitor.

Conforme detalhado, o cenário proposto permite o estabelecimento de um sistema de votação online utilizando um canal público (internet), sem comprometer a segurança das informações trafegadas. Além disso, essa configuração pode contar com uma camada adicional de segurança, empregando um canal seguro para o tráfego de dados, como, por exemplo, o uso de VPNs.

5 EXPERIMENTOS E RESULTADOS

Neste capítulo, são apresentados os experimentos realizados com base no cenário proposto.

Inicialmente, foi desenvolvida uma rotina para gerar o modelo de cédula de votação de acordo com a configuração do número de candidatos e eleitores desejados, possibilitando a simulação de diferentes cenários de votação.

A partir desse modelo, procedeu-se à avaliação de diferentes algoritmos de criptografia, com foco no desempenho em relação ao tempo de processamento, medido em segundos, e aos ciclos de CPU. A análise desses parâmetros foi essencial para avaliar a eficiência dos algoritmos criptográficos. Essas medições permitem verificar a possibilidade de otimização de recursos, a identificação de possíveis gargalos e a melhoria do uso do processador.

Em cada função criptográfica avaliada, foram selecionados três algoritmos: um clássico e dois pós-quânticos, escolhidos com base em sua relevância em pesquisas sobre criptografia aplicada à votação eletrônica. A seleção priorizou os algoritmos mais referenciados na literatura dessa área. A justificativa para a escolha dos algoritmos clássicos deve-se à necessidade de comparar seu desempenho com os algoritmos pós-quânticos, a fim de identificar se haverá um grande impacto no desempenho com o uso dos algoritmos pós-quânticos. Além disso, essa comparação visa avaliar a possibilidade de substituição, caso os algoritmos pós-quânticos não se adequem ao cenário proposto.

Após uma análise comparativa, o algoritmo criptográfico mais adequado foi escolhido para ser integrado as simulações. Posteriormente, os três algoritmos selecionados foram incorporados à configuração, permitindo a implementação completa do cenário de votação previsto.

Os resultados obtidos não apenas validaram o cenário proposto, mas também permitiram identificar o desempenho dos algoritmos criptográficos avaliados em diferentes cenários de votação assim como a identificação de potenciais melhorias. Dessa forma, o estudo contribui para o desenvolvimento de abordagens mais eficientes e seguras para a implementação de sistemas de votação eletrônica baseados em criptografia pós-quântica.

5.1 Ambiente de simulação

O ambiente de simulação empregado para a realização dos experimentos descritos neste trabalho foi configurado utilizando a linguagem de programação Python 3.11, com a IDE Visual Studio Code, versão 1.97. A execução dos experimentos foi realizada em

um PC com um processador AMD Ryzen 3 PRO 4350G, com gráficos integrados Radeon, operando a uma frequência de 3,80 GHz. O sistema contava com 16 GB de memória RAM e estava rodando o sistema operacional Windows 10 Pro. Essa configuração proporcionou a infraestrutura necessária para implementar e executar os algoritmos de criptografia clássicos e pós-quânticos, além de permitir a avaliação do desempenho do sistema no contexto de uma aplicação de votação online.

5.2 Simulação com a criptografia homomórfica

Inicialmente, foram realizados testes utilizando algoritmos de criptografia homomórfica. A simulação permitiu a execução de operações de soma diretamente sobre dados cifrados, sem a necessidade de decifrá-los, garantindo assim a privacidade durante o processamento. Para validar o modelo proposto, diferentes experimentos foram conduzidos, analisando o desempenho em termos de tempo de processamento e ciclos de CPU.

Foram avaliados os algoritmos homomórficos Paillier, BFV e CKKS. Para cada um, foi desenvolvida uma rotina que incluiu a geração prévia das chaves pública e privada, a criptografia do voto utilizando a chave pública de cada eleitor, a soma homomórfica e a descriptografia dos votos somados por meio da chave privada do centro de controle responsável pela contagem.

Antes de iniciar cada cenário de votação, foi realizada, para cada algoritmo, uma soma homomórfica em paralelo com uma soma em claro, utilizando os mesmos valores. Ao final, esses resultados foram comparados para verificar se os resultados eram iguais. Esse procedimento teve o objetivo de validar se os algoritmos estavam funcionando corretamente.

No experimento inicial, foram fixados cinco candidatos e 100 eleitores, que escolheram uma das opções disponíveis por meio de uma função randômica, a fim de gerar um resultado o mais aleatório possível. Em seguida, mantendo o mesmo número de candidatos e utilizando o mesmo processo randômico de escolha, foram simuladas votações com 1.000 e 10.000 eleitores para cada algoritmo. Para cada configuração, foram realizadas 10 simulações. As Figuras 15, 16 e 17 apresentam a média dos resultados obtidos para cada algoritmo.

Os resultados obtidos mostram que houve uma variação linear no tempo de processamento e no número de ciclos de clock no algoritmo de Paillier: à medida que o número de eleitores foi multiplicado por 10, tanto o tempo de processamento quanto os ciclos de clock apresentaram variações proporcionais. Além disso, destaca-se que o algoritmo de Paillier apresentou o pior desempenho em relação aos parâmetros avaliados.

Os algoritmos BFV e CKKS tiveram um desempenho superior, especialmente para valores a partir de 1.000 eleitores. Para o número de 10.000 eleitores, o CKKS

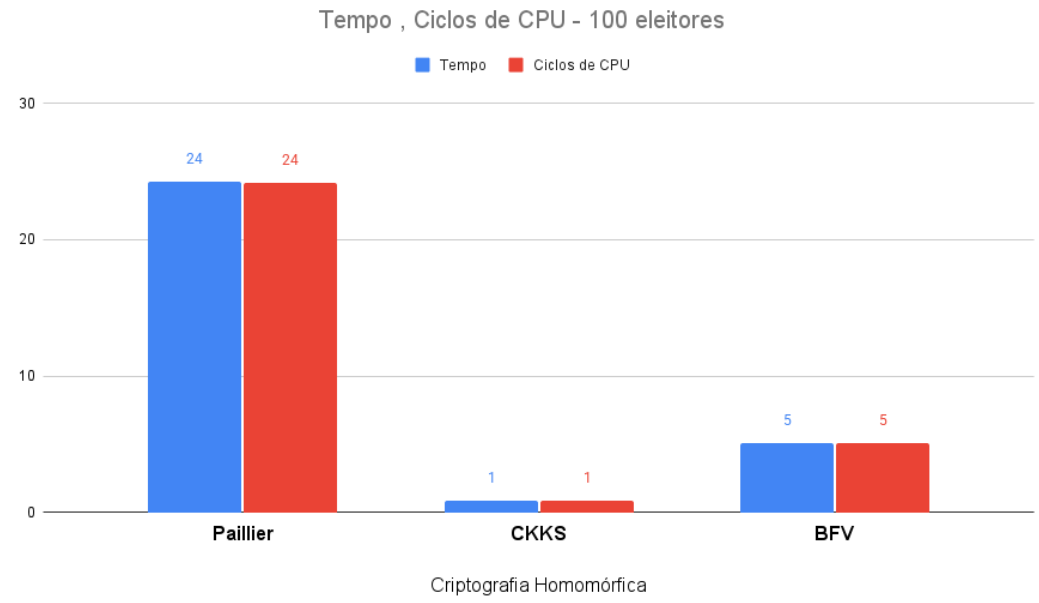

Figura 15 – Tempo de processamento e ciclos de CPU para 100 eleitores para algoritmos homomórficos

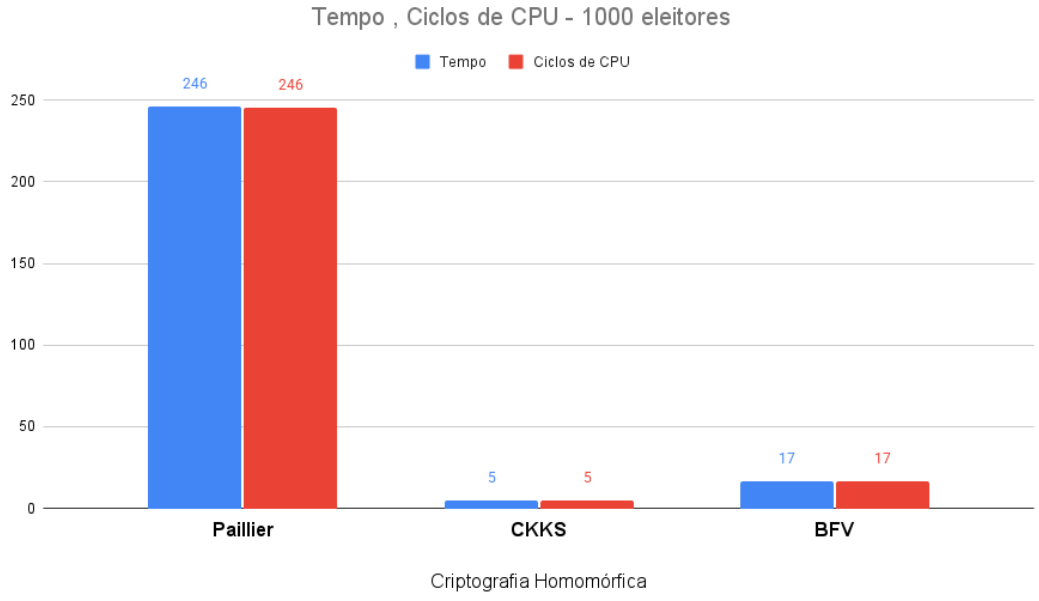

Figura 16 – Tempo de processamento e ciclos de CPU para 1.000 eleitores para algoritmos homomórficos

demonstrou-se consideravelmente mais eficiente do que os demais algoritmos, destacando sua capacidade de processamento para grandes volumes de dados.

No segundo experimento, o número de eleitores foi mantido constante em 1.000, enquanto o número de candidatos variou entre 3, 6 e 10. As Figuras 18, 19 e 20 apresentam as médias do tempo de processamento e dos ciclos de CPU obtidas nas simulações de cada algoritmo.

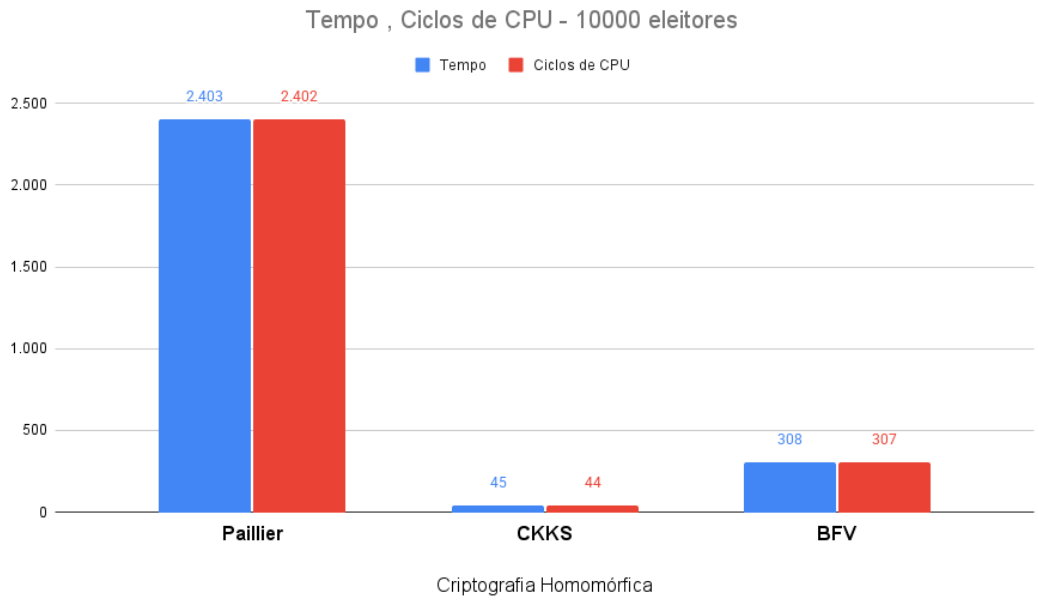

Figura 17 – Tempo de processamento e ciclos de CPU para 10.000 eleitores para algoritmos homomórficos

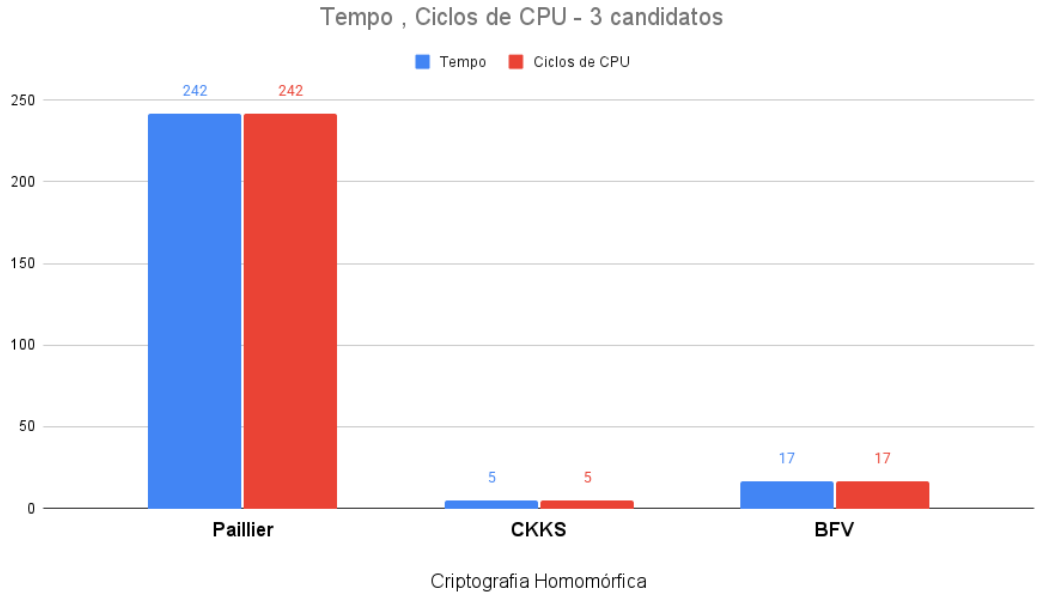

Figura 18 – Tempo de processamento e ciclos de CPU para 3 candidatos para algoritmos homomórficos

Manter o número de eleitores constante em 1.000 e variar o número de candidatos resultou em apenas pequenas variações no tempo de processamento e nos ciclos de CPU. A partir dos experimentos iniciais, observou-se que o desempenho no cenário de votação proposto neste estudo apresenta uma variação mais expressiva à medida que o número de eleitores aumenta. Assim, para as simulações subsequentes, optou-se por fixar o número de candidatos em 5, enquanto o número de eleitores será variável, a fim de explorar seu

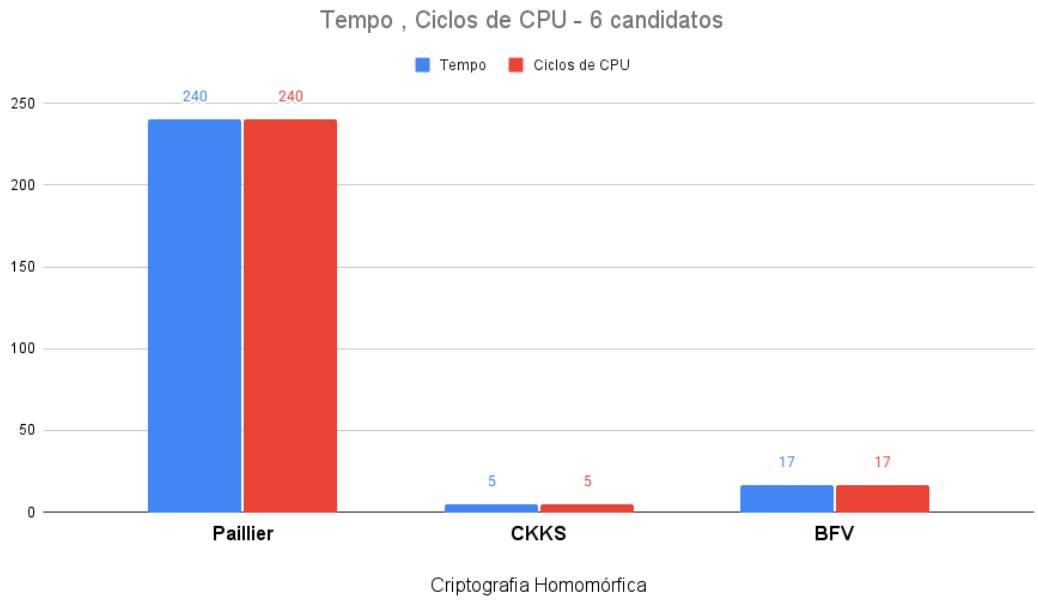

Figura 19 – Tempo de processamento e ciclos de CPU para 6 candidatos para algoritmos homomórficos

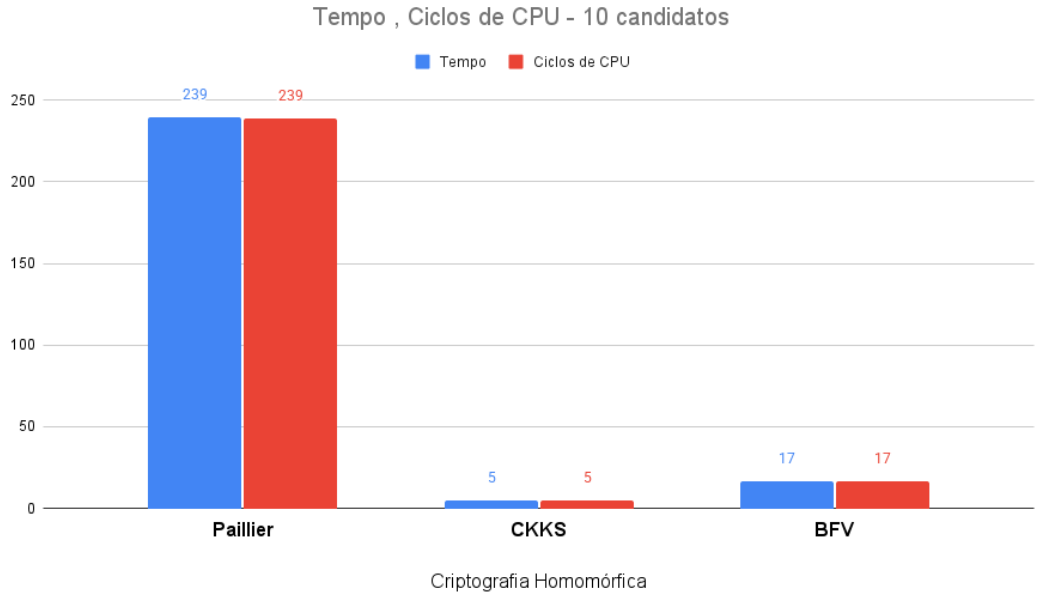

Figura 20 – Tempo de processamento e ciclos de CPU para 10 candidatos para algoritmos homomórficos

impacto no desempenho dos algoritmos criptográficos.

A principal limitação para o aumento do número de candidatos está no modelo de representação do voto, uma vez que, quanto maior o número de candidatos, maior será a quantidade de algarismos necessários para representar as possibilidades de escolha do voto. Em simulações com mais de 10 candidatos, os algoritmos CKKS e BFV não apresentaram resultados corretos devido a um erro de *overflow* na soma homomórfica de

números grandes, sendo necessários mais estudos para aprimorar o modelo da cédula de votação para um número maior de candidatos.

De maneira geral, os algoritmos homomórficos pós-quânticos avaliados na simulação apresentaram desempenho superior em comparação com o algoritmo clássico.

Em termos de desempenho computacional, foi observado que o algoritmo CKKS obteve os melhores resultados. Esse desempenho superior pode ser atribuído à sua capacidade de processar grandes volumes de dados, proporcionando tempos de resposta significativamente reduzidos. A eficiência do CKKS resulta de sua habilidade de realizar operações diretamente em números de ponto flutuante, o que o torna particularmente adequado para cenários que demandam cálculos complexos, como é o caso da contagem de votos em sistemas eleitorais (62). Com base nos resultados obtidos, o CKKS foi selecionado como o algoritmo principal para a realização da soma homomórfica no cenário proposto, sendo empregado nas simulações subsequentes.

O comportamento identificado nas simulações dos algoritmos homomórficos evidencia que, embora o impacto do número de candidatos seja marginal, o crescimento no número de eleitores impõe uma carga significativa no desempenho. Esse fator indica que, para garantir escalabilidade e eficiência, é essencial considerar adaptações e aprimoramentos no cenário proposto, como a adoção de algoritmos mais modernos e otimizados para lidar com a soma homomórfica em contextos com mais de 10.000 eleitores.

5.3 Função Hash

Após a verificação da viabilidade da soma homomórfica, foi incorporada uma função de hash para garantir a integridade dos dados de voto. Para isso, um hash foi gerado para cada voto criptografado e verificado antes de ser somado, assegurando a integridade do voto. Os algoritmos SHA-2, SHA-3 e BLAKE2 foram avaliados nesta simulação. Nessa simulação, o número de candidatos foi fixado em 5, e o número de eleitores foi testado nos valores de 100, 1.000 e 10.000.

Foram realizadas 10 simulações com cada algoritmo e as Figuras 21, 22, 23 apresenta a média dos resultados.

Nas simulações utilizando a função hash, os algoritmos apresentaram um desempenho próximo, sendo o SHA-2 o mais eficiente. Esse comportamento deve-se ao fato de que os algoritmos SHA-2 e BLAKE2 apresentaram desempenho superior ao SHA-3, que tem como foco principal a segurança em aplicações que requerem uma proteção mais robusta (50).

Além disso, conforme descrito em (78), a função SHA-2 não possui segurança pós-quântica, e não foram observados estudos relevantes sobre a segurança pós-quântica

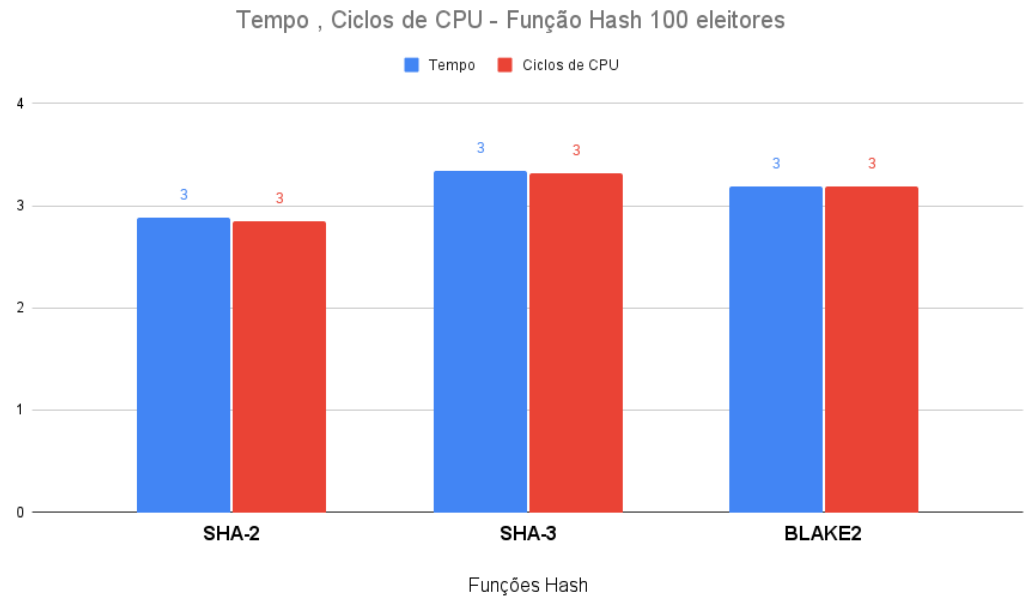

Figura 21 – Tempo de processamento e ciclos de CPU com 100 eleitores para funções hash

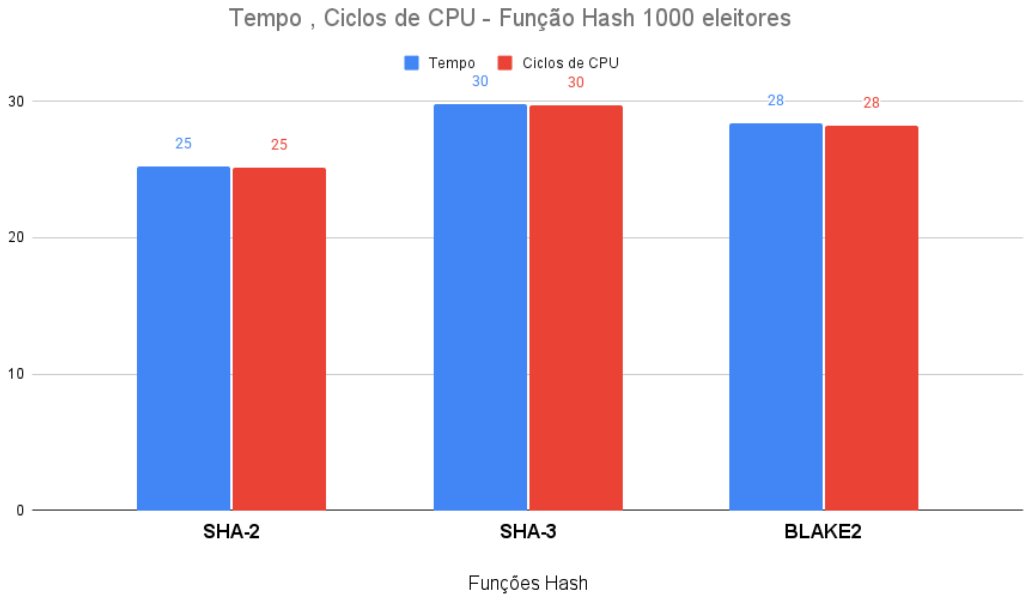

Figura 22 – Tempo de processamento e ciclos de CPU com 1.000 eleitores para funções hash

do algoritmo BLAKE2.

Dessa forma, levando em conta o desempenho próximo dos algoritmos e a recomendação do NIST para o SHA-3 como algoritmo de hash padrão para aplicações pós-quânticas (49), a função de hash escolhida para o cenário proposto foi a SHA-3.

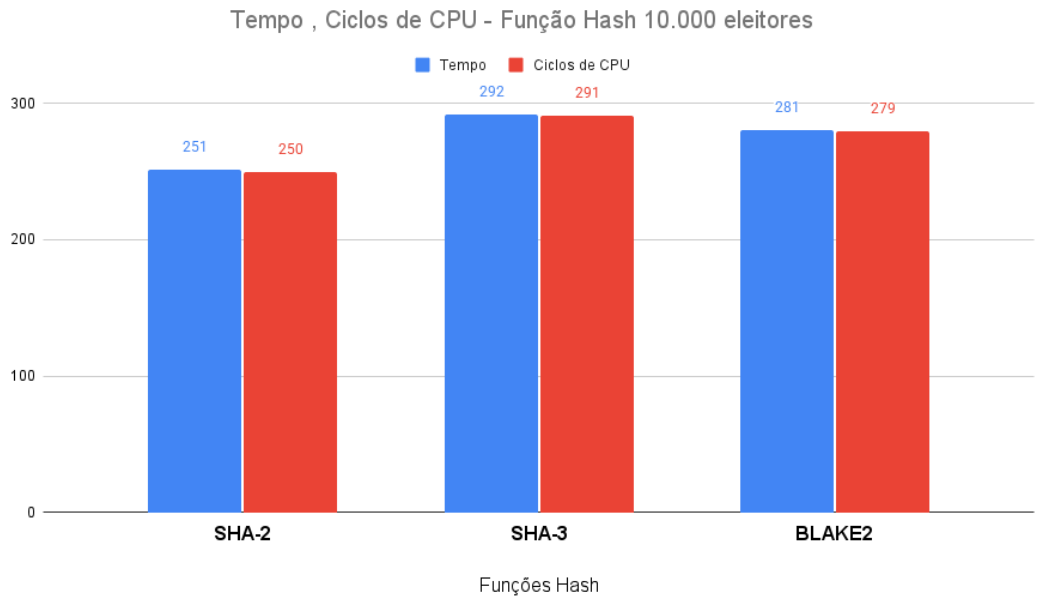

Figura 23 – Tempo de processamento e ciclos de CPU com 10.000 eleitores para funções hash

5.4 Assinatura Digital

Nas simulações para assinatura digital, inicialmente foram gerados os pares de chaves para os eleitores. Cada eleitor utilizou sua chave privada para assinar seu voto, garantindo sua autenticidade e o não repúdio. Para essa simulação, cada voto criptografado foi assinado e verificado antes de ser somado, assegurando sua validade. O número de candidatos foi fixado em 5, e o número de eleitores variou entre 100, 1.000 e 10.000. Os algoritmos CRYSTALS-Dilithium, ECDSA e SPHINCS+ foram avaliados nessa simulação.

Conforme observado nas Figuras 24, 25 e 26, o algoritmo ECDSA apresentou o melhor desempenho, seguido pelo CRYSTALS-Dilithium e pelo SPHINCS+. No entanto, como discutido em seções anteriores, o ECDSA não possui proteção pós-quântica e, portanto, foi descartado da configuração final. Para garantir o melhor desempenho no cenário proposto, o CRYSTALS-Dilithium foi escolhido devido à sua alta eficiência e robustez contra ataques de computadores quânticos.

Cabe destacar também que tanto o CRYSTALS-Dilithium quanto o SPHINCS+ foram escolhidos pelo NIST como padrão de assinatura digital pós-quântica para futuras implementações (40).

5.5 Configuração completa

Ao final de todas as avaliações de desempenho dos algoritmos, foram realizadas simulações utilizando as funções criptográficas implementadas com os algoritmos CKKS,

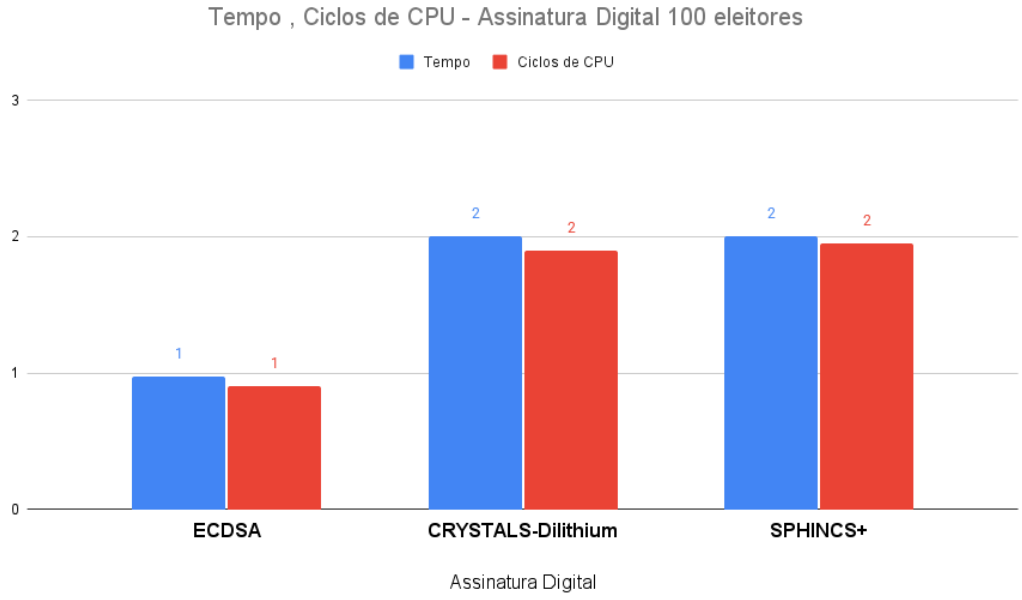

Figura 24 – Tempo de processamento e ciclos de CPU com 100 eleitores para assinatura digital

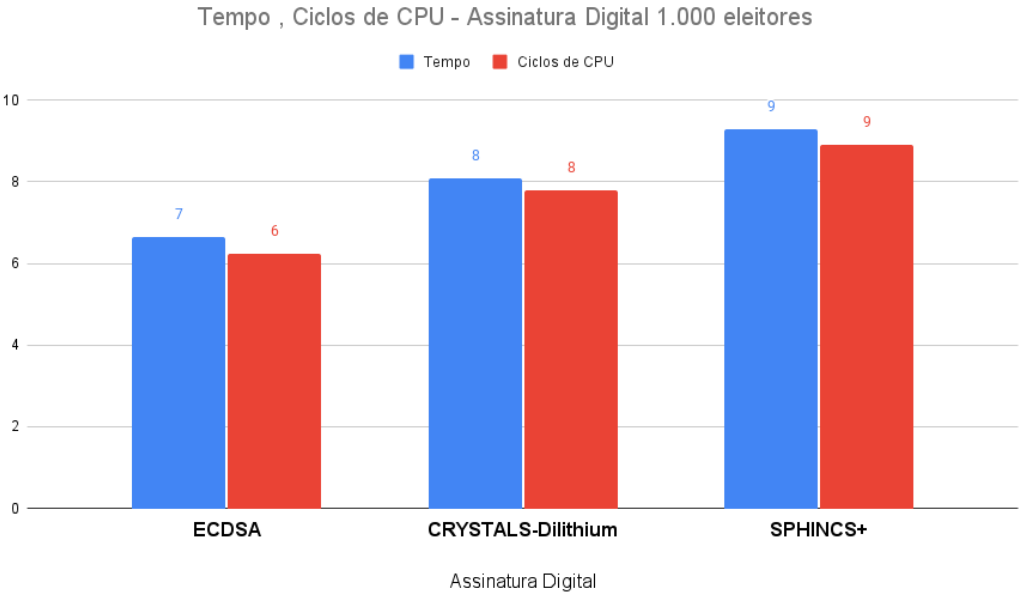

Figura 25 – Tempo de processamento e ciclos de CPU com 1.000 eleitores para assinatura digital

SHA-3 e CRYSTALS-Dilithium. Nessas simulações, o número de eleitores variou entre 100, 1.000 e 10.000, enquanto o número de candidatos foi fixado em 5. A Figura 27 apresenta a média de 10 simulações para cada cenário.

Nas simulações avaliadas, observou-se uma variação linear nos parâmetros analisados à medida que o número de eleitores era multiplicado por 10. Para o número máximo de eleitores considerado na simulação, ou seja, 10.000, os algoritmos criptográficos pós-

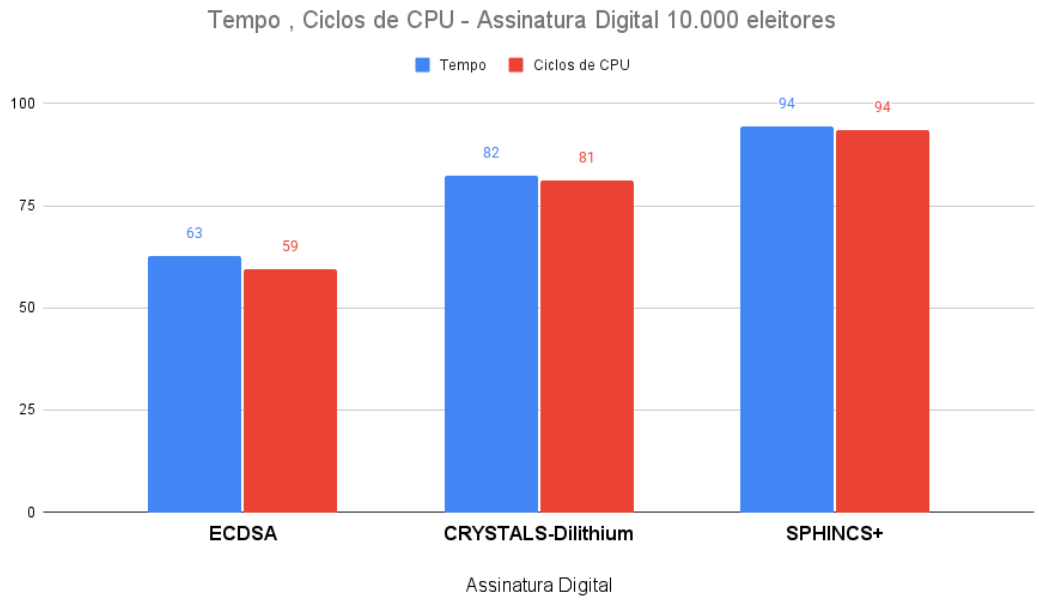

Figura 26 – Tempo de processamento e ciclos de CPU com 10.000 eleitores para assinatura digital

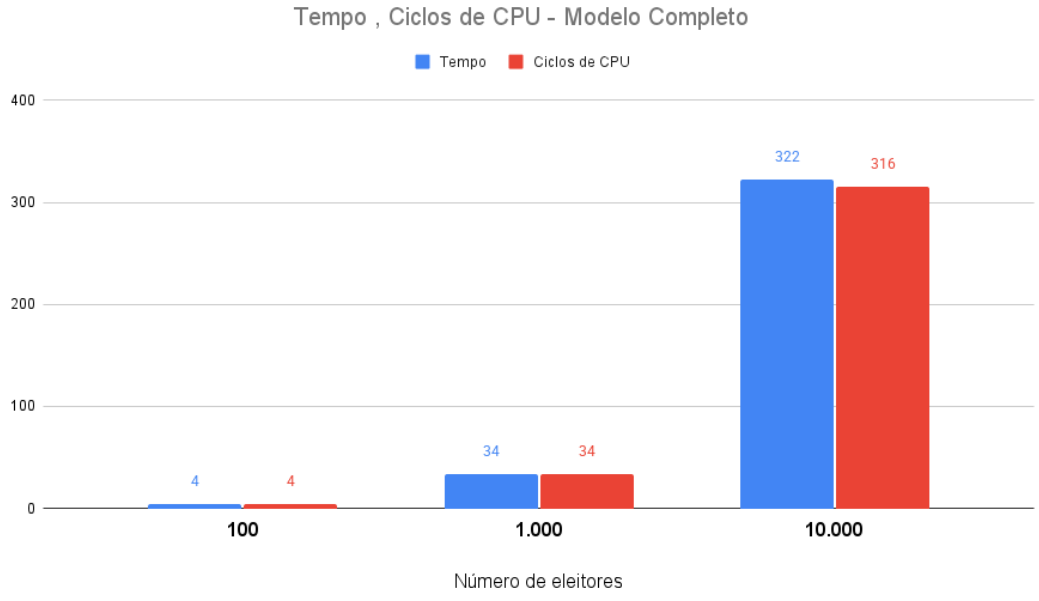

Figura 27 – Tempo de processamento e ciclos de CPU para configuração completa

quânticos demonstraram desempenho satisfatório, considerando que as simulações foram realizadas em um computador pessoal comum. Esse desempenho melhoraria caso fossem utilizados servidores com maior poder de processamento, o que permitiria reduzir o tempo de execução.

Apesar dos desafios enfrentados caso a contagem ultrapasse 10.000 votos, uma possibilidade para acelerar o processo seria dividir a contagem em zonas eleitorais, com cada uma sendo responsável pela sua própria contagem, tornando esta configuração viável

para eleições em grande escala, dependendo da configuração adotada.

De maneira geral, as simulações realizadas demonstraram que o cenário proposto pode ser aplicado em situações reais, com ajustes pontuais. A configuração final atende aos principais requisitos de segurança, incluindo integridade, confidencialidade, anonimato e autenticidade, além de garantir resistência a ataques de computadores quânticos por meio do emprego de algoritmos criptográficos pós-quânticos que asseguram esses requisitos.

Com base nos resultados obtidos, pode-se concluir que a otimização dos algoritmos criptográficos empregados é um fator essencial para a viabilidade das aplicações práticas. Esta necessidade se torna ainda mais evidente em cenários de votação eletrônica, nos quais o desempenho e a eficiência impactam diretamente a escalabilidade do sistema, assim como a experiência dos usuários. Nesse contexto, é imprescindível garantir um equilíbrio entre segurança e eficiência computacional, de modo a viabilizar a adoção da criptografia pós-quântica em sistemas eleitorais de larga escala, sem comprometer a segurança e a confiabilidade do processo eleitoral.

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

O cenário de votação online apresentado neste trabalho demonstrou ser eficaz nas simulações dos algoritmos criptográficos empregados, garantindo os requisitos essenciais de segurança propostos. A avaliação do desempenho das diferentes soluções criptográficas, incluindo algoritmos pós-quânticos, evidenciou sua viabilidade e eficiência na implementação de sistemas eleitorais seguros.

Durante as simulações, os algoritmos pós-quânticos, como o CRYSTALS-Dilithium, CKKS e SHA-3, mostraram-se robustos e eficientes para o ambiente de votação online, sendo capazes de resistir aos potenciais ataques de computadores quânticos. Esses algoritmos não apenas garantiram a segurança dos dados eleitorais, mas também se destacaram em termos de desempenho, com tempos de processamento e consumo de recursos adequados para a escalabilidade. Assim, são considerados alternativas viáveis para serem empregados em eleições de grande porte, dependendo do cenário analisado.

Apesar dos resultados satisfatórios nos cenários simulados, faz-se necessário um estudo aprofundado para a otimização de algoritmos e criptografia pós-quântica aplicados à votação eletrônica, à medida que a quantidade de dados aumenta.

Portanto, os resultados obtidos demonstram que os algoritmos criptográficos pós-quânticos empregados não apenas atendem aos requisitos de segurança exigidos para processos eleitorais, mas também oferecem uma solução viável para enfrentar as ameaças futuras, especialmente no contexto da computação quântica. O desenvolvimento de criptografia pós-quântica se mostra essencial para garantir a robustez e a confiança no sistema de votação, reafirmando sua aplicabilidade em um futuro em que a computação quântica será uma realidade.

6.1 Trabalhos Futuros

Diversas possibilidades de aprimoramento do cenário de votação online proposto podem ser exploradas em trabalhos futuros. Um dos aspectos fundamentais a ser melhorado é a estrutura da cédula de votação, de modo a permitir a inclusão de um número maior de candidatos, atendendo a uma gama mais ampla de configurações eleitorais. A expansão dessa funcionalidade pode tornar o modelo mais flexível e aplicável a diferentes contextos eleitorais.

Outra linha de pesquisa relevante é a investigação de outros algoritmos pós-quânticos, além dos já utilizados, para avaliar seu desempenho e segurança em sistemas de votação. Testar diferentes algoritmos pode oferecer novas perspectivas sobre como otimizar

a segurança e a eficiência dos sistemas de votação eletrônica, garantindo maior resistência contra ataques futuros. A verificação das possibilidades de otimização dos algoritmos selecionados também é crucial, especialmente em termos de tempo de processamento e consumo de recursos, a fim de garantir que o sistema permaneça escalável para eleições de grande porte.

Além disso, a implementação de técnicas de prova de conhecimento zero pode ser explorada para garantir o requisito de segurança de verificabilidade. Essas técnicas permitem que uma parte prove à outra que possui certas informações sem revelar o conteúdo dessas informações, o que é especialmente valioso em cenários de votação, onde a privacidade dos eleitores deve ser preservada. Em um cenário de votação eletrônica em larga escala, onde existem ameaças computacionais, como os ataques quânticos, o uso de provas de conhecimento zero se destaca como uma abordagem promissora para melhorar a segurança, sem comprometer a privacidade e a integridade do processo eleitoral.

Por fim, uma linha de pesquisa futura envolve o desenvolvimento de um software que integre o cenário proposto e os algoritmos empregados, viabilizando sua implementação prática em cenários reais, além de permitir a incorporação de outros algoritmos criptográficos. Este software deverá ser projetado para atender de maneira eficaz aos requisitos essenciais de segurança, escalabilidade e usabilidade, com o objetivo de possibilitar sua adoção em processos eleitorais de grande porte.

REFERÊNCIAS

1 MAGKOS, E.; KOTZANIKOLAOU, P.; DOULIGERIS, C. Towards secure online elections: models, primitives and open issues. *Electronic Government*, v. 4, n. 3, p. 249–268, 2007.

2 CRAMER, R.; GENNARO, R.; SCHOENMAKERS, B. A secure and optimally efficient multi-authority election scheme. *European transactions on Telecommunications*, Wiley Online Library, v. 8, n. 5, p. 481–490, 1997.

3 ASIF, R. Post-quantum cryptosystems for internet-of-things: a survey on lattice-based algorithms. *IoT*, MDPI, v. 2, n. 1, p. 71–91, 2021.

4 KHO, Y.-X.; HENG, S.-H.; CHIN, J.-J. A review of cryptographic electronic voting. *Symmetry*, Multidisciplinary Digital Publishing Institute, v. 14, n. 5, p. 858, 2022.

5 AVGEROU, C.; GANZAROLI, A.; POULYMENAKOU, A.; REINHARD, N. Interpreting the trustworthiness of government mediated by information and communication technology: Lessons from electronic voting in brazil. *Information technology for development*, Taylor & Francis, v. 15, n. 2, p. 133–148, 2009.

6 HEIBERG, S.; LAUD, P.; WILLEMSON, J. The application of i-voting for estonian parliamentary elections of 2011. In: SPRINGER. *International Conference on E-Voting and Identity*. [S.l.], 2011. p. 208–223.

7 GERLACH, J.; GASSER, U. Three case studies from switzerland: E-voting. *Berkman Center Research Publication No*, v. 3, n. 2009, p. 2020–2021, 2009.

8 STANDARD, O. Election markup language (eml) version 5.0 process and data requirements. 2007.

9 MOAYED, M. J.; GHANI, A. A. A.; MAHMOD, R. A survey on cryptography algorithms in security of voting system approaches. In: IEEE. *2008 International Conference on Computational Sciences and its Applications*. [S.l.], 2008. p. 190–200.

10 KRIMMER, R.; VOLKAMER, M.; DUENAS-CID, D. E-voting–an overview of the development in the past 15 years and current discussions. In: SPRINGER. *International Joint Conference on Electronic Voting*. [S.l.], 2019. p. 1–13.

11 KAIM, G.; CANARD, S.; ROUX-LANGLOIS, A.; TRAORÉ, J. Post-quantum online voting scheme. In: SPRINGER. *International Conference on Financial Cryptography and Data Security*. [S.l.], 2021. p. 290–305.

12 LIAO, G. Multi-candidate electronic voting scheme based on fully homomorphic encryption. In: IOP PUBLISHING. *Journal of Physics: Conference Series*. [S.l.], 2020. v. 1678, n. 1, p. 012064.

13 CHILLOTTI, I.; GAMA, N.; GEORGIEVA, M.; IZABACHÈNE, M. A homomorphic lwe based e-voting scheme. In: SPRINGER. *Post-Quantum Cryptography*. [S.l.], 2016. p. 245–265.

14 AZIZ, A.; QUNOO, H.; SAMRA, A. Using homomorphic cryptographic solutions on e-voting systems [pdf file]. 2018.

15 GAO, S.; ZHENG, D.; GUO, R.; JING, C.; HU, C. An anti-quantum e-voting protocol in blockchain with audit function. *IEEE Access*, IEEE, v. 7, p. 115304–115316, 2019.

16 FARZALIYEV, V.; WILLEMSON, J.; KAASIK, J. K. Improved lattice-based mix-nets for electronic voting. *Cryptology ePrint Archive*, 2021.

17 MAHTO, D.; YADAV, D. K. Rsa and ecc: A comparative analysis. *International journal of applied engineering research*, v. 12, n. 19, p. 9053–9061, 2017.

18 SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, SIAM, v. 41, n. 2, p. 303–332, 1999.

19 ZHU, H.; TAN, Y.-a.; ZHU, L.; WANG, X.; ZHANG, Q.; LI, Y. An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks. *Sensors*, MDPI, v. 18, n. 5, p. 1663, 2018.

20 HASSIJA, V.; CHAMOLA, V.; SAXENA, V.; CHANANA, V.; PARASHARI, P.; MUMTAZ, S.; GUIZANI, M. Present landscape of quantum computing. *IET Quantum Communication*, Wiley Online Library, v. 1, n. 2, p. 42–48, 2020.

21 ALAGIC, G.; APON, D.; COOPER, D.; DANG, Q.; DANG, T.; KELSEY, J.; LICHTINGER, J.; MILLER, C.; MOODY, D.; PERALTA, R. et al. Status report on the third round of the nist post-quantum cryptography standardization process. *National Institute of Standards and Technology, Gaithersburg*, 2022.

22 BLANCO, D. Y. Marcos del; ALONSO, L. P.; ALONSO, J. A. H. Review of cryptographic schemes applied to remote electronic voting systems: remaining challenges and the upcoming post-quantum paradigm. *Open Mathematics*, De Gruyter, v. 16, n. 1, p. 95–112, 2018.

23 LI, H.; KANKANALA, A. R.; ZOU, X. A taxonomy and comparison of remote voting schemes. In: IEEE. *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*. [S.l.], 2014. p. 1–8.

24 LIAW, H.-T. A secure electronic voting protocol for general elections. *Computers & Security*, Elsevier, v. 23, n. 2, p. 107–119, 2004.

25 CHAUM, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, ACM New York, NY, USA, v. 24, n. 2, p. 84–90, 1981.

26 BENALOH, J. D. C. *Verifiable secret-ballot elections*. [S.l.]: Yale University, 1987.

27 CHEN, A. C. Homomorphic encryption based on post-quantum cryptography. In: IEEE. *2023 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*. [S.l.], 2023. p. 1–5.

28 GENTRY, C. Fully homomorphic encryption using ideal lattices. In: *Proceedings of the forty-first annual ACM symposium on Theory of computing*. [S.l.: s.n.], 2009. p. 169–178.

29 CHAUM, D. Blind signatures for untraceable payments. In: SPRINGER. *Advances in Cryptology: Proceedings of Crypto 82*. [S.l.], 1983. p. 199–203.

30 HARDWICK, F. S.; GIOULIS, A.; AKRAM, R. N.; MARKANTONAKIS, K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In: IEEE. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. [S.l.], 2018. p. 1561–1567.

31 BERENJESTANAKI, M. H.; BARZEGAR, H. R.; IOINI, N. E.; PAHL, C. Blockchain-based e-voting systems: a technology review. *Electronics*, MDPI, v. 13, n. 1, p. 17, 2023.

32 ZHENG, Z.; XIE, S.; DAI, H.-N.; CHEN, X.; WANG, H. Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, Inderscience Publishers (IEL), v. 14, n. 4, p. 352–375, 2018.

33 LIU, Y.; WANG, Q. An e-voting protocol based on blockchain. *Cryptology ePrint Archive*, 2017.

34 JAFAR, U.; AZIZ, M. J. A. A state of the art survey and research directions on blockchain based electronic voting system. In: SPRINGER. *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*. [S.l.], 2021. p. 248–266.

35 KIAYIAS, A.; YUNG, M. The vector-ballot e-voting approach. In: SPRINGER. *International Conference on Financial Cryptography*. [S.l.], 2004. p. 72–89.

36 HUSSIEN, H.; ABOELNAGA, H. Design of a secured e-voting system. In: IEEE. *2013 International Conference on Computer Applications Technology (ICCAT)*. [S.l.], 2013. p. 1–5.

37 SRIVASTAVA, V.; BAKSI, A.; DEBNATH, S. K. An overview of hash based signatures. *Cryptology ePrint Archive*, 2023.

38 BALDI, M.; CHIARALUCE, F. Cryptanalysis of a new instance of mceliece cryptosystem based on qc-ldpc codes. In: IEEE. *2007 IEEE International Symposium on Information Theory*. [S.l.], 2007. p. 2591–2595.

39 National Institute of Standards and Technology. *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)*. [S.l.], 2024. Disponível em: <https://doi.org/10.6028/NIST.FIPS.203>.

40 National Institute of Standards and Technology. *FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA)*. [S.l.], 2024. Disponível em: <https://doi.org/10.6028/NIST.FIPS.204>.

41 REGEV, O. Lattice-based cryptography. In: SPRINGER. *Annual International Cryptology Conference*. [S.l.], 2006. p. 131–141.

42 AJTAI, M. Generating hard instances of lattice problems. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. [S.l.: s.n.], 1996. p. 99–108.

43 MICCIANCIO, D.; REGEV, O. Lattice-based cryptography. *Post-quantum cryptography*, Springer, p. 147–191, 2009.

44 REGEV, O. The learning with errors problem. *Invited survey in CCC*, Citeseer, v. 7, n. 30, p. 11, 2010.

45 CORON, J.-S.; DODIS, Y.; MALINAUD, C.; PUNIYA, P. Merkle-damgård revisited: How to construct a hash function. In: SPRINGER. *Annual International Cryptology Conference*. [S.l.], 2005. p. 430–448.

46 STANDARDS, N. I. of; TECHNOLOGY. *Secure Hash Standard (SHA-2)*. 2002. FIPS Publication 180-4. Acesso em: 5 mar. 2025. Disponível em: <https://doi.org/10.6028/NIST.FIPS.180-4>.

47 MERKLE, R. C.; DAMGÅRD, I. A design principle for hash functions. In: SPRINGER-VERLAG. *Advances in Cryptology – CRYPTO '89 Proceedings*. New York, NY, 1989. p. 262–277.

48 LEIGHTON, T.; CHEN, G. Sha-2: The standard for cryptographic hash functions. *Security and Privacy Journal*, v. 1, n. 1, p. 1–5, 2007. Discusses the transition from SHA-1 to SHA-2 due to vulnerabilities such as collision resistance.

49 STANDARDS, N. I. of; TECHNOLOGY. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. 2015. FIPS PUB 202. Disponível em: <https://doi.org/10.6028/NIST.FIPS.202>.

50 KELSEY, J. Sha-3: What it is and why it matters. *Communications of the ACM*, v. 59, n. 8, p. 36–37, 2016. Artigo que compara SHA-3 e SHA-2, destacando os casos de uso de cada um. Disponível em: <https://doi.org/10.1145/2934664>.

51 AUMASSON, J.-P.; NEVES, L.; OSVIK, D.; ROGAWAY, P. Blake2: High-speed cryptographic hash function. *IACR Cryptology ePrint Archive*, v. 2013, p. 458, 2013. Acesso em: 5 mar. 2025. Disponível em: <https://eprint.iacr.org/2013/458>.

52 BIRYUKOV, A.; DINU, D.; KHOVRATOVICH, D. *Argon2: The Memory-Hard Function for Password Hashing and Other Applications*. 2015. Documentação do Argon2, que utiliza o BLAKE2 para proteção de senhas. Disponível em: <https://password-hashing.net/>.

53 ZYCH, M. D. *Quantum Safe Cryptography Based on Hash Functions: A Survey*. Dissertação (Mestrado), 2018.

54 SCHNEIER, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. [S.l.]: John Wiley & Sons, 1996.

55 MERCURI, R. Electronic vote tabulation: Checks and balances. In: ACM. *Proceedings of the 2002 ACM conference on Computer supported cooperative work*. [S.l.], 2002. p. 16–20.

56 DUCAS, L.; KILTZ, E.; LEPOINT, T.; LYUBASHEVSKY, V.; SCHWABE, P.; SEILER, G.; STEHLÉ, D. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, p. 238–268, 2018.

57 SHEN, Z.; WEI, J. Dilithium: Efficient and secure signatures from module-lwe. *Cryptology ePrint Archive*, 2019. Acesso em: 2025-02-12. Disponível em: <https://eprint.iacr.org/2019/1453>.

58 BERNSTEIN, D. J.; LANGE, T.; PETERS, C. Elliptic curve cryptography. In: *Lecture Notes in Computer Science*. [S.l.]: Springer, 2009. v. 4867, p. 1–25.

59 BERNSTEIN, D. J.; LANGE, T. Post-quantum cryptography. *Nature*, Nature Publishing Group, v. 549, n. 7671, p. 188–194, 2017.

60 STANDARDS, N. I. of; TECHNOLOGY. *FIPS 205: Post-Quantum Cryptographic Algorithms*. 2025. Disponível em: <https://www.nist.gov/publications/fips-205-post-quantum-cryptographic-algorithms>.

61 PAILLIER, P. Public-key cryptosystems based on composite degree residuosity classes. In: *Advances in Cryptology — EUROCRYPT 1999*. Springer, 1999. p. 223–238. Disponível em: <https://link.springer.com/chapter/10.1007/3-540-48910-X_15>.

62 CHEON, J. H.; COSTACHE, A.; MORENO, R. C.; DAI, W.; GAMA, N.; GEORGIEVA, M.; HALEVI, S.; KIM, M.; KIM, S.; LAINE, K. et al. Introduction to homomorphic encryption and schemes. *Protecting Privacy through Homomorphic Encryption*, Springer, p. 3–28, 2021.

63 KIM, A.; PAPADIMITRIOU, A.; POLYAKOV, Y. Approximate homomorphic encryption with reduced approximation error. In: SPRINGER. *Cryptographers' Track at the RSA Conference*. [S.l.], 2022. p. 120–144.

64 BRAKERSKI, Z. Fully homomorphic encryption without modulus switching from classical gapsvp. In: SPRINGER. *Annual cryptology conference*. [S.l.], 2012. p. 868–886.

65 BRAKERSKI, Z.; VAIKUNTANATHAN, S. Fully homomorphic encryption from ring-lwe and security for key dependent messages. *SIAM Journal on Computing*, SIAM, v. 43, n. 6, p. 1897–1944, 2014.

66 DONG, H.; YANG, L. A voting scheme with post-quantum security based on physical laws. *arXiv preprint arXiv:1805.12480*, 2018.

67 GABRIEL, A. J.; ALESE, B. K.; ADETUNMBI, A. O.; ADEWALE, O. S.; SARUMI, O. A. Post-quantum crystography system for secure electronic voting. *Open Computer Science*, De Gruyter Open Access, v. 9, n. 1, p. 292–298, 2019.

68 FUJIOKA, A.; OKAMOTO, T.; OHTA, K. A practical secret voting scheme for large scale elections. In: SPRINGER. *International Workshop on the Theory and Application of Cryptographic Techniques*. [S.l.], 1992. p. 244–251.

69 KARAYUMAK, F.; OLEMBO, M. M.; KAUER, M.; VOLKAMER, M. Usability analysis of helios—an open source verifiable remote electronic voting system. In: *2011 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 11)*. [S.l.: s.n.], 2011.

70 HALEVI, S.; SHOUP, V. Design and implementation of helib: a homomorphic encryption library. *Cryptology ePrint Archive*, 2020.

71 BLUM, M.; FELDMAN, P.; MICALI, S. Non-interactive zero-knowledge and its applications. In: *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. [S.l.: s.n.], 2019. p. 329–349.

72 YANG, R.; AU, M. H.; ZHANG, Z.; XU, Q.; YU, Z.; WHYTE, W. Efficient lattice-based zero-knowledge arguments with standard soundness: construction and applications. In: SPRINGER. *Annual International Cryptology Conference*. [S.l.], 2019. p. 147–175.

73 PINILLA, R. M. *Fully post-quantum protocols for e-voting, coercion resistant cast as intended and mixing networks*. Dissertação (Mestrado) — Universitat Politècnica de Catalunya, 2018.

74 JUELS, A.; CATALANO, D.; JAKOBSSON, M. Coercion-resistant electronic elections. In: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. [S.l.: s.n.], 2005. p. 61–70.

75 RØNNE, P. B.; ATASHPENDAR, A.; GJØSTEEN, K.; RYAN, P. Y. Coercion-resistant voting in linear time via fully homomorphic encryption.

76 BOYEN, X.; HAINES, T.; MÜLLER, J. A verifiable and practical lattice-based decryption mix net with external auditing. In: SPRINGER. *European Symposium on Research in Computer Security*. [S.l.], 2020. p. 336–356.

77 KILTZ, E.; MALONE-LEE, J. A general construction of ind-cca2 secure public key encryption. In: SPRINGER. *IMA International Conference on Cryptography and Coding*. [S.l.], 2003. p. 152–166.

78 AKINORI, H. Security of hash functions against attacks using quantum computers. *NTT Technical Review*, NTT , v. 21, n. 7, p. 43–47, 2023.