Pós-Graduação em Ciência da Computação

“Proposta de um Modelo para Verificabilidade E2E no Sistema Eletrônico de Votação Brasileiro Utilizando Mecanismos de Criptografia Visual”

Por

Gleudson Pinheiro Varejão Junior

Dissertação de Mestrado

Universidade Federal de Pernambuco

posgraduacao@cin.ufpe.br

www.cin.ufpe.br/~posgraduacao

RECIFE, 2014

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Gleudson Pinheiro Varejão Junior

"Proposta de um Modelo para Verificabilidade E2E no Sistema Eletrônico de Votação Brasileiro Utilizando Mecanismos de Criptografia Visual"

Este trabalho foi apresentado a Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de mestre em Ciência da Computação.

Orientador: Prof. Dr. Ruy José G. B. De Queiroz

RECIFE, 2014

Catalogação na fonte
Bibliotecária Jane Souto Maior, CRB4-571

V292p Varejão Junior, Gleudson Pinheiro
Proposta de um modelo para verificabilidade E2E no sistema eletrônico de votação brasileiro utilizando mecanismos de criptografia visual /Gleudson Pinheiro Varejão Junior. – Recife: O Autor, 2014.
130 f.: il., fig., quadro.

Orientador: Ruy José Guerra Barretto de Queiroz.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn. Ciência da Computação, 2014.
Inclui referências.

1. Ciência da computação. 2. Segurança da informação. 3. Criptografia. 4. Sistemas eleitorais. I. Queiroz, Ruy José Guerra Barretto de (orientador). II. Título.

004 CDD (23. ed.) UFPE- MEI 2014-167

Dissertação de Mestrado apresentada por **Gleudson Pinheiro Varejão Junior** à Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco, sob o título "**Proposta de um Modelo para Verificabilidade E2E no Sistema Eletrônico de Votação Brasileiro Utilizando Mecanismos de Criptografia Visual**" orientada pelo **Prof. Ruy José Guerra Barretto de Queiroz** e aprovada pela Banca Examinadora formada pelos professores:

_____

Prof. Carlos Alexandre Barros de Mello
Centro de Informática/UFPE

_____

Prof. Roberto Samarone dos Santos Araújo
Instituto de Ciências Exatas e Naturais/ UFPA

_____

Prof. Ruy José Guerra Barretto de Queiroz
Centro de Informática /UFPE

Visto e permitida a impressão.
Recife, 21 de agosto de 2014.

_____

Profa. Edna Natividade da Silva Barros
Coordenadora da Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco.

Primeiro a Deus por todas as coisas. Aos meus pais, Gleudson e Maria Isabel. Aos meus filhos, esposa e especialmente em memória da minha querida irmã, Karoline Varejão.

AGRADECIMENTOS

Agradeço a todas as pessoas que contribuíram diretamente e indiretamente com o desenvolvimento desta dissertação de mestrado, em especial ao meu orientador Prof. Dr. Ruy de Queiroz, por ter confiado a mim sua amizade e dedicado a sua experiência ao nosso projeto de pesquisa que tanto contribui com o crescimento da democracia. Desde antes de ingressar oficialmente no mestrado, quando me deu a oportunidade de assistir suas aulas como ouvinte e posteriormente a aprovação, respeitou minhas limitações de tempo e confiou no meu potencial.

Agradeço ainda a todos os professores e funcionários do Centro de Informatica da Universidade Federal de Pernambuco, que de alguma forma ajudaram nessa longa caminhada.

RESUMO

A história relata a ascensão da democracia sendo seleta a pequenos grupos de uma população, como frequentemente ocorria em algumas nações. O Brasil é um país democrático que tem participação da sociedade, que exerce seu direito democrático através dos seus representantes. No entanto, evidências descritas por Diego Aranha em (ARANHA, 2014) apontam que a maneira pela qual eles são eleitos nem sempre atinge níveis aceitáveis de segurança e confiabilidade do processo. Desde então os Sistemas Eletrônicos de Votação (SEV) vêm sendo empregados em países como Holanda, Índia, Alemanha e Brasil, tendo como principal objetivo atender aos requisitos, propriedades, regras e leis instauradas para um sistema eleitoral, primando pela conformidade de padrões e preceitos democráticos específicos de cada nação. No Brasil, o início do processo de informatização das eleições ocorreu no ano de 1996, onde então foi apresentada ao mundo a aplicabilidade de um modelo de votação 100% eletrônico, e que, segundo autoridades responsáveis pelo processo, é apontado como seguro e isento à fraude. Desde então muitas discussões surgiram a respeito da segurança do mesmo. Um dos assuntos mais pautados entre profissionais e pesquisadores de áreas afins ao sistema é a impossibilidade de se realizar um processo chamado verificabilidade “fim-a-fim” (em inglês, “end-to-end”, abreviação E2E), que visa prover mecanismos que possibilitam a verificação do voto por parte do eleitor, muito em decorrência da inexistência de um mecanismo que viabilize a materialização do voto. Levando em consideração os relatos, torna-se latente a necessidade do vínculo entre a transparência e automação de recursos, mitigando os riscos na ocorrência de fraudes e maximizando as possibilidades de auditoria e recontagem dos votos. Dessa forma, a criptografia computacional vem mostrando-se uma das principais ferramentas para atender demandas de segurança em SEV. Este trabalho visa estudar e avaliar os princípios de um SEV, bem como suas principais tecnologias e desafios de segurança. A partir do estudo realizado, é descrita a proposta de um modelo utilizando criptografia visual, a fim de prover possíveis mecanismos que atendam o requisito de verificabilidade E2E com a materialização do voto de um modo não tradicional, tendo como foco o emprego desse esquema no Sistema Eletrônico de Votação brasileiro.

Palavras chaves: Sistema Eletrônico de Votação. Criptografia. Criptografia Visual. Verificabilidade E2E.

ABSTRACT

The story chronicles the rise of democracy being select small groups of a population, as often occurred in some nations. Brazil is a democratic country with participation of society, exercising their democratic rights through their representatives. However, evidence described by Diego Spider in (ARANHA, 2014) suggests that the manner in which they are elected not always reaches acceptable levels of safety and reliability of the process. Since then the Electronic Voting Systems (SEV) has been used in countries such as the Netherlands, India, Germany and Brazil, having as main objective to meet the requirements, properties, rules and laws in place to an electoral system, striving for standards compliance and precepts democratic nation-specific. In Brazil, the beginning of the computerized election process occurred in 1996, which was then presented to the world the applicability of a model 100% electronic voting, and that officials responsible for the process, is touted as secure and free to fraud. Since then many discussions arose about the safety of it. One of the issues most guided between professionals and researchers in areas related to the system is the inability to perform a process called verifiability "end-to-end" (in English, "end-to-end", abbrev. E2E), which aims to provide mechanisms that enable the verification of voting by the voter, much due to the lack of a mechanism which facilitates the materialization of the vote. Taking into consideration the above-reported, it becomes latent the link between the need for transparency and automation of resources and mitigate risks in fraud and maximizing the chances of audit and recount. Thus, the computational encryption has proved one of the main tools to meet security demands in SEV. This work aims to study and evaluate the principles of a SEV, as well as its key technologies and security challenges. From the study, the proposed model using visual cryptography is described in order to provide possible mechanisms that meet the requirement of verifiability of E2E voting with the materialization of a non-traditional way, focusing on the use of this scheme in System Brazilian electronic Voting.

Key words: Electronic Voting System. Cryptography. Visual Cryptography. E2E Verifiability.

LISTA DE FIGURAS

LISTA DE QUADROS

ABREVIAÇÕES E ACRÔNIMOS

SEV – Sistema Eletrônico de Votação

E2E – End-to-End

UnB – Universidade de Brasília

TSE – Tribunal Superior Eleitoral

EVIV – End-to-End Verificable Internet Voting

DRE – Direct Recording Eletronic

VVPAT – Voter Verified Paper Audit Trails

IVVR – Independent Voter Veriable Record

RFID – Radio-frequency identification

VST – Voter Security Token

EVM – Electronic Voting Machines

BPS – Ballot Preparation System

CEV – Cédulas Eletrônicas do Voto

BUE – Boleta Única Eletrônica

DNI – Documento Nacional de Identificação

SSL – Secure Socket Layer

IDC – Interdisciplinay Center

TRE – Tribunal Regional Eleitoral

INPE – Instituto Nacional de Pesquisas Espaciais

CTA – Centro de Telemática de Área

IBM – International Business Machines

BU – Boletim da Urna

VPN – Virtual Private Network

MD5 – Message-Digest Algotithm

SHA – Secure Hash Algorithm

OTP – One-time Pad

XOR – Exclusive or

CRV – Cédula de Registro de Voto

CCV – Código de Confirmação do Voto

NIS – Número Identificador Singular

WBB – Web Bulletin Board

SUMÁRIO

CAPÍTULO 6

CAPÍTULO 1

"Por vezes sentimos que aquilo que fazemos não é senão uma gota de água no mar. Mas o mar seria menor se lhe faltasse uma gota."

Madre Teresa de Calcutá

Introdução

A história relata a promoção da democracia sendo seleta a pequenos grupos de uma população, como ocorreu na Grécia antiga. A sua idealização foi então ganhando extensão e sendo inserida em diversas nações ao redor do mundo. Em países considerados democráticos, opta-se geralmente pela participação indireta da população, que exerce o estado democrático a partir dos seus representantes legais. Para a seleção destes, se faz necessário a existência de um processo comum que garanta de forma justa e segura uma eleição.

Os Sistemas Eletrônicos de Votação (SEV) surgiram tendo como alicerce os avanços da área tecnológica e com o aumento massivo dos recursos computacionais. Em meio aos diversos problemas vinculados ao uso de um sistema de votação tradicional, os SEVs apresentam fundamentalmente a busca para solucionar desafios intrínsecos ao processo como: a redução do tempo entre o final de uma eleição e a publicação do seu resultado; a extinção de erros no preenchimento das cédulas de papel; a possibilidade de que pessoas com baixo grau de instrução possam votar; entre outras.

Os SEVs estão sendo usados em diversos países e têm como alvo principal o fornecimento dos requisitos, propriedades, regras e leis instauradas para o sistema eleitoral, primando à conformidade com os padrões e princípios democráticos específicos de cada nação. Em muitos países, as eleições oficiais são acondicionadas por instituições governamentais que em geral optam pelo uso de um Sistema Eletrônico de Votação. Esses sistemas por sua vez expressam uma

quantidade relevante de brechas de segurança e, na sua grande maioria, não viabilizam um processo efetivo de auditoria externa, o que prejudica a transparência total do sistema, fora que muitos desses são desenvolvidos por empresas que fazem uso de modelos computacionais de arquiteturas fechadas (proprietárias), o que dificulta ainda mais a fixação de padrões nesse mercado.

No Brasil, o início do processo de informatização das eleições ocorreu em 1996, onde então foi apresentada ao mundo a aplicabilidade de um modelo de votação na forma eletrônica em sua completude e que, segundo autoridades responsáveis, ainda é apontado como seguro e isento à fraude. Esse processo eleitoral informatizado se alastrou aos poucos pelo país, até que no ano de 2000 todos os municípios brasileiros o implantaram.

Para muitos, o sistema eletrônico de votação brasileiro proporcionou um grande avanço para o país afinal, segundo asseveração dos seus responsáveis, e contrariando até certo ponto a lógica, uma vez que a empresa responsável pelo hardware (Diebold) é americana e seus componentes são importados, todo o processo de fabricação das urnas ocorre internamente e o resultado de uma eleição é dado com muita celeridade. No entanto, há quem divirja da segurança em vários pontos desse processo. Ao longo desses anos de utilização das urnas eletrônicas de votação, houve diversas revelações de fraudes e muitos relatórios com provas circunstanciais (ARANHA, 2014), colocando em cheque a inviolabilidade da urna brasileira.

Partindo desse terreno fecundo para pesquisa, cientistas e especialistas de todo mundo e de diversas iniciativas, como as governamentais, privadas e acadêmicas, estão interessados em estudar os SEVs, muito em decorrência de seus grandes desafios. Suas falhas criam um ambiente propício para pesquisadores que buscam resolver os problemas inerentes ao uso desses sistemas, tendo como objetivo principal torná-los mais seguros e robustos para o bem da democracia.

1.1. Motivações da pesquisa

Os principais métodos de criptografia ergueram-se como técnicas militares, criadas para promover a transferência segura e sigilosa de informações estratégicas.

Em anos, a criptografia foi de uso e entendimento exclusivo de especialistas, visto que os mecanismos de crifragem e decifragem, eram custosos e, geralmente eram parte integrante do segredo. Em meio à segunda Guerra Mundial, as técnicas de criptografia ganharam uma nova propulsão, com o emprego da automação desses métodos, fazendo uso de sistemas eletromecânicos. O caso mais referenciado nesse sentido foi a máquina Enigma descrito por Simon Singh no *Livro dos Códigos* (SINGH, 2001). Em outra vertente, surgiram as metodologias de criptoanálise, que contaram com significativas contribuições do “pai da computação moderna”, Allan Turing.

Nesse momento da história, os segredos militares deixaram de ser o principal foco da aplicabilidade das técnicas de criptografia. Nos dias atuais, dada a ampla utilização de sistemas que visam proporcionar transações comerciais com segurança e privacidade, como as transações bancárias e autenticação em redes privadas, por exemplo, a criptografia tornou-se o modelo mais próximo para fornecer uma segurança efetiva.

Paralelamente aos estudos das técnicas de criptografia, há um grande fórum mundial de discussão sobre a segurança dos sistemas empregados em eleições. Incidências de fraudes eleitorais não é um problema novo, nem tão pouco irrelevante. Alguns eventos podem ser destacados ao longo da sua existência, como forma de endossar o presente trabalho, como exemplo, o relatório do professor Diego Aranha (ARANHA, 2012) que apresenta uma análise da segurança do software da urna eletrônica brasileira, que foi abalizado na experiência vivida pela equipe da Universidade de Brasília (UnB) enquanto participantes da 2º edição dos Testes Públicos de Segurança do Sistema Eletrônico de Votação, organizados pelo Tribunal Superior Eleitoral (TSE) no ano de 2012.

Levando em consideração os relatos, é latente a necessidade da amarração da transparência com a automação de recursos, mitigando assim os riscos da ocorrência de fraudes e potencializando as possibilidades de auditoria e recontagem dos votos. Dessa forma, a criptografia computacional vem apresentando ferramentas adequadas para atender demandas quanto à segurança de um Sistema Eletrônico de Votação (SEV).

1.2. Objetivo geral

A pesquisa tem como principal desígnio estudar e avaliar os princípios de um Sistema Eletrônico de Votação (SEV), bem como suas principais tecnologias e desafios existentes. A partir desse estudo é descrita a proposta de um modelo utilizando criptografia visual, a fim de prover mecanismos que atendam o requisito de verificabilidade E2E com a possibilidade real da materialização do voto de um modo não tradicional, tendo como foco o emprego desse esquema no Sistema Eletrônico de Votação (SEV) brasileiro.

1.3. Objetivos específicos

Diante da necessidade em se manter o alto nível dos critérios de segurança estabelecidos para um Sistema Eletrônico de Votação (SEV), bem como garantir o direito do eleitor num estado democrático, este trabalho apresenta os seguintes objetivos específicos:

1) Realizar análise e contextualização dos sistemas de votação, tratando desde os requisitos para seu desenvolvimento, passando pelos seus principais desafios, chegando então as gerações que contemplam os modelos desse tipo de sistema;

2) Realizar estudo em alguns dos principais sistemas eletrônicos de votação de terceira geração existente no continente americano, com o objetivo de explorar uma análise comparativa entre os mesmos;

3) Realizar análise do sistema eletrônico de votação brasileiro, em conjunto com as principais técnicas de criptografia empregadas em SEVs na atualidade;

4) Enfatizar o estudo dos modelos de criptografia visual, como o principal mecanismo a ser aplicado no sistema brasileiro. A escolha da criptografia visual, trás uma série de novidades a esse campo de pesquisa, principalmente no que se refere ao uso de um modelo criptográfico não convencional. Além disso, o emprego da criptografia visual no modelo proposto insere menor custo computacional ao processo de decriptação;

5) Desenvolver uma proposta para aplicação de criptografia visual no sistema eletrônico de votação brasileiro, a fim de prover o requisito de verificabilidade E2E a esse sistema.

1.4. Organização da dissertação

Este trabalho está organizado da seguinte forma. No Capítulo 2 é abordada a caracterização dos sistemas de votação, passando primeiramente pela evolução desses sistemas, tratando dos seus principais requisitos e desafios e então abordando os principais modelos de sistemas de votação, classificados como: modelo tradicional; de primeira geração; de segunda geração; de terceira geração e os End-to-End Verificable Internet Voting (EVIV), incluindo sua distribuição ao redor do mundo. No Capítulo 3 é realizada uma análise dos principais Sistemas Eletrônicos de Votação de terceira geração – E2E. Sendo debatida inicialmente a importância do requisito de verificabilidade E2E em um SEV, passando então para o detalhamento dos sistemas: Scantegrity II; Helios Voting; Vot.ar e finalizando com o SEV da Venezuela. No Capítulo 4 é feita a introdução ao sistema eletrônico de votação brasileiro, que servirá como base para o entendimento da proposta desse trabalho descrita no Capítulo 6. No Capítulo 5 são abordados os principais modelos da criptografia moderna empregados em SEV, dando ênfase aos modelos de criptografia visual que são utilizados como elemento dessa proposta. Por fim, no Capítulo 6 é descrita a proposta, sendo detalhado desde o emprego da criptografia visual no SEV brasileiro, até os mecanismos necessários para a viabilização desse modelo na urna brasileira. Finalizando a produção, estão descritos a conclusão e os trabalhos a serem realizados no futuro.

CAPÍTULO 2

"Descobrir consiste em olhar para o que todo mundo está vendo e pensar uma coisa diferente."

Roger Von Oech

Caracterização de sistemas de votação

Recentemente diversos trabalhos sobre SEVs vêm sendo pesquisados e propostos ao redor do mundo. Este capítulo aborda a caracterização dos sistemas de votação, passando primeiramente por sua evolução, tratando dos seus principais requisitos e desafios, e então abordando os principais modelos de sistemas de votação, classificados segundo o professor Pedro Rezende (REZENDE, 2012) como: sistema de votação tradicional, sistemas de votação de primeira geração, de segunda geração, de terceira geração e os sistemas de votação pela Internet. É descrito também a distribuição desses sistemas ao redor do mundo.

2.1. A evolução dos sistemas de votação

O voto por voz é considerado o mais antigo sistema de votação utilizado em uma democracia. A forma de se produzir uma eleição partia do Princípio de que os eleitores anunciavam em voz alta seu voto, para que as outras pessoas envolvidas no pleito pudessem registrar a quantidade de votos para cada candidato.

Segundo descrito por Douglas W. Jones em (DOUGLAS, 2012), numa eleição no Estado de Missouri em 1846, relatou-se que um eleitor se encaminhou até o local da votação, então ficou na fila esperando e prestes a gritar seu voto. Sob uma análise sucinta, pode-se constatar o uso do mecanismo de autenticação, onde o juiz eleitoral empossa o eleitor, anuncia seu nome e o eleitor realiza a

promessa sob a bíblia de que ainda não votou e que ele está autorizado a votar naquele lugar. Este relato está ilustrado na Figura 1.

Figura 1 – Pintura do processo eleitoral do Estado de Missouri em 1846 (DOUGLAS, 2012)

Há uma grande amostra para o mecanismo de autenticação detectado no modelo descrito em (DOUGLAS, 2012) e visto na Figura 1. Uma vez que o eleitor está chamando o seu nome em voz alta, todos os seus conhecidos e amigos saberão que ele é realmente quem diz ser. Após isso ele também vai falar em voz alta o nome do candidato que quer eleger, dessa forma, todos ao redor poderão ouvir sua escolha, inclusive os oficiais responsáveis pela votação, que são os responsáveis diretos em anotar o registro do voto. Existem muitos oficiais ao redor, como forma de prover redundância ao registro e, por conseguinte maior segurança. No entanto o melhor mecanismo do modelo atende pelo fato de que o sistema permite que qualquer pessoa em pé ao redor, qualquer cidadão, possa também fazer um registro independente da votação.

O grande problema do modelo descrito em (DOUGLAS, 2012), está na possibilidade de manipulação dos votos, uma vez que não há qualquer segredo no escrutínio e todo mundo pode saber como e em quem o eleitor votou. Este tipo de coerção aos eleitores, tanto nas formas mais leves, quanto nas mais agressivas, é que produz um enorme problema de segurança a esse sistema, visto que não havia nenhuma proteção à privacidade dos eleitores, tornando-se fácil a intimidação ou compra dos votos.

Todos os problemas relatados afetam seriamente a segurança de um sufrágio e isto impulsionou mudanças, como o emprego de tecnologias. Para as

eleições, as cédulas de votação foram as primeiras formas de tecnologias utilizadas. Em 1870, por exemplo, foi desenvolvida uma urna que continha um bloqueio, através de uma fechadura, certificando assim que ninguém pudesse abrir e remover as cédulas. Essa tecnologia foi concebida para proporcionar integridade e proteção para o sigilo do voto, no entanto, se os procedimentos não fossem seguidos a risca ou se as pessoas tentassem violar a segurança da eleição, de forma astuta, abrir-se-ia uma série de possibilidades para fraudar o sistema.

Com o objetivo de potencializar a segurança para o sigilo do voto, vários processos foram iniciados em meados dos anos 1800, principalmente na Austrália, onde foram introduzida uma série de inovações tecnológicas, destacando-se a criação da cédula pré-impressa por Michel Radwin em (RADWIN, 1995). Na ocasião, ao invés do eleitor levar sua própria cédula, o governo era que se responsabilizava pela impressão da cédula, em seguida os eleitores apenas iam ao local da votação para realizar o registro em segredo, dentro de uma “cabine indevassável”.

No final do século XIX, a Revolução Industrial estava caminhando a passos largos, trazendo com si uma série de avanços tecnológicos, em especial a capacidade de projetar e construir dispositivos mecânicos. Desse avanço surgiram relevantes projetos de dispositivos de votação mecanismos e suas cabines, que viriam a entrar em produção no final do século XIX e se destacarem no primeiro semestre do século XX, sendo então a tecnologia de votação mais empregada nos EUA. A Figura 2 representa uma máquina de votar mecânica, construída durante a Evolução Industrial.

Figura 2 – Máquina de votar mecânica, construída durante a Revolução Industrial

Estas máquinas produziam um registro direto das escolhas dos eleitores, fazendo isso através de um sistema de alavancas e engrenagens sem a necessidade do eleitor ter que anotar. A afirmação a respeito dessas máquinas era forte, os primeiros projetistas evidenciavam a garantia total do sigilo do voto, além de ser absolutamente à prova de fraldes, declarando praticamente seus inventos como o instrumento salvador de uma democracia. No entanto, o requisito de verificabilidade do voto (Seção 2.2.4) fica comprometido, além de serem máquinas complexas e com milhares de engrenagens em movimento, favorecendo naturalmente as falhas mecânicas. Outro grande problema era seu tamanho desproporcional e seu alto custo de projeto.

Nos anos de 1950 e 1960, surgiu um novo tipo de tecnologia baseada em computação, utilizando cartões perfurados, em que os dados da votação ficariam registrados nos cartões, através da perfuração por parte do eleitor. Um dos principais problemas com os cartões perfurados eram seus picotes, como resultado da perfuração para fora dos pequenos buracos. Na grande maioria dos casos, estes picotes não eram destacados do cartão, fechando novamente o buraco efetuado pelo eleitor e assim podiam não entrar na contagem dos votos.

Ainda neste capítulo (Seção 2.4) é abordada a classificação dos SEV, traçando um estudo da sua evolução baseada em gerações.

2.2. Requisitos chaves de um SEV

Em um sistema de votação tradicional, considera-se factível a existência de erros na contagem dos votos, a existência de pessoas capazes de venderem os seus votos ou, ainda mais grave, que possam existir agentes coercitivos entre os candidatos a eleição, mesmo que isso não resulte em um impacto considerável no resultado final de um processo eleitoral. No caso dos SEVs é importante que estes cumpram qualidades desejáveis de um processo eleitoral.

Devemos então avaliar os requisitos chaves de um Sistema Eletrônico de Votação (SEV), especialmente para que possamos entender sob que aspectos ocorrem a execução de todo o processo eleitoral e o que visa entregar um projeto de SEV. Neste trabalho são descritos essencialmente os requisitos considerados mais proeminentes de um SEV, no caso: integridade; privacidade; incoercibilidade e verificabilidade.

2.2.1. Integridade do processo

O requisito de integridade em Sistemas Eletrônicos de Votação (SEV) objetiva a garantia de três condições básicas:

- **Integridade do pessoal:** Todo o recurso humano envolvido no projeto, implementação, administração e operação do SEV, devem ser incorruptíveis e de integridade inflexível, inclusive todo pessoal envolvido com a distribuição e armazenamento dos dados e equipamentos;
- **Integridade do sistema:** O sistema pode e deve ser posto à prova de integridade, após a validação e certificação de auditores externos;
- **Integridade dos votos:** A mais importante escala, que visa garantir que os votos não possam ser modificados, forjados e/ou descartados durante o processo de votação, até o término de todo o processo eleitoral.

2.2.2. Privacidade do voto

Segundo relatado por Michel Radwin e Phil Klein em (RADWIN, 1995), as principais propostas de protocolos para SEV, descrevem diversas propriedades de privacidade e segurança. Fundamentalmente, um protocolo confiável tem como objetivo garantir que o SEV não permita que qualquer indivíduo tenha condições ainda que ínfimas de desvendar qual o voto de um determinado eleitor, nem tampouco que o eleitor tenha possibilidades, mesmo que de forma involuntária, provar publicamente qual foi a sua escolha. Isto quer dizer que quando um eleitor apresenta seu voto através de um canal de comunicação, ele pressupõe que um indivíduo mal intencionado pode está ouvindo esse canal e pode interceptar os dados.

A fim de atingir a propriedade da privacidade, o protocolo escolhido deve aplicar algum mecanismo confiável de encriptação dos dados, como por exemplo, um sistema de criptografia assimétrica.

Outro ponto importante desse requisito descreve o anonimato, que visa impedir qualquer associação entre o voto e a identidade do eleitor. A segregação destes dados deve fomentar a impossibilidade de relacionar o eleitor com o respectivo voto, quer seja durante o processo de votação, ou até mesmo após esse a finalização desse processo.

2.2.3. *Receipt-freeness*

Um requisito essencial para prover mecanismos de auditoria externa, é elevar o nível de resistência a agentes coercitivos do sistema de votação, ou seja, o eleitor não pode ter a menor possibilidade de provar em quem votou. O sistema de votação nesse caso deve ser capaz de fornecer mecanismos que garantam o cumprimento dessa propriedade, fazendo com que seja obstada a prática de fraudes, como exemplo, a compra de voto e a coação de eleitores.

2.2.4. Verificabilidade do voto

Esse requisito é fornecido quando, independentemente do modelo empregado, é possível verificar que todos os votos foram computados e contados corretamente.

É comum encontrar duas definições de verificabilidade, a individual e a universal, onde respectivamente compreende-se que cada eleitor possa verificar se seu voto está correto e efetuar a contagem dos outros votos e que todos possam verificar que a contagem dos votos está correta, mas não necessariamente sendo possível verificar cada voto individualmente.

Nos sistemas de votação tradicionais (Seção 2.4.1), qualquer pessoa entende o seu funcionamento, por isso o requisito de verificabilidade não se destaca como no nível de SEVs, em que fazem uso de técnicas conhecidas apenas por um cenário restrito de indivíduos. Neste tipo de sistema se faz necessário que os eleitores consigam obter uma prova do seu voto, para que possam confiar nele.

Este trabalho visa elaborar e propor um modelo que possa vir a fornecer esse requisito ao Sistema Eletrônico de Votação brasileiro.

2.2.5. Outros requisitos

Além dos requisitos chaves anteriormente descritos, segundo Rui Rocha (ROCHA, 2004), um sistema eletrônico e votação deve atender a requisitos básicos que fornecem confiabilidade na utilização desses sistemas. A seguir estão descritos alguns desses requisitos:

- **Exatidão:** Um SEV é considerado exato se: 1) não for possível que um voto legítimo seja modificado; 2) não for possível que um voto legítimo seja

eliminado da contagem geral; 3) não for possível que um voto inválido entre no resultado final de uma votação;

- **Democracia:** Um SEV é considerado democrático se: 1) só permitir que eleitores autorizados possam votar; 2) cada eleitor possa votar apenas uma vez;
- **Conveniência:** Um SEV é considerado conveniente se o eleitor pode desempenhar seu direito de voto de forma rápida e com o mínimo de equipamentos e competências necessários;
- **Flexibilidade:** Os equipamentos de votação que contemplam um SEV devem suportar uma variedade de questões relacionadas com o processo de votação, como por exemplo, a utilização por pessoas que possuam necessidades especiais.

2.3. Principais reptos de um SEV

Alguns dos principais reptos de um SEV estão diretamente ligados ao requisito de verificabilidade do voto, onde na grande maioria dos sistemas, o eleitor não tem a possibilidade de executar um processo para cotejo do seu registro. Nesta seção são discutidas duas contraposições clássicas relacionadas a esse requisito: 1) verificabilidade x privacidade; 2) verificabilidade x incoercibilidade. A partir disso, é possível compreender melhor a importância da utilização desse recurso, bem como sua complexidade dado o confrontamento existente com outros requisitos chaves do sistema.

Como complemento ao entendimento desse tópico, é tratada ainda a interposição entre as transações e tolerância a falhas inerentes a esse tipo de sistema, bem como a escassez de implementações e os principais ataques que o assolam.

2.3.1. Verificabilidade x Privacidade

Os requisitos de verificabilidade e sigilo do voto a priori se manifestam como contraditórios. Então devemos considerar a seguinte hipótese: o eleitor “X” deve ser capaz de receber e conferir as garantias quanto à integridade das eleições que participa, sobretudo, que o registro do seu voto tenha sido contabilizado de forma expressamente correta. Queremos então que “X” possa sacar algumas

informações do registro, a fim de comprovar se seu voto foi realmente contabilizado, mas nenhuma dessas ações, em nenhuma das fases do processo, deve revelar em quem “X” votou. Os processos que disponibilizam o requisito de verificabilidade do voto não devem revelar como e em quem “X” votou, mesmo que involuntariamente, ou ainda que o mesmo esteja disposto a tornar público seu sufrágio a um agente coercitivo.

Desde a construção das primeiras estruturas de voto secreto, os sistemas de votação, na sua grande maioria enfatizaram mais o requisito de privacidade que a propriedade de verificabilidade, pode-se comprovar isso a partir de alguns mecanismos clássicos utilizados, como a “cabine indevassável” de votação e as urnas seladas como forma de garantir o sigilo constitucional do voto. O fato é que diferentes estágios do processo eleitoral podem ser verificáveis dentro de uma escala aceitável. Os eleitores podem examinar visualmente que seus votos são contabilizados conforme sua intenção, os observadores podem ser autorizados a estarem presentes no local da votação e na fase da contagem dos votos, e as auditorias pós-eleição podem verificar que as cédulas de papel não evidenciam discrepâncias significativas do registro eletrônico.

Podemos acrescer ainda mais o percentual de verificabilidade, pois na grande maioria dos processos eleitorais modernos, ainda é necessário confiar nos oficiais da eleição e no sistema eletrônico de votação instaurado. Os eleitores geralmente não recebem qualquer garantia de que seus votos não foram perdidos ou adulterados e que todos os votos registrados são contados corretamente. Resta somente aos eleitores confiar que o equipamento foi programado e testado sem possibilidade alguma de haver desacertos. Então, a ideia fundamental é tornar possível a verificação da integridade de uma eleição como um todo.

2.3.2. Verificabilidade x Incoercibilidade

Diversos autores, como Schoenmakers (SCHOENMAKERS, 2000), pregam que a única solução para este desafio é o recurso a Sistemas Eletrônicos de Votação baseados em encriptação homomórfica (Seção 5.1.7), uma vez que este mecanismo permite decifrar o resultado da eleição sem decifrar os votos individuais. Entretanto, esses sistemas de votação possuem entraves críticos em decorrência da técnica utilizada, como o grande volume de tráfego de dados gerado, o que implica diretamente na sua utilização em eleições de grande escala.

É proeminente argumentar a existência de processos eleitorais que necessitem de altos níveis de verificabilidade fornecidas pelos mecanismos de criptografia, ao passo que fornecem garantias quanto à incoercibilidade. O fato é que, para muitos pesquisadores esses requisitos não convergem no mesmo momento, ou seja, o mecanismo de incoercibilidade é desnecessário desde o início, pois o caráter remoto do processo torna-o incapaz de fornecer garantias factíveis. Já a verificabilidade E2E, tratada como um dos principais objetos dessa pesquisa, a ser fornecida por esquemas e ferramentas criptográficas, é um meio considerado por muitos, como a garantia de um nível admissível de integridade ao processo eleitoral.

2.3.3. Escassez de implementações

Embora já exista uma quantidade apreciável de propostas para SEVs, ainda é grande a carência por implementações nessa área. Algumas empresas produzem sistemas para esse setor, no entanto apenas uma pequena parte delas opta por distribuir seus projetos como código aberto e, essa predominância de sistemas de código proprietário representa um fator que dificulta consideravelmente o estudo e a evolução de SEVs.

A grande maioria de propostas ainda deriva de ambientes acadêmicos e experimentais, onde periodicamente são apresentados trabalhos que visam o avanço de SEVs. Por exemplo, podem ser citados trabalhos relevantes para área como os descritos no Capítulo 3.

2.4. Classificação de sistemas de votação

Segundo Pedro Rezende em (REZENDE, 2012), a evolução dos sistemas de votação eletrônica segue as respectivas tecnologias: 1ª geração – Urnas DRE; 2ª geração – Urnas VVPAT; 3ª geração – Urnas E2E. Os tópicos a seguir têm como objetivo fornecer um entendimento a respeito das gerações descritas pelo autor, além de tratar como complemento, os sistemas de votação tradicional e os sistemas de votação pela Internet (EVIV).

2.4.1. Sistema de votação tradicional

Os sistemas de votação tradicional são considerados os mais antigos entre todos os sistemas de votação existentes. Seu modelo é tipicamente caracterizado pelo uso de cédulas de papel como registro do voto e, essas são depositadas em urnas tradicionais. Países como Alemanha, Holanda e Japão fazem uso desse sistema, seguindo algumas especificidades próprias ao processo.

Os sistemas de votação baseados em cédulas de papel trabalham com protocolos que consistem basicamente em três fases:

- **Identificação e habilitação para registrar o voto:** Na data agendada para a eleição, o votante comparece à seção eleitoral e apresenta um documento que evidencie sua identidade eleitoral, nesse momento suas informações são conferidas em uma lista oficial, como forma de comprovar sua legitimidade para votação. Em seguida, ele recebe uma cédula de papel contendo uma marca oficial que certifique sua integridade e evite fraudes no processo;
- **Registro do voto na cédula:** A cédula de papel possui uma lista com os nomes dos candidatos elegíveis, em que o eleitor faz uma marca com uma caneta ou registra o voto perfurando a cédula ao lado do nome do candidato. Na cédula ainda pode existir um espaço em branco para que o eleitor escreva o nome e/ou o número correspondente ao candidato a ser votado;
- **Apuração dos votos:** Após o término da votação, as autoridades competentes abrem as urnas e procedem com a contagem manual das cédulas, ou então fazem uso de algum equipamento específico para automatizar a contagem.

Conforme já foi dito, cada país possui especificidades relacionadas ao emprego da cédula de papel. Na Alemanha, por exemplo, o processo de votação para a principal câmara legislativa em Bundestag (Parlamento da Alemanha), o eleitor tem direito a registrar dois votos em uma mesma cédula, sendo um voto para o candidato direto e outro voto para um partido específico. Conforme Stefan Koch em (STEFAN, 2009), essas particularidades segue as determinações do sistema eleitoral de cada país.

Ainda segundo Stefan Koch (STEFAN, 2009), a cédula de papel do sistema eleitoral alemão, consiste basicamente em duas listas, divididas entre candidatos e partidos, para realizar o registro do voto o eleitor marca um “X” dentro de um círculo que fica ao lado do nome do candidato e outro “X” no círculo ao lado do nome do partido, seguindo sua intenção de voto.

Na Holanda, por exemplo, o eleitor faz uso de um lápis de cor vermelha para registrar a sua intenção na cédula de papel. A cédula contém uma lista partidária com vários nomes de candidatos, chegando a alguns momentos constar até 60 nomes, o que consequentemente deixa a cédula num tamanho fora do comum e afeta critérios de usabilidade. Para votar o eleitor preenche a cédula com um círculo bem ao lado do nome do candidato de sua preferência. Juntamente com o nome do candidato, a cédula possui outras informações relevantes, como por exemplo, o nome do partido. As principais vantagens e desafios existentes em um sistema de votação tipicamente tradicional estão descritas no Quadro 1.

Principais vantagens	**Principais desafios**
• Todos os eleitores compreendem facilmente a forma de votar; • Todos sabem como é realizada a apuração e recontagem dos votos; • Todos os eleitores veem o armazenamento do voto na urna; • Existe a possibilidade de recontagem em um processo de auditoria, visto que o voto está materializado; • Tem baixo custo, porque necessita de menores recursos comparados a outros sistemas; • É o recurso mais utilizado quando demais modelos apresentam falhas.	• Demora muito tempo para obter o resultado de uma eleição; • Pode apresentar problemas como rasura ou má marcação da cédula, fazendo com seja necessário a anulação; • Pode haver erros na contagem feita manualmente, devido a falhas humanas; • Em casos de erros na contagem, não existe contraprova do voto; • Desconfiança em algumas nações devido a grande quantidade de fraudes já ocorridas.

Quadro 1 – Vantagens e desafios do sistema de votação tradicional

2.4.2. Sistema de votação de 1ª geração (DRE)

Mais conhecido como sistema de votação com gravação eletrônica direta, do inglês *Direct Recording Eletronic (DRE)*, são dispositivos que dependem unicamente de software para efetuar o processo de registro do voto, de tal forma que não concebem outros métodos para comprovação do sufrágio, como por exemplo, a materialização do voto através da impressão. Seu emprego foi iniciado amplamente na década de noventa, em nações como Holanda, Índia, Alemanha e Brasil. Segundo relatado por Américo Monteiro em (MONTEIRO, 2001), o Brasil foi o primeiro a realizar um processo de votação 100% informatizado fazendo uso de um sistema de 1ª geração, ou seja, aplicando as urnas eletrônicas DRE desde a fase de alistamento até a fase de apuração e totalização dos votos.

Uma urna DRE é um equipamento composto tipicamente por hardware e um software embarcado, no qual o eleitor registra sua intenção de voto através do toque na tela ou utilizando um teclado adaptado, como ocorre nas eleições brasileiras. Conforme descrito por Regivaldo Costa em (COSTA, 2008), as urnas DREs não fazem uso de papel para realizar o registro dos votos, que tão somente são armazenados em um dispositivo de memória secundária, podendo ou não estar encriptados. Ao fim da fase de votação, os votos são encaminhados para o local autorizado pelo órgão competente e então é produzida a totalização dos votos. As Figuras 3 e 4 ilustram respectivamente dois modelos clássicos de urnas que contemplam o modelo de 1ª geração – DRE.

Figura 3 – Modelo de urna DRE usada na Holanda até 2006

Figura 4 – Modelo de urna DRE usada no Brasil até os dias atuais

Assim como em um sistema de votação tradicional, cada país possui particularidades na utilização das urnas do tipo DRE. O Quadro 2 descreve as principais vantagens e desafios desse modelo em um processo eleitoral.

Principais vantagens	Principais desafios
• A totalização dos votos ocorre de forma quase que automática; • O tempo de apuração total dos votos é de no máximo 24 horas; • Não há como existir rasuras ou má marcação por parte do eleitor; • Possui boa interface e um designe enxuto, o que facilita o seu uso por diversas pessoas; • São projetadas para suporta diversos ambientes.	• Causa a falsa ideia de segurança absoluta; • Extremamente difícil realizar a detecção de uma fraude; • Por não existir a materialização do voto, a possibilidade de recontagem é limitada; • Descarta a possibilidade de auditoria por parte do eleitor; • Pouco conhecimento sobre o funcionamento dos softwares das DREs, fazendo com que seja necessário confiar plenamente nos projetistas e órgãos responsáveis pelo desenvolvimento.

Quadro 2 – Vantagens e desafios das máquinas DREs

Relatos de pesquisadores apontam para uma série de problemas envolvendo as urnas do tipo DREs, entre os principais temos alguns revelados através de processos de auditoria independente realizados em equipamentos de diversos países e que apontaram esse tipo de urna com não segura. Um dos mais relevantes é o caso da Índia descrito por Hari Prasas em (PRASA, 2010), onde foram apontados possíveis ataques ao processo eleitoral como: adulteração do software da CPU antes mesmo da fabricação; substituição de CPU clonada; substituição de unidade clonada e troca do display original da urna. Outro caso foi relatado pelos pesquisadores holandeses Jacobs e Pieters em (JACOBS, 2009), que destacaram a facilidade em substituir os chips do software, fazendo com que fosse possível realizar a contagem de votos de forma adulterada. Outro problema estava na possibilidade de espionar uma votação usando uma técnica conhecida como tempest que visa interceptar e escutar emissões de radio frequência de um dispositivo, esta técnica poderia perfeitamente causar a quebra do sigilo do voto.

Todos os problemas relatados pelos pesquisadores significam riscos concretos e impelem a um agravante, pois as máquinas do modelo DRE não apresentam mecanismos suficientes que possam disponibilizar o requisito de verificabilidade do voto, abrindo espaço para que muitos dos ataques possam vir a ser executados e passem despercebidos. A Figura 5 ilustra segundo o professor Pedro Rezende (REZENDE, 2012) a Custódia do voto em uma máquina DRE, o que evidencia a falta de controle em algumas fases de uma eleição.

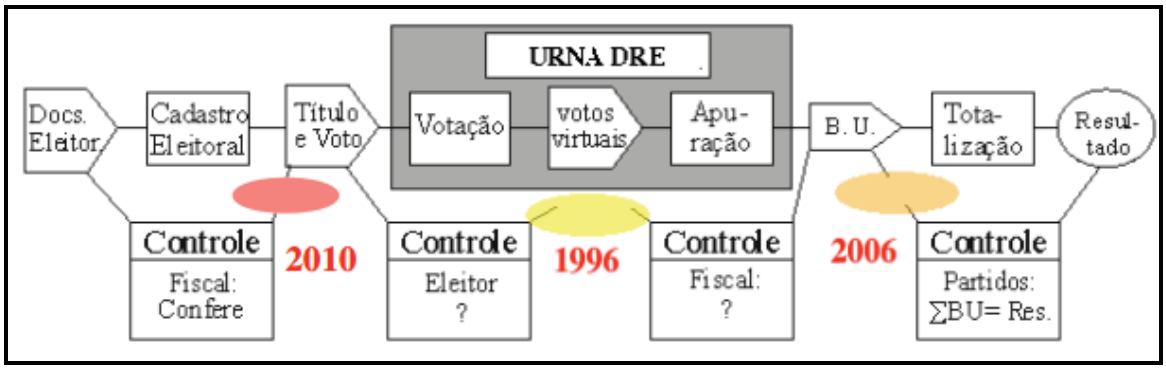

Figura 5 – Custódia do voto em máquinas DRE (REZENDE, 2012)

No Capítulo 6 é proposto um modelo utilizando criptografia visual que possibilita a inserção de um mecanismo para a verificabilidade dos votos em máquinas do tipo DRE, mais especificamente para o sistema eletrônico de votação brasileiro.

2.4.3. Sistema de votação de 2ª geração (IVVR ou VVPAT)

Os pesquisadores Ronald Rivest e John Wack foram os primeiros a propor o conceito do *princípio da independência do software* (RIVEST, 2006), que expressa que se houver uma modificação ou erro não detectado no software, este não poderá causar uma modificação ou erro indetectável no resultado da apuração dos votos. As máquinas que utilizam este princípio são chamadas de máquinas de votar de 2ª geração conforme descrito por Rebecca Mercuri em (MERCURI, 2000), pois conferem uma segunda maneira de contabilizar os votos sem a dependência total do registro eletrônico realizado pelo software. Um modelo de urna de 2ª geração – IVVR ou VVPAT pode ser visto na Figura 6.

Figura 6 – Urna Smartmatic, com VVPAT, usada na Venezuela

Exemplos dessas máquinas são os sistemas de contagens por escâner ópticos, do inglês: *Precint Count Optical Scan (PCOS)* e DREs com o voto impresso conferível pelo eleitor, do inglês: *Voter Verified Paper Audit Trails (VVPAT)*. Posteriormente a literatura técnica definiu esse conceito como *Independent Voter Veriable Record (IVVR)*. A figura 7 ilustra segundo Pedro Rezende (REZENDE, 2012) a custódia do voto em máquina do tipo IVVR ou VVPAT.

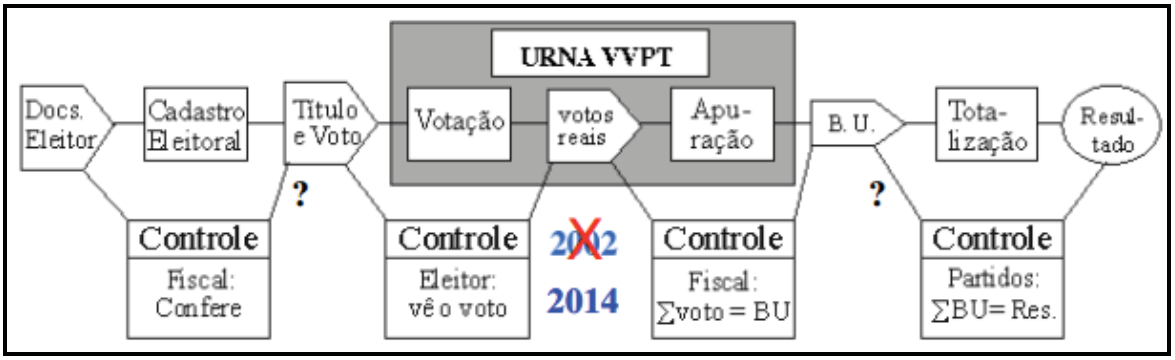

Figura 7 – Custódia do voto em máquinas VVPAT (REZENDE, 2012)

Outro exemplo é a nova tecnologia empregada pela empresa argentina MSA, em que faz uso de cédulas com chips de RFID para registro do voto e nestas mesmas cédulas o voto é materializado de forma impressa. O Quadro 3 mostra as vantagens e desafios das máquinas que seguem o modelo de 2ª geração.

Principais vantagens	Principais desafios
• Permite processo de auditoria futuras, visto que a cédula marcada pelo eleitor já consiste na materialização do voto; • Com o voto depositado no escâner, o eleitor sabe se o mesmo foi realmente registrado, visto que esse tipo de máquina rejeita cédulas com marcações incorretas, dando ainda a chance de o eleitor utilizar outra em branco; • Em caso de falta de energia a votação poderá continuar, pois a maioria dos escâneres possui bateria interna.	• Dificuldade com acessibilidade para eleição com muitos candidatos; • Pode ocorrer manipulação no resultado e mesmo assim a fraude passar despercebida.

Quadro 3 – Vantagens e desafios dos sistemas de 2ª Geração

2.4.4. Sistema de votação de 3ª geração (E2E)

Também conhecidos como *End-to-End Voter Verifiable (E2E)*, esses sistemas de votação são dotados de características que atendem os requisitos de integridade e sigilo do voto. Sua construção tem por base permitir a verificação do voto pelo eleitor, fornecendo um mecanismo que possibilita saber se os votos não foram adulterados, ao mesmo passo que não revela quais candidatos foram votados. Seguindo características das máquinas de 2ª geração (VVPAT), os

sistemas de 3º geração possuem duas vias de verificação, o software e a cédula, contando ainda com um diferencial que permite que o eleitor possa obter um recibo do seu voto. Com esse processo, disponibiliza-se a verificação fim-a-fim (E2E) do voto, garantindo assim que o voto marcado é realmente o voto computado pela urna. Este recibo insere outra característica importante, a saber, a possibilidade de se identificar em um processo de auditoria qual das duas vias foi possivelmente adulterada, o que não é possível nas máquinas de 2ª geração.

Uma das principais distinções desse processo está na cédula, onde num sistema E2E há o registro de um código de verificação. Esse código de verificação será fornecido ao eleitor como um recibo, possibilitando ao mesmo verificar se o seu voto está de acordo com a sua intenção, sem, entretanto, fazer qualquer tipo de vinculo direto a intenção do voto em candidato especifico. Dessa forma qualquer eleitor ou terceira parte pode verificar o voto, porém não saberá em quem foi votado, garantindo assim a propriedade do sigilo do voto. A Figura 8 ilustra um modelo de urna de 3ª geração – E2E.

Figura 8 – Máquina Vot.ar usada na Argentina desde 2010

As características desse sistema possibilitam diversas maneiras de implementação, a grande maioria delas fornecendo baixo custo. A votação pode ser realizada com papel e caneta pura e simplesmente, sem fazer o emprego de qualquer artifício criptográfico e talvez obscuro para a maioria dos eleitores leigos. Entretanto, o emprego de mecanismos criptográficos é expressamente

recomendado para esse modelo, visto que a automação além de fornecer agilidade ao processo como um todo, também adiciona maior confiabilidade.

Segundo Pedro Rezende (REZENDE, 2012), nos sistemas de 3ª geração, se houver alguma diferença entre o resultado eletrônico e a verificação pelo registro material, o processo integrado permite rastrear, em tempo real, o erro ou desvio ocorrido numa ou noutra trilha. O eleitor terá como saber que seu voto foi contado conforme marcado, ou não, mas sem poder provar a terceiros em quem efetivamente votou. A Figura 9 ilustra segundo Pedro Rezende (REZENDE, 2012) a custódia do voto em máquinas do tipo E2E.

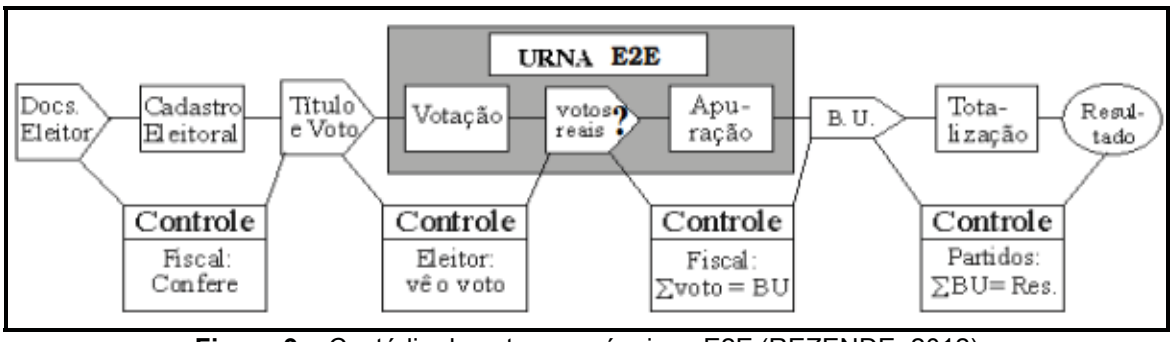

Figura 9 – Custódia do voto em máquinas E2E (REZENDE, 2012)

Ainda conforme descrito por Pedro Rezende (REZENDE, 2012) em 2012, dois modelos eram conhecidos como sistemas aderentes a tais critérios: 1) o modelo que usa redes de misturadores do tipo Mix & Mesh, utilizado, por exemplo, pelo sistema Scantegrity II (Seção 3.3), usado nos EUA; e 2) o modelo que usa registro integrado tipo RFID em cédula, implementado pelo sistema Vot.Ar (Seção 3.5), usado na Argentina.

O maior desafio teórico encontrado em sistemas de 3ª geração está na forma de proteger o sigilo do voto. Em redes de misturadores como a Mix & Mesh (CHAUM, 1981), é imprescindível a correta seleção, implementação e operação dos algoritmos e protocolos criptográficos, pois sem isso é provável que ao invés de fortalecer a segurança, tenham-se mais problemas, como por exemplo, as limitações intrínsecas do modelo no que se refere a confiabilidade, confidencialidade e desempenho, uma vez que funções que garantem o anonimato ficam por vezes centralizadas em um conjunto de pequenos nós, ou seja, quanto menor for a rede, mais sérias se tornam essas limitações (COSTA, 2008).

2.5. *End-to-End Verificable Internet Voting (EVIV)*

Considerando algumas características e desafios existentes nos sistemas de votação de 3ª geração – E2E, conforme descrito acima, Rui Joaquim, Carlos Ribeiro e Paulo Ferreira propuseram o *End-to-End Verificable Internet Voting (EVIV)* (JOAQUIM, 2013). Segundo os autores, esse tipo de sistema disponibiliza garantias consideráveis quanto à integridade, em conjunto com propriedades de privacidade e segurança que oferecem a possibilidade do registro do voto em terminais públicos.

Na grande maioria dos sistemas de votação pela Internet, para prover garantias à privacidade do eleitor e à integridade da eleição, se faz necessário confiar no pleno funcionamento do sistema cliente, porém, esse processo de confiabilidade não é trivial, nem facilmente alcançável dada a complexidade computacional do modelo e o simples fato de que esses terminais (sistemas clientes) geralmente são vulneráveis a inúmeras ameaças virtuais.

Ainda segundo os pesquisadores Rui Joaquim, Carlos Ribeiro e Paulo Ferreira em (JOAQUIM, 2013), os sistemas EVIV propõem mecanismos que visam garantir a privacidade e integridade da eleição através da utilização de um dispositivo considerado inviolável que realiza a cifragem e autenticação dos votos, no caso o *Voter Security Token (VST)*, e também do uso de uma solução de *code voting* como forma de comunicação segura entre o eleitor e o dispositivo a partir do terminal potencialmente inseguro. Dessa forma, através da aplicação de um conjunto de protocolo e técnicas como: *Code Voting; Mark Pledge*; Cifra de múltipla decifra (Seção 5.1.6) e encriptação homomórfica (Seção 5.1.7), o EVIV faz com que nenhuma terceira parte mal intencionada tenha possibilidades de alterar um voto ou quebrar seu sigilo sem passar despercebido, ao possibilitar que o eleitor verifique se o seu voto foi realmente contabilizado segundo sua intenção, fazendo isso através do confrontamento de cadeia de caracteres e a partir da possibilidade de que qualquer interessado pelo processo eleitoral possa verificar que os votos registrados no sistema foram corretamente contados.

Por ser considerado também um sistema E2E, o EVIV preza bastante pela integridade da eleição. Conforme descrito pelos pesquisadores Paulo Ferreira, Rui Joaquim e Carlos Ribeiro (FERREIRA, 2009), o sistema agrupa os conceitos por baixo do protocolo de *Code Voting,* conforme descrito por Rui Joaquim em (JOAQUIM, 2009); da técnica *Mark Pledge,* conforme descrita por Ben Adida em

(ADIDA, 2009) e do processo de contagem de votos homomórfica, descrita por Martin Hirt e Kazue Sako em (HIRT, 2000), possibilitando uma verificação *cast-as-intended* por parte do eleitor e a propriedade de verificabilidade universal da contagem dos votos *counted-as-recorded*, o que faz com que qualquer interessado possa realizar a contagem independente dos votos e confirmar o resultado da eleição, sem que seja quebrado o requisito do sigilo.

As características principais dos sistemas EVIV podem ser resumidas em duas propriedades básicas: 1) cada voto é contabilizado conforme desejo do eleitor; 2) ninguém, além do eleitor e seu VST, têm conhecimento do conteúdo do voto. Além disso, possui também as seguintes características:

- Mobilidade completa do eleitor, visto que todo processo de votação pode ser feito online;
- Forte autenticação do eleitor;
- Nenhuma entidade tem conhecimento do conteúdo de todos os votos;
- Não é necessária a utilização de um canal anônimo durante o processo de registro do voto;
- Fortes garantias quanto à privacidade e integridade do voto, mesmo sendo feito a partir de um terminal potencialmente inseguro;
- Verificabilidade robusta por parte do eleitor.

Ainda conforme pesquisa comparativa realizada por Rui Joaquim, Carlos Ribeiro e Paulo Ferreira (JOAQUIM, 2013), o modelo EVIV é o único sistema E2E que, além de possibilitar a mobilidade total do eleitor, fornece garantias de que nenhuma entidade consegue quebrar o sigilo do voto, juntamente com a não necessidade de submeter anonimamente o voto em terminais inseguros. Um breve comparativo traçado entre o modelo EVIV e outros sistemas *E2E web-based* pode ser visto no Quadro 4.

	Internet E2E			
	Helios	**VeryVote**	**SCV**	**EVIV**
Mobilidade completa do eleitor				X
Forte autenticação do eleitor	X		X	X
Entidade tem conhecimento total dos votos	X		X	X
Não é necessário o uso de um canal anônimo		X		X
Garantias à privacidade e integridade do voto		X	X	X
Permite verificabilidade *cast-as-intended*		X		X
Permite verificabilidade universal	X	X	X	X
Permite perguntas de respostas abertas	X			

Quadro 4 – Comparativo entre o EVIV e outros sistemas E2E

Existe, em contrapartida, grande desconfiança nas propostas apresentadas para esse tipo de sistema, visto que um sufrágio realizado em casa, por exemplo, tem falhas críticas de segurança por não garantir a "cabine indevassável" e ser vulnerável a coação de eleitores conforme foi visto na Seção 2.2.3.

De fato esse tipo de sistema traz grande avanço nas pesquisas sobre SEVs, porém pode até ser empregado numa universidade, por exemplo, onde os eleitores eventualmente conseguem resistir a coação e saibam conferir a integridade do software, mas ainda não pode ser considerado como um modelo aplicável em eleições abertas de um país. Ainda assim, é importante frisar que existem alguns trabalhos que propõem e reforçam possíveis esquemas resistentes a coerção, como por exemplo, o descrito por Ben Adida em (ADIDA, 2009); o descrito por Martin Hirt e Kazue Sako em (HIRT, 2000) e o descrito por Tal Moran e Moni Naor em (MORAN, 2006)

2.6. SEVs ao redor do mundo

Conforme mencionado anteriormente, os Sistemas Eletrônicos de Votação vêm sendo utilizados e testados em diversos países ao redor do mundo, destacando-se, a Austrália, Alemanha, Argentina, Bélgica, Brasil, Canadá, Cazaquistão, Estônia, Finlândia, Filipinas, França, Holanda, Índia, Irlanda, Israel, Itália, Noruega, Romênia, Reino Unido e Suíça.

Um caso bastante conhecido é o da Holanda (JACOBS, 2009), que utilizou durante muitos anos as urnas DREs (Seção 2.4.2). Um relato interessante foi que, após a introdução desse modelo de votação no país, um grupo de ativistas contrários se reuniu e decidiu efetuar investigações para detectar possíveis problemas na segurança da urna. O grupo conseguiu revelar que essas máquinas

possuem graves problemas de segurança, onde, por exemplo, com apenas um minuto de acesso foi possível abri-las e substituir suas ROMs, possibilitando assim executar alterações no código do software da urna. Conseguiram também mostrar que houve problemas com o sigilo do voto onde alguém, com um receptor de rádio, seria capaz de descobrir como o eleitor votou. Devido a esses graves problemas e com uma forte campanha desses ativistas, a Holanda decidiu erradicar as urnas DREs e voltou a usar o sistema baseado em cédulas de papel.

Na Alemanha, a princípio também foi adotada a máquina de votação eletrônica de 1ª Geração (Seção 2.4.2), porém em uma decisão histórica, o Tribunal Constitucional decidiu que o eleitor teria o direito de entender porque e como seus votos estavam sendo contabilizados de forma íntegra, mesmo sem ter conhecimento especializado. Como essas máquinas só podem ser compreendidas por um programador e não têm nenhum tipo de transparência que permita aos eleitores verificar o seu registro de voto, o tribunal considerou ilegal o emprego das urnas DREs. Desde então a Alemanha já não usa votação através de DREs, retornando a utilizar as tradicionais cédulas de papel (Seção 2.4.1).

Outro país que adotou o voto eletrônico foi a África do Sul, onde na ocasião foram usados computadores no processo de contagem numa eleição histórica, ocorrida em 1994, e vencida por Nelson Mandela. Porém, durante o processo de tabulação dos votos um problema crítico foi notado. Alguém teve acesso à rede de computadores e alterou o processo de contagem dos votos, que acarretou na adição de votos para partidos da oposição. Essa foi claramente uma tentativa de fraudar o processo eleitoral num período muito frágil na história desse país. Possivelmente, esse problema não foi suficiente para mudar os resultados do sufrágio, mas poderia tê-lo arruinado, obrigando assim a realização de uma nova eleição.

Outro exemplo interessante de votação eletrônica é na Índia, onde a eleição de 2014 contou mais de 800 milhões de votos e quase todos os votos foram em máquinas eletrônicas, que naquele país são chamadas de EVMs (Electronic Voting Machines). A verdade é que a Índia usa mais de 1,4 milhões dessas máquinas em todo o país. Elas são fabricadas por empresas, que são de propriedade do governo indiano, elas são projetadas com características muito diferentes das máquinas de votação utilizadas nos EUA ou Europa.

No Brasil, temos um caso único e exclusivo, onde as urnas eletrônicas DREs sem papel, Figura 4, ainda são utilizadas em âmbito nacional (SCHOENMAKERS, 2000). No Capítulo 4 é detalhado todo o modelo de votação adotado pelo Brasil, como forma de justificativa para a proposta descrita no Capítulo 6.

Em relação à distribuição dos modelos correspondentes a cada geração, o pesquisador Amilcar Brunazo descreveu em (BRUNAZO, 2014), um relatório que realiza a identificação dessa distribuição ao redor do mundo, conforme representado no Quadro que segue.

Tradicional	**SEV - DRE**	**SEV - VVPAT**	**SEV - E2E**	**SEV – EVIV**
- Alemanha - Holanda - Irlanda - Inglaterra - Paraguai **Obs:** esses países erradicaram as urnas DREs	- Brasil	- Bélgica - Rússia - Irlanda - EUA - Canadá - México - Venezuela - Peru - Equador - Argentina	- EUA - Israel - Equador - Argentina	- Implementações acadêmicas

Quadro 5 – Atual distribuição dos modelos usados no mundo (BRUNAZO, 2014)

CAPÍTULO 3

"O conhecimento nos faz responsáveis."

Che Guevara

Análise de SEVs de 3ª Geração – E2E

Este capítulo contempla um estudo detalhado dos principais SEVs de 3ª geração, dando maior ênfase aos principais projetos de 3ª geração existentes atualmente ao redor do mundo, com o intuito de confrontá-los ao atual cenário brasileiro, no que diz respeito à evolução dos estudos para utilização de SEVs, em comparação as outras nações.

3.1. Princípio da independência do Software em SEVs

Para o melhor entendimento sobre a importância do desenvolvimento e emprego de Sistemas Eletrônicos de Votação de 3ª geração, deve-se entender o princípio da independência do software para esse tipo de sistema. Descrito pelos pesquisadores Ronald Rivest e Jonh Wack em 2006 (RIVEST, 2006), esse princípio têm como objetivo confrontar a problemática existente em se validar/certificar a confiança dos softwares instalados em urnas eletrônicas.

> *"Um sistema de votação é independente do software se uma modificação ou erro não detectado no seu software não pode causar uma modificação ou erro indetectável no resultado da eleição"*

Pode-se entender como um conceito que visa fornecer mecanismos para a detecção de erros ou fraudes ocorridas na apuração eletrônica dos votos, considerando inclusive a real possibilidade de sua ocorrência. Exige-se também que o voto do eleitor fique registrado em algum meio materializado que torne o

processo totalmente independente do software desenvolvido para uma urna eletrônica de votação.

Diferentemente dos equipamentos de votação desenvolvidos no resto do mundo, as urnas eletrônicas brasileiras utilizadas desde 2006 (Seção 4.1), realizam a autenticação do eleitor através da digitação do número da sua identificação eleitoral no próprio equipamento que colhe o seu voto, de forma que um eventual erro ou fraude não detectada no software pode resultar em quebra do sigilo do voto (PERES, 2008), ocorrendo, por exemplo, a partir de algum malware que grava a sequência de teclas digitas pelo eleitor. Além disso, um erro ou fralde ocorrida em qualquer outro processo possivelmente não pode ser detectado, visto que não há uma forma de auditar os registros de votação.

Antes mesmo de ser formalmente descrito em 2006, algumas iniciativas já eram propostas, como forma de garantir a independência do software em sistemas eleitorais. No Brasil, por exemplo, em 1998 o Fórum do Voto Eletrônico clamava pela adoção do voto impresso conferível pelo eleitor. Em 2000, a Ph.D. Rebecca Mercury (MERCURI, 2000), defendeu sua tese de doutorado com foco na importância dos sistemas de 3ª Geração (Seção 2.4.4), como forma de prover auditabilidade do resultado em SEVs. Em 2004, a Venezuela tornou-se pioneira na implantação em eleições oficiais de sistemas eleitorais de 2ª Geração (Seção 2.4.3), conhecidas como máquinas DRE (Seção 2.4.2) com capacidade de materialização do voto e atualmente utilizam um sistema que possibilita a verificabilidade do voto em várias instâncias do processo.

O Capítulo 6 deste trabalho visa apresentar um modelo que contemple a materialização do voto nas urnas brasileiras, como forma de garantir o princípio da independência de software em SEVs.

3.2. Por que verificabilidade E2E em eleições

Na incessante busca pelo aumento da segurança e confiabilidade dos seus sistemas eletrônicos de votação, muitos países têm apostado em dois princípios essenciais:

- **Princípio da publicidade:** Ser capaz de demonstrar que o resultado eleitoral foi correto. Isso significa que o conteúdo do voto tem de ser público

e conferível pelo eleitor no local de votação e pelo fiscal de partido durante a apuração.

- **Princípio do sigilo do voto:** Não possibilitar a identificação do autor do voto. É fundamental para se evitar a coação de eleitores, que é uma fraude com poder muito elevado de distorcer o resultado eleitoral.

Sistemas eletrônicos de votação com verificabilidade fim-a-fim (E2E) permitem que os eleitores auditem se seus votos são expressos como destinados, coletados como elencados, e contabilizados como recolhidos, ou seja, proporcionam uma apuração democrática capaz de ser conferida pela sociedade. Essencialmente, os sistemas de votação com verificabilidade prestam a garantia aos eleitores de que cada etapa da eleição funcionou corretamente. Ao mesmo tempo, os sistemas de votação devem proteger a privacidade do eleitor e evitar a possibilidade de influencia e coação eleitoral. Vários sistemas de votação com verificabilidade fim-a-fim têm sido propostos, geralmente variando em usabilidade e praticidade.

Normalmente, os sistemas de votação que empregam criptografia usam uma espécie de quadro de avisos público onde os funcionários eleitorais publicam informações que os eleitores e outros agentes envolvidos usam para o processo de verificação. No momento da votação, os eleitores podem, opcionalmente, receber um recibo de votação. Após os votos serem contados, os resultados e a verificação da informação são exibidos nesse mesmo quadro de avisos. Os eleitores podem então utilizar os seus comprovantes como forma de verificar se os seus votos foram recolhidos, conforme esperado, e qualquer partido de qualquer candidato pode verificar se o registro está correto em relação aos votos recolhidos. Se algum eleitor encontrar uma discrepância no resultado, ele tem algum tempo para um registro de impugnação, antes de o resultado ser validado. No Capítulo 6 vemos uma proposta que leva em consideração todas essas definições, sendo ela aplicada especificamente no sistema de votação brasileiro.

Mais formalmente, o que tem sido variavelmente chamado de E2E (do inglês, “End-to-End”, ou Fim-a-Fim), votos codificados, criptografia, ou auditoria de sistema abertos de voto, são os sistemas que preservam o sigilo eleitoral e que proporcionam:

- **Verificabilidade do eleitor:** Algum tempo depois de lançar o seu voto, cada eleitor pode confirmar que seu voto foi “recolhido como elencado”, verificando a preservação da privacidade de recepção da informação contra um registro público de recibos postados pelos funcionários eleitorais.
- **Verificabilidade universal:** Qualquer pessoa pode verificar que os votos foram “contados como recolhidos”, ou seja, a correspondência postada é correta com relação ao registro público dos recibos postados.

Com relação às eleições de auditoria aberta, há apenas um pequeno número de projetos relevantes, entre elas está detalhado a seguir alguns casos de eleições realizadas na atualidade que proporcionam a verificabilidade do voto e alguns sistemas que disponibilizam este requisito.

3.3. SEV Americano (Scantegrity II)

O Scantegrity II é um SEV proposto inicialmente por David Chaum, Aleksander Essex, Richard Carback, Alan Sherman, Jeremy Clark, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan e Emily Shen. Segundo descrito por seus autores em (CHAUM, 2008), trata-se de um sistema *open source* que faz uso de códigos de confirmação impressos com tinta especial invisível nas cédulas de votação, como forma de maximizar a integridade da eleição que utiliza sistemas de votação ópticos por escaneamento (Seção 2.4.3).

Foi utilizado pela primeira vez em novembro de 2009 em uma eleição de Takoma Park, no estado americano de Maryland, sendo empregado novamente em novembro de 2011 na mesma região.

O mecanismo do Scantegrity II baseia-se em duas etapas: 1) uma para o processo de votação; 2) uma para emissão de um recibo. Cada parte da cédula de votação é numerada com uma identificação idêntica, no entanto exclusiva. A primeira parte possui uma lista com os nomes dos candidatos elegíveis e uma bolha ao lado de cada nome que armazena um campo óptico de reconhecimento da marca, mecanismo usado em máquinas Precint Count Optical Scan (Seção 2.4.3), nesse campo o eleitor deverá marcar de acordo com a sua intenção de voto, além disso, cada bolha armazena uma sequência de caracteres alfanuméricos gerados de forma pseudoaleatória, chamados de código de confirmação,

impressos com tinta invisível ao olho nu. Na Figura 10 podemos ver um exemplo de impressão da cédula do sistema Scantegrity II.

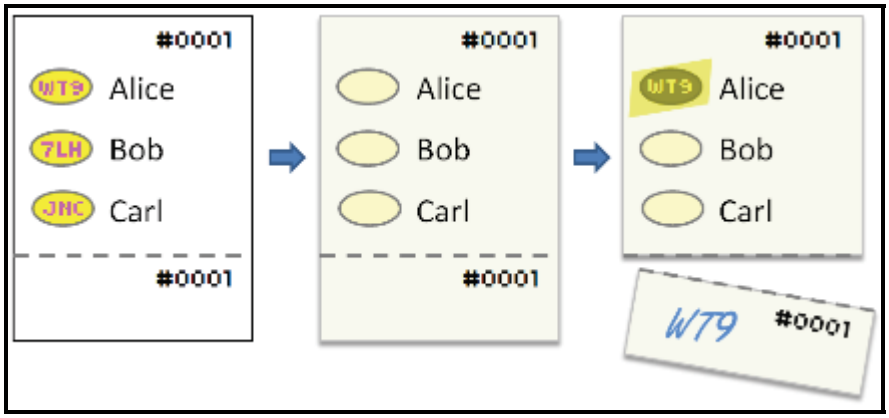

Figura 10 – Impressão especial realizada na cédula do sistema Scantegrity II (CHAUM, 2008)

No momento da votação, o eleitor recebe a cédula conforme visto na Figura 10 (centro); nessa etapa, a cédula ainda não deve revelar nenhum código de confirmação. Fazendo uso de uma caneta especial que é responsável por decodificar o segredo, ele define sua intenção de voto marcando a bolha correspondente ao candidato e, nesse momento, é revelado o código de confirmação, como pode ser visto na Figura 10 (direita). A marca feita com a caneta de tinta especial deixa a região mais escura, fazendo com que o escâner óptico a reconheça no momento do depósito da cédula, registrando assim o voto.

A parte que corresponde ao recibo pode ser destacada facilmente, devido a uma linha perfurada existente na cédula, e não afetando a leitura do escâner óptico. O recibo encontra-se na parte inferior da cédula conforme Figura 10 (direita) e é nele que o eleitor pode escrever o código de confirmação revelado após a marcação, como forma de verificação posterior.

Três características são exigidas ao processo de geração dos códigos de confirmação das cédulas de votação:

1) Devem ser únicos dentro de cada eleição em cada cédula de votação;
2) Para cada candidato, em cada disputa e em cada cédula, são selecionados de modo pseudoaleatorizado e independentes dentro do conjunto de códigos possíveis;
3) O código de confirmação correspondente ao candidato deve ser mantido em segredo para o eleitor até o momento de sua escolha.

Conforme descrito por David Chaum (CHAUM, 2008), o sistema funciona atendendo aos seguintes processos:

1) **Registro para votação:** O eleitor chega à seção eleitoral, confere-se então se o mesmo está regularizado perante o registro eleitoral, depois de autenticado é emitida uma cédula única que lhe é entregue juntamente com a caneta de tinta especial. O eleitor também tem a opção de solicitar uma segunda cédula para fins de auditoria, sendo possível a partir desta, verificar a regularidade dos códigos de confirmação impressos na cédula. Essa cédula é marcada como "voto de auditoria" pelos funcionários da seção eleitoral, como forma de garantir que o eleitor não vote duas vezes. É permitido ao eleitor levar essa cédula de votação, com objetivo de utilizá-la posteriormente em uma etapa de verificação;
2) **Processo de votação:** O eleitor entra na cabine secreta de votação e, usando a caneta especial, marca sua intenção de voto na cédula. Um funcionário da seção eleitoral auxilia o eleitor a introduzir a cédula marcada em um escâner óptico. O equipamento lê a identificação da cédula e a escolha do eleitor, menos o código de identificação;
3) **Criação do recibo:** O eleitor pode escolher por verificar o seu voto posteriormente em uma página Web criando um recibo de votação. Para tanto, o eleitor deve transcrever manualmente o código de confirmação revelado no momento da votação na parte inferior da sua cédula. O recibo deve ser marcado, em seguida, por um funcionário eleitoral como "cédula votada**"** e o eleitor destaca esta parte para uma posterior verificação.
4) **Verificação do voto:** O Scantegrity II provê um método para verificação do voto, como forma de revelar qualquer discrepância no resultado apresentado pelos registros públicos. A verificação ocorre em dois passos. Primeiro, o funcionário responsável pegará a cédula original em um invólucro que mostra o código de verificação, mas não o conteúdo da cédula. Então o destaque do eleitor é comparado com a cédula. Caso seja necessário, pode ser realizada uma análise forense para determinar se as fibras dos papéis conferem. A segunda parte deve revelar as letras das marcações na cédula, no entanto, sem que haja a possibilidade de revelar os candidatos associados. A cédula deve então se postada em um segundo invólucro, que

revelará as marcações, mas não mostrará os números de série. O responsável então anotará as posições das letras marcadas. O invólucro é depositado em um recipiente específico. Nesse momento são escolhidas outras cédulas falsas com as mesmas posições de letras, porém associadas a outros candidatos, sendo todas depositadas no mesmo recipiente. A caixa é misturada. Então cada invólucro é colocado a vista de todos. A cédula do eleitor estará misturada entre as outras. Assim, revela-se que a marcação feita é a mesma dos registros, tudo sem identificar o candidato da mesma. Através desse processo, qualquer contestação pode ser resolvida, visto que revelará se o erro ocorreu no leitor ótico ou pelo eleitor

O Scantegrity II apresenta uma série de vantagens ao processo eleitoral. O Quadro 6 mostra as principais vantagens e desafios do modelo.

Principais vantagens	**Principais desafios**
• Além das vantagens de um VVPAT, adiciona melhorias como: velocidade do resultado; possibilidade de auditoria por contagem das cédulas e o eleitor verifica se o voto é aceito na máquina; • O eleitor tem possibilidade de acompanhar todo o processo, com exceção da geração dos códigos de confirmação; • O eleitor mantém o sigilo do seu voto, pois o código de confirmação não revela sua identidade; • O eleitor pode escolher auditar a cédula de votação conferindo o código de confirmação; • O eleitor pode verificar o voto na web; • Qualquer pessoa pode conferir o resultado da eleição.	• O eleitor depende da forma como os códigos de confirmação são gerados, precisando confiar totalmente nos responsáveis por isso.

Quadro 6 – Vantagens e desafios do sistema Scantegrity II

3.4. SEV Americano (Helios Voting)

O sistema Helios Voting foi proposto por Ben Adida e C. Andrew Neff (ADIDA, 2006), e é considerado o primeiro sistema de votação E2E pela Internet, tendo sua primeira versão sido lançada no ano de 2008.

É um sistema *web-based* de código aberto, indicado para votações organizadas por qualquer organização, grupo ou comunidade e que faz uso de mecanismos que permitem auditoria aberta (*open-audit*), ou seja, cada eleitor pode auditar e verificar seu voto. Foi desenhado com base no modelo de Benaloh (BENALOH, 2006), utilizando recursos recentes de tecnologias web e técnicas criptográficas avançadas, com o intuito principal de assegurar a integridade dos votos e a privacidade do eleitor, levando em consideração um ambiente inseguro como a Internet, ao mesmo passo que, através de provas matemáticas, garante que a contagem dos votos é confiável.

Levando em conta que a integridade e a privacidade dos votos são consideradas como os principais propósitos do modelo, então mesmo que todo o sistema esteja corrompido ainda é possível verificar o seu funcionamento e, contando com um número significativo de auditores, torna-se quase impossível uma fraude passar despercebida. Para tanto, o *Helios Voting* implementa dois métodos que garantem a verificabilidade: 1) um que pode ser usado pelos eleitores como forma de verificar a consistência do voto entregue ao *Ballot Preparation System (BPS)*, imediatamente antes da submissão do voto; 2) outro que pode ser executado pelos administradores do sistema para verificar o mix dos votos, a decifra e a contagem da votação, que são produzidos pelo modelo de redes de misturadores e canais anônimos (Seção 5.1.2). Mesmo levando em conta que estes dois métodos focam nos eleitores e nos administradores do processo, todos os envolvidos podem auditar a eleição por completo fazendo uso de ambos os métodos descritos. Após a contagem dos votos, os administradores do pleito tornam pública a lista de eleitores associado ao resumo criptográfico (hash) do seu voto, tornando possível a verificação da corretude de seu voto. Esse modelo pode ser visto na Seção 5.1.8.

O sistema por definição utiliza recursos da técnica El Gamal (Seção 5.1.1) e implementam a propriedade da verificabilidade universal através de redes de misturadores verificáveis (Seção 5.1.2). O Helios também permite o uso de cifras de múltipla decifra (Seção 5.1.6).

Conforme descrito, o navegador web tem um sentido relevante para o funcionamento do Helios Voting, particularmente, todos os dados da eleição, o voto cifrado, o voto em claro e o fator de pseudoaleatoriedade, são armazenados no cache do navegador antes da efetivação do voto e uma parte essencial da aplicação cliente, o *Ballot Preparation System (BPS)*, é executado pelo navegador web através de Javascript.

Segundo Estehghari e Desmedt (ESTEHGHARI, 2010) o processo de votação é executado de acordo com as etapas a seguir:

1) O eleitor recebe por e-mail um convite para participação de uma eleição pelo administrador do pleito;
2) O eleitor utilizando um navegador web acessa o site da eleição e estabelece uma ligação com o BPS;
3) O eleitor interage diretamente com o BPS respondendo as perguntas feitas. As respostas dessas perguntas são enviadas para o BPS em claro através do navegador, antes do BPS as armazenar;
4) Antes de o BPS preparar o voto cifrado, é exibida ao eleitor a confirmação do seu voto, na qual o eleitor pode aceitá-lo ou ainda alterá-lo caso ache necessário;
5) No caso de haver a confirmação do voto, o BPS então cria o voto cifrado e mostra o hash do voto ao eleitor. Este pode escolher se deseja depositar o voto ou executar um processo de verificação da sua corretude:
    a) Se desejar depositar o voto, o BPS remove a informação necessária para criar o voto cifrado e solicita a autenticação do eleitor para garantir a elegibilidade. Em seguida, o voto cifrado é assinado pelo BPS, armazenado na base de dados e enviado para o e-mail cadastrado pelo eleitor, contendo a confirmação do seu voto, no caso o hash da eleição e do voto cifrado;
    b) Se optar por auditar o voto, o BPS então gera um voto auditado, que na sua formação de dados inclui o identificador da eleição, o voto em claro, o voto cifrado e a pseudoaleatoriedade utilizada para criar o voto da eleição. O eleitor, ao inserir um voto auditado no BPS, pode conferir os valores do resumo criptográfico da eleição, bem como confirmar que a cifra do voto foi verificada e que a prova está correta.

É necessário levar em conta que a criação de um voto cifrado é um processo anônimo e como tal, todos os interessados podem verificar a confiabilidade do *Ballot Preparation System (BPS)*. É importante ressaltar também que o Helios Voting não garante mecanismos de privacidade conforme descrito por Estehghari Desmedt (ESTEHGHARI, 2010), apenas a integridade dos votos e tanto o BPS quanto o terminal de preparação e depósito do voto precisam ser confiáveis para garantir a privacidade do eleitor.

3.5. SEV Argentino (Vot.ar)

No ano de 2011, a República Argentina empregou dois sistemas distintos para realizar o voto eletrônico: o sistema Point&Vote, utilizado na cidade de Buenos Aires e o Vot.ar, utilizado nas províncias de Chaco, Córdoba, Buenos Aires, Santa Fé e Salta, o primeiro trata-se de uma máquina fabricada pela empresa espanhola Indra e a segunda pela empresa argentina MAS.

Conforme descrito pelo *Comitê Multidisciplinar Independente (CMIND)* em (CMIND, 2011), ambas são consideradas máquinas de 2ª geração – VVPAT. Possuem uma tela sensível ao toque que é responsável por apresentar as opções para registro de votação, e ainda coletar as opções do eleitor. No trabalho mencionado também são apresentadas diferenças entre as máquinas mencionadas, trataremos de forma mais especifica da máquina Vot.ar, por apresentar diferenciais consideráveis de inovação para SEVs.

Segundo o site oficial do fabricante e relato apresentado pelo *CMIND* (CMIND, 2011), o equipamento Vot.ar possui uma arquitetura interna proprietária desenvolvida pelo seu fabricante. Montados em valises monobloco, com fonte de alimentação ininterrupta (No-break). Uma tela sensível ao toque, com leitores de CD e com uma impressora/leitora das Cédulas Eletrônicas do Voto (CEV). A tampa da valise, quando aberta, serve de anteparo para a tela/teclado. Em contra partida a máquina não conta com memória interna, por tanto, quando ocorre seu desligamento sua capacidade de armazenar votos ou a identificação do eleitor torna-se nula, o que inclusive evidencia a sua não classificação como uma máquina de 1ª geração – DRE.

A Célula Eletrônica do Voto (CEV), ilustrada nas Figuras 11 e 12, inicialmente chamada de Boleta Única Eletrônica (BUE), é responsável por armazenar o registro do voto através de um chip de radio frequência (RFID)

embarcado, além de servir como papel para impressão, tornando a CEV um agente de armazenamento eletrônico e impresso do voto. A Cédula Eletrônica de Votação é composta por:

1) **Face superior:** Dados e instruções impressas;
2) **Face inferior:** Papel térmico para impressão do voto;
3) **Parte interna:** Chip RFID de memória para registro do voto;
4) **Lateral:** Etiqueta numerada, bipartida e destacável.

Figura 11 – Cédula Eletrônica de Voto (CEV) (CMIND, 2011)

Figura 12 – Chip RFID de memória e impressora/leitora do chip (CMIND, 2011)

A máquina Vot.ar não necessita de uma preparação prévia, ou seja, não precisam ser alimentadas com informações e nem lacradas como ocorre com as máquinas de 1ª geração. O processo de inicialização ocorre de forma simples no dia da eleição, em que as máquinas são levantadas a partir de um CD-ROM igual para todas as outras máquinas, inclusive podendo este, ser retirado após o término do processo de inicialização. Ainda segundo o *CMIND* (CMIND, 2011), o processo de votação é executado de acordo com as seguintes etapas:

1) O eleitor se encaminha para sua seção eleitoral e apresenta o seu Documento Nacional de Identificação (DNI) para o mesário responsável. Este então verifica a autenticidade das informações contidas no documento. Após o processo de autenticação, o mesário assina na CEV inviolada, destaca uma parte da etiqueta numerada e entrega a cédula ao eleitor. A etiqueta destacada é armazenada junto da caderneta do eleitor para permitir futuras auditorias;

2) O eleitor vai até a máquina de votação e insere a CVE na parte da impressora/leitora, seguindo as instruções impressas no verso da cédula. Esse processo pode ser visto na Figura 13.

Figura 13 – Processo de inserção da CVE na impressora/leitora (CMIND, 2011)

3) Na tela da máquina são expostas as três opções de como o eleitor pode registrar seu voto. São elas: por categoria; lista completa de todos os candidatos ou voto em branco. Para selecionar a opção, o eleitor precisa basicamente tocar na foto do candidato ou navegar através da lista, ou então pressionar o botão de voto em branco;

4) Após a escolha, o sistema pergunta se o eleitor quer confirmar o voto, no caso afirmativo ele seleciona o botão “Sí”, caso contrário seleciona o botão “No”;

5) Após o voto ser registrado com sucesso, o eleitor dobra a CEV com o objetivo de ocultar a parte impressa, então ele volta para o mesário que solicita o destacamento da parte da etiqueta restante, como forma de

comparar com a outra que já havia sido destacada, se a conferência for positiva, elas serão prontamente descartadas. Em seguida o eleitor se dirige até a urna e realiza o depósito da CEV, neste momento sem etiquetas, e na presença dos mesários;

6) Finalizando o processo, o eleitor assina a lista impressa chamada "Folha de Votação" ao lado do seu nome, o mesário então carimba e assina uma folha na caderneta do eleitor e devolve a DNI.

O mecanismo de apuração dos votos é usado pelos próprios mesários na presença dos fiscais dentro da própria seção eleitoral, eles podem realizar a conferência do voto um a um, proporcionando um processo extremamente transparente às partes envolvidas. O resultado da apuração é então impresso e, em seguida enviado pela Internet para a central de totalização que efetua a contagem dos votos. Toda a operação é executada fazendo uso de protocolos seguros de comunicação (SSL). Em geral o Vot.ar apresenta uma série de vantagens ao processo eleitoral. No Quadro 7, estão descritas as principais vantagens e desafios desse modelo.

Principais vantagens	Principais desafios
• A apuração e totalização dos votos leva pouco tempo, bem semelhante às urnas DRE, ocorrendo geralmente em menos de 24 horas; • Transparência em quase todo o processo eleitoral, o que fornece maior grau de segurança ao sistema; • É um sistema que permite auditoria através da materialização do voto, necessitando apenas de uma amostra bem dimensionada; • O eleitor pode conferir se o voto está devidamente registrado na própria CEV antes de depositá-la; • Em caso de problemas físicos com a máquina, outra pode ocupar seu lugar instantaneamente, sendo apenas necessário carregar novamente o CD-ROM de boot.	• Possibilidade de adicionar CEVs fraudadas junto as originais, como forma de alterar a contagem dos votos, fazendo uso de uma fraude clássica conhecida como "Engravidamento de Urnas"; • O eleitor não pode verificar se o seu voto foi devidamente computado após a eleição.

Quadro 7 – Vantagens e desafios do sistema Vot.ar

3.6. SEV Israelense (Wombat)

O sistema Wombat nasceu de um projeto acadêmico, cujo objetivo principal é explorar e viabilizar o mecanismo de votação eletrônica com verificabilidade E2E. Além dos princípios básicos implementados para um SEV, esse sistema da maior ênfase aos recursos que favorecem a simplicidade e design do projeto, de acordo com os modelos mais tradicionais de votação.

O projeto foi, em sua grande maioria, desenvolvido pelos pesquisadores do Interdisciplinay Center (IDC), auxiliados por estudantes da Universidade de Tel Aviv. O sistema de redes de misturadores (Seção 5.1.2) utilizado pelo Wombat é baseado em um mecanismo chamado de Verificatum (WIKSTRON, 2011), e foi desenvolvido pelo pesquisador Douglas Wikstrom. Atualmente, o projeto é desenvolvido e mantido sob a liderança de Alon Rosen, Tashma Amnon, Riva Bem e Jonathan Bem-Nun.

No ano de 2012, esse sistema foi empregado oficialmente nas eleições para presidente e vice-presidente da união dos estudantes e para diretor da escolha no Interdisciplinay Center (IDC) em Herzliya Israel. Conforme descrito por Ralf Kusters, Tomaz Truderung e Andreas Vogt em (KÜSTERS, 2012), o sistema Wombat executa o seguinte processo para votação.

1) **Processo de identificação**: Primeiro, o eleitor entra no local oficial de votação e entrega o seu cartão de identificação para verificação. Nesse momento a comissão responsável pela votação analisa se o eleitor consta na lista de eleitores cadastrados e se o mesmo ainda não registrou seu voto. Se estiver tudo correto, a comissão eleitoral permite que o eleitor se dirija para a cabine de votação;
2) **Preparação do voto**: Nesse momento, o eleitor entra na cabine de votação e faz a seleção de seu voto numa tela sensível ao toque. A máquina de votar então imprime uma cédula que possui duas partes destacáveis: uma constando o voto em puro texto e outra em representada por um código de barra bidimensional *(QR Code)*, juntamente com um número de série. Na parte que consta o código QR, está representado o nome do candidato selecionado de forma encriptada, através do uso de um sistema de criptografia de chave pública: $Enc_{pk}(c,s)$, onde s é uma semente pseudoaleatória;

3) **Cédula para auditoria:** Nessa fase do processo, o eleitor opta em usar a cédula para votação ou para auditoria. Se a escolha for por não auditar, o eleitor deverá dobrar o voto sobre a parte que contém o puro texto impresso na cédula e então deixar a cabine de votação, dando prosseguimento à fase quatro do processo. No entanto, se a escolha for por auditar o processo, a máquina de votação demonstra como a cédula foi criada. Esse processo ocorre através da execução de um algoritmo que checa se a mensagem original e a mensagem encriptada que aparecem na cédula são compatíveis. Esse algoritmo pode ser executado ainda na estação de votação, ou posteriormente;
4) **Processo de verificação:** O eleitor deve verificar se a mensagem original coincide com a mensagem cifrada na cédula impressa na segunda etapa (Preparação do Voto). Se o resultado não for satisfatório, uma inconsistência é revelada e a máquina de votação é desqualificada. Caso a verificação for consistente, o eleitor retorna à etapa 2 (Preparação do Voto) para votar com outra cédula, pois uma cédula usada no processo de auditoria não pode ser utilizada como registro de voto;
5) **Processo de votação:** Nesse momento, o eleitor entrega a cédula dobrada para comissão responsável pela votação. Eles então marcam a cédula, a mensagem cifrada é digitalizada e publicada em uma página na Internet. Depois se destaca a cédula ao meio, dividindo a parte cifrada da parte original perante a comissão. A mensagem original é então lançada na urna e a parte cifrada fica com o eleitor como um recibo. Esse recibo materializado serve como objeto para verificar se o voto foi efetivamente codificado e armazenado na página Web.
6) **Fase de apuração dos votos:** Estando as seções eleitorais fechadas, inicia-se a apuração dos votos. O processo eletrônico de apuração é realizado publicamente na página Web e consiste em dois passos, considerando que todos os votos são envelopes e estão lacrados com um cadeado: 1) embaralhar de forma aleatória todos os envelopes lacrados na página Web, alterando seus cadeados ao mesmo tempo; 2) abrir todos os cadeados para que os envelopes embaralhados possam revelar a mensagem original.

No final deste processo, todos podem ler o conteúdo dos envelopes. No entanto, ninguém pode vincular os envelopes abertos os votos criptografados. Dessa forma, todos podem verificar os resultados da eleição, preservando a privacidade dos eleitores. Além disso, em posse dos recibos, o eleitor pode verificar o voto na página Web, bastando apenas digitar o código contido no recibo e constatar na tela um código associado ao voto. Esse mecanismo também preserva o sigilo do voto. As etapas básicas do processo de votação no sistema Wombat podem ser vistas na Figura 14.

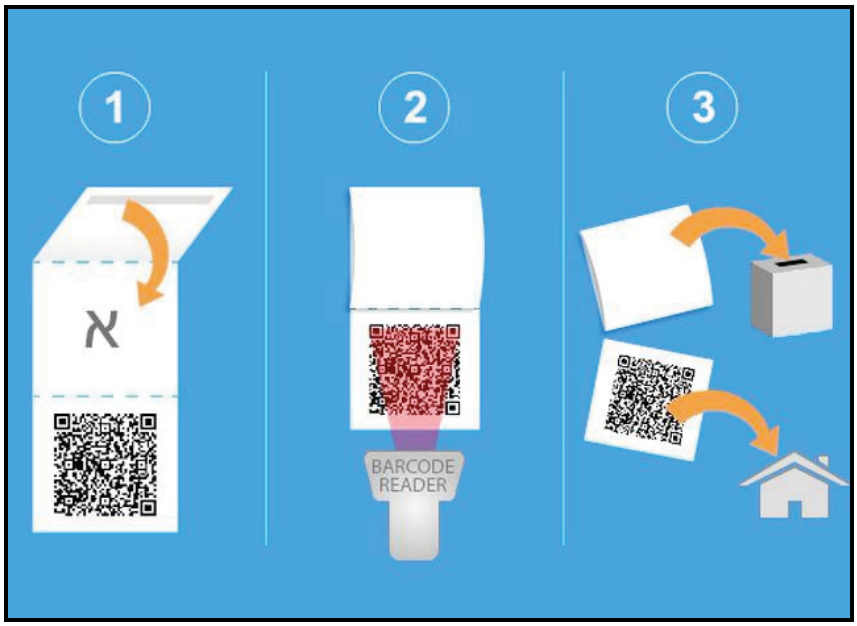

Figura 14 – Processo de votação no sistema Wombat

O sistema Wombat apresenta uma série de vantagens ao processo eleitoral. O Quadro 8 mostra as principais vantagens e desafios do modelo.

Principais vantagens	Principais desafios
• Permite auditoria por parte do eleitor na própria cédula; • O eleitor tem a possibilidade de verificar seu voto em uma página Web; • É fornecida a possibilidade de recontagem dos votos, pois parte da cédula é depositada em uma urna tradicional.	• É suscetível a ataques de colisão (Clash Attack). Conforme descrito em (KÜSTERS, 2012).

Quadro 8 – Vantagens e desafios do sistema Wombat

CAPÍTULO 4

"Só um sentido de invenção e uma necessidade intensa de criar levam o homem a revoltar-se, a descobrir e a descobrir-se com lucidez."

Pablo Picasso

O SEV Brasileiro

O Tribunal Superior Eleitoral (TSE) mantém e gerencia o sistema eleitoral brasileiro, tendo sua sede estabelecida na capital da República Federativa do Brasil (Brasília), conta com filiais operacionais distribuídas pelas federações nacionais, nas quais se dá o nome de Tribunal Regional Eleitoral (TRE).

É de responsabilidade de cada estado produzir auditoria, controle e fiscalização em seu território, primando sempre pelo perfeito andamento do sistema de votação, cadastramento e consolidação das eleições ocorridas a cada dois anos, respeitando a alternância de eleições para Prefeito e Vereadores e, em outro momento, para Deputados Estaduais, Deputados Federais, Senadores, Governadores e Presidente da República.

O sistema eleitoral brasileiro, ocorrendo de forma mais expressiva no período seguinte à redemocratização brasileira, levanta como centro de discussão e garantia de direitos, as definições a respeito da cidadania eleitoral. Em vários momentos na história das eleições, a democracia ligada ao direito de escolha de seus representantes tornou-se ofuscada por demandas centralizadas de grupos de interesse político minoritário, onde desenvolviam mecanismos que direcionavam o voto, popularmente conhecido como "Voto de Cabresto", em que por inserção de ameaças e coerção o eleitor era condicionado a votar em determinado representante popular.

No período que antecedeu o estado novo e no intermédio entre o término do regime do presidente Getúlio Vargas até o início do regime da ditadura militar de

1964, o sistema de votação era consideravelmente frágil, principalmente no que diz respeito às investidas para efetuar fraudes eleitorais, muito por conta da falta de maturidade no processo de logística como um todo e n o gerenciamento cadastral dos eleitores. Sem contar que as cédulas eram produzidas em papel, seguindo o modelo de sistemas de votação tradicional (Seção 2.4.1), o que oferecia grande facilidade na manipulação de resultados de um sufrágio.

Em marcos históricos do sistema eleitoral brasileiro, o voto não acontecia de forma secreta, levando a um cenário bastante favorável para manipulações de votos e resultados. Durante a construção da Justiça Eleitoral, seu quadro funcional era considerado deficitário, o sistema de fato só iniciou sua estruturação com maiores evidências quanto sua eficiência na década de 80, quando foram criadas equipes de trabalho preparadas para as atividades eleitorais, onde eram criteriosamente selecionadas e treinadas com o intuito de coibir a prática de fraudes ao sistema eleitoral. Durante essa época as eleições eram desenvolvidas com a participação de colaboradores designados pelos prefeitos dos municípios.

O papel conceitual de uma democracia necessita de um alicerce que apoie seu fortalecimento e sua fundamentação, para isso, a figura da Justiça Eleitoral em qualquer instância deve gerenciar e desenvolver mecanismos que estimulem a relevância da participação de uma população no processo eleitoral por completo.

Nas próximas seções, são abordados os principais componentes que formam o processo eleitoral brasileiro, incluindo os principais desafios de segurança que o SEV brasileiro precisa trabalhar.

4.1. A urna brasileira

Conforme descrito por Diego F. Aranha, Marcelo Monte Karam, André de Miranda, Felipe Scarel em (ARANHA, 2014), no ano de 1995, com a organização e criação de uma comissão técnica liderada por pesquisadores do Instituto Nacional de Pesquisas Espaciais (INPE) e do Centro de Telemática de Área (CTA), foi declarada uma especificação de requisitos funcionais para a primeira urna eletrônica brasileira, batizada então de Coletor Eletrônico de Votos (CEV).

A urna eletrônica brasileira é uma máquina responsável pela coleta e apuração dos votos, sendo fundamentalmente classificada como uma máquina de primeira geração do tipo *Direct Recording Electronic Voting (DRE)* (Seção 2.4.2), tendo em seu funcionamento características únicas de gravação eletrônica dos

votos, sem disponibilizar a materialização do voto através da impressão do voto para conferência do eleitor. Essa ultima característica, demonstra que a urna é um equipamento eleitoral cuja confiabilidade do resultado apurado está diretamente dependente da entrega de garantias técnicas do próprio software instalado nela.

Foi inicialmente desenvolvida pela Omnitech nos anos de 1995 e 1996. Depois, teve seu processo de fabricação Custódia do pela Unisys, uma empresa desenvolvedora de soluções em tecnologia da informação, que obteve essa permissão após participar de uma concorrência com duas outras empresas focadas em produtos que seguem linhas de produção totalmente diferentes, no caso a International Business Machines (IBM) e a Procomp. Na ocasião, a IBM sugeriu um projeto desenvolvido no Japão, baseado em um notebook; já a Procomp propôs a adaptação de um quiosque de autoatendimento bancário. A empresa vencedora da licitação forneceu a urna eletrônica modelo UE96, que foi posteriormente aperfeiçoada e se tornou o padrão brasileiro que é utilizado até os dias atuais no processo eleitoral.

As versões mais recentes, de 2006 a 2010, possuem mecanismos adicionais que permitem a identificação por biometria, entanto esse mecanismo ainda não atende uma lei que entrará em vigo em 2014, em que determina que a máquina de identificação do eleitor, não deve ter nenhum tipo de conexão com a urna eletrônica.

A primeira etapa do projeto-piloto para emprego da identificação biométrica na urna brasileira, foi realizada durante as eleições municipais de 2008, onde na oportunidade, o novo sistema foi testado em 100 urnas nas cidades de São João Batista (Santa Catarina), em Fátima do Sul (Mato Grosso do Sul) e Colorado D'Oeste (Rondônia). Em decorrência ao alto custo de aquisição dos equipamentos, essa sistemática está sendo adotada de forma gradativa.

É importante frisar que o mecanismo adotado na urna brasileira possui uma série de problemáticas, como por exemplo, a possibilidade do mesário liberar o voto por meio de senha próprio, como forma de solucionar um cenário de falso positivos. No entanto, isso vai de encontro ao objetivo inicial do projeto de biometria que era impedir que alguém pudesse votar em nome de outros, pois mantém aberta a possibilidade de executar a frade do mesário, que consiste na inserção de votos em nome de eleitores ausentes.

4.1.1. Componentes de hardware

No contexto funcional, a urna eletrônica brasileira segue a arquitetura computacional convencional, onde temos um computador (hardware) que roda softwares. Difere-se apenas em alguns componentes básicos, no caso: o terminal do eleitor, que é a urna propriamente dita e é também onde os eleitores registram suas intenções de voto; e o micro terminal, que é utilizado apenas pelos mesários para acompanhamento e controle da votação.

As urnas foram desenvolvidas seguindo diversos modelos empregados em cada eleição desde 1996. Geralmente, os modelos apresentaram a mesma arquitetura computacional de hardware, embora ainda ocorram algumas modificações em decorrência da evolução tecnológica. Os modelos de urnas já produzidos no Brasil foram: UE2000; UE2002; UE2006 e UE2009. A Figura 15 ilustra a visão traseira de uma urna UE2009.

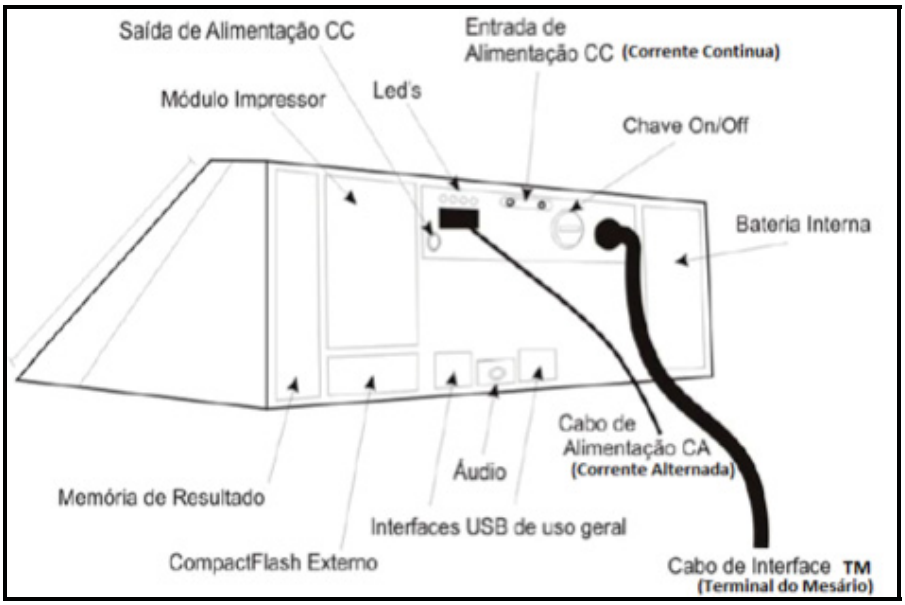

Figura 15 – Visão traseira da UE2009

4.1.2. Componentes de software

A urna eletrônica brasileira é composta pelos seguintes componentes de software: o sistema operacional; a aplicação com o nome dos candidatos e um módulo criptográfico de dados.

Todas as urnas empregadas em uma eleição possuem os mesmos componentes de software. O que diferencia uma urna da outra são os dados que são inseridos, como: município, zona e seção eleitoral; tabela de partido e

candidatos que disputam a eleição em tal seção; tabela de eleitores da seção e foto dos candidatos.

O primeiro modelo da urna (1996 até 2000) usava o sistema operacional Virtuosa que possibilita o compartilhamento do processador em um ambiente multiprogramado, ou seja, onde vários processos são realizados concorrentemente. Os modelos UE2002, UE2004 e UE2006 rodavam o sistema operacional Windows CE, um sistema com características fortes de impossibilidade de auditoria, principalmente em decorrência do seu tamanho, e por ser um sistema proprietário, seu código fonte possui módulos não conhecidos. A partir de 2008, todos os modelos passaram a empregar o sistema operacional Linux, o que apresentou um grande ganho para a arquitetura de software da urna, como: economia; transparência de processos e principalmente segurança, visto que por ser um sistema de código aberto, é plenamente possível realizar auditorias ao seu código.

4.2. Fases do processo de votação brasileiro

De modo geral um processo de votação convencional possui as seguintes etapas: 1) inicialização; 2) autenticação; 3) votação; 4) recolhimento dos votos; 5) contagem dos votos. O quadro a seguir descreve sucintamente o que ocorre em cada uma dessas etapas.

Etapa	Sistema tradicional	SEV
Inicialização	• Registro nos cadernos eleitorais • Elaboração dos boletins de votos	• O mesmo que o sistema tradicional • Geração de senhas • Distribuição de senhas
Autenticação	• Apresentação do cartão de eleitor e BI	• O mesmo que o sistema tradicional • Nome de utilizador e senhas • Algum mecanismo não tradicional de autenticação
Votação	• Marcação na cédula de votação	• Registro eletrônico do voto
Recolhimento dos votos	• Depósito dos votos na urna	• Envio eletrônico do voto
Contagem dos votos	• Contagem manual voto a voto	• Contagem eletrônica dos votos

Quadro 9 – Descrição geral das etapas de um processo de votação convencional

No caso do sistema brasileiro, esse processo é composto por fases específicas e possuem algumas características e semelhanças com o processo convencional. Nas seções a seguir estão detalhadas cada uma das fases específicas do sistema brasileiro.

4.2.1. Fase de alistamento

Conforme especificado no artigo 6º do Código Eleitoral, a fase de alistamento é obrigatória para todos os eleitores brasileiros, com exceção dos inválidos, os mais de setenta anos e os que se encontram fora do Brasil. Também é facultativo o alistamento para os analfabetos e os menores de 18 anos.

O ato de alistar-se tem o efeito de qualificação e inscrição do eleitor perante o órgão competente, no caso do Brasil, a Justiça Eleitoral. A qualificação é a comprovação de que o cidadão está legalmente apto a se alistar e participar da votação. De acordo com Benaloh (BENALOH, 2006), a inscrição é o registro do nome e dos dados do eleitor perante a Justiça Eleitoral. Na fase de alistamento, o eleitor adquire o titulo oficial eleitoral, que é a forma de comprovar que está apto a participar do processo de votação.

Para tornar-se apto à fase de alistamento, o eleitor precisa ir a um cartório eleitoral mais próximo, apresentar prova de identificação e do cumprimento das obrigações militares. Isso ocorre mediante apresentação dos seguintes documentos:

- Carteira de identidade;
- Certificado de cumprimento do serviço militar;
- Certidão de nascimento ou casamento;
- Comprovante de residência

Desde o ano de 2006, e mais fortemente esse ano (2013), está sendo implantada a tecnologia de biometria no sistema eleitoral, que inicialmente foi direcionada para três cidades específicas, depois atingindo 61 cidades e com prazo máximo de completude para 2014, conforme descrito em (ZMOGINSKI, 2010).

Esse modelo de alistamento através de sistema biométrico faz uso de um equipamento que registra duas digitais de cada mão, além da digital do polegar e

do dedo indicador. Esse sistema computacional é composto basicamente por um laptop, um scanner, um software especificamente desenvolvido para essa função e uma máquina fotográfica digital.

4.2.2. Fase de votação

Na fase de votação, 60 (sessenta) dias antes das eleições, o juiz responsável pela zona eleitoral designará os locais das seções eleitorais. Em cada seção deverá constar uma mesa receptora, composta de 06 (seis) mesários que são convocados e nomeados pelo juiz eleitoral.

Os componentes da mesa receptora também são escolhidos 60 (sessenta) dias antes das eleições. O processo de escolha usa critérios como: ser eleitores da seção correspondente; de preferência os que possuem curso superior, os professores e os servidores do Poder Judiciário. Segundo o Código Eleitoral – artigo 120, a mesa é composta por: um presidente; primeiro e segundo mesários; primeiro e segundo secretários e um suplente.

Pelo menos 72 (setenta e duas) horas antes da eleição, o presidente da mesa receptora recebe os documentos e equipamentos necessários para o desenvolvimento das atividades, todo o material é enviado pelo Juiz responsável pela zona eleitoral e se constitui em: cabine de votação; caderno de votação; as cédulas oficiais e uma urna eletrônica lacrada. Todo o processo eleitoral ocorre no primeiro domingo do mês de outubro, das 08 (oito) horas da manhã até às 05 (cinco) horas da tarde, no entanto os componentes da mesa receptora devem chegar às 07 (sete) horas (horário de Brasília), para providenciar o funcionamento da urna eletrônica e imprimir a “zerézima”.

A “zerézima” é um documento extremamente relevante ao processo de votação brasileiro, que deve ser emitido em cada seção eleitoral indicando que não existe nenhum voto registrado na urna. O órgão máximo responsável por todo processo eleitoral, no caso do Brasil o Tribunal Superior Eleitoral (TSE), usa esse documento como forma de garantir que não há registros de votos para nenhum dos candidatos, mas na prática o documento é composto apenas de uma lista contendo os nomes dos candidatos e quantos votos possuem como a fase de votação ainda não foi iniciada, é concludente que esse documento esteja zerado, por isso o nome de “zerézima”.

4.2.3. Fase de apuração dos votos

Exatamente às dezessete horas (horário de Brasília), o processo de votação é encerrado e começa então o processo de apuração dos votos que consiste em realizar a coleta de todos os votos da urna eletrônica. O presidente da mesa é responsável por enviar um comando do terminal da urna e ela fornece o resultado total da soma dos votos da seção e em seguida é impresso o Boletim da Urna (BU). Depois de impresso, o arquivo digital gerado pela urna é encriptado, gravado em uma mídia eletrônica, podendo ser um disquete ou pendrive e então é enviado para o cartório eleitoral.

Ao receber as mídias eletrônicas, o cartório responsável por cada seção eleitoral as envia através de uma rede privada de computadores (VPN) da Justiça Eleitoral para o TRE de cada estado. Esses dados são direcionados para uma máquina totalizadora do TRE.

4.2.4. Fase de totalização dos votos

Em posse dos dados, a máquina totalizadora realiza a verificação da procedência e correção das informações. Para tanto, ela verifica se o BU foi recebido de uma urna oficial, se a identificação confere com a mesma enviada para a seção de onde os dados foram enviados, se o BU foi gerado pelo software oficial da Justiça Eleitoral e utiliza-se de uma chave criptográfica secreta para decriptar o resultado transmitido.

Após a checagem da integridade de todos esses dados, a máquina totalizadora soma os resultados que foram transmitidos pelo cartório eleitoral. Se a eleição foi para governador, deputado estadual, deputado federal ou senador, então dá-se por encerrado a votação no Tribunal Regional Eleitoral (TRE) e o resultado segue para divulgação em um sistema do Tribunal Superior Eleitoral (TSE). Caso a eleição seja para presidente, as informações são transmitidas para o TSE, via rede privada de computadores (VPN). Ele recebe os dados de todos os TREs e realiza o mesmo procedimento de soma dos votos, sem a necessidade de chegar a integridade dos dados novamente. Por fim, o TSE finaliza a totalização da votação e envia para o seu sistema de divulgação. No caso das eleições serem a nível municipal, o responsável pela totalização dos votos é o Juiz Eleitoral e a Junta Eleitoral.

4.3. Desafios e recomendações de segurança para urna brasileira

Segundo relatório produzido pelo professor Diego Aranha e equipe (ARANHA, 2014), que apresenta uma análise de segurança do software da urna eletrônica brasileira, evidenciou-se diversas vulnerabilidades que possibilitam a recuperação em ordem dos votos computados. Na oportunidade, foram apresentados cenários onde as vulnerabilidades permitem a possibilidade de fraude no processo eleitoral. Ainda segundo o Diego Aranha e equipe (ARANHA, 2014), os principais problemas de projeto e/ou implementação de mecanismos de segurança do software da urna brasileira são:

1) **Proteção inadequada do sigilo do voto:** Os votos são armazenados fora de ordem, fazendo uso de um mecanismo elementar de embaralhamento de registros, no entanto é trivial recuperá-los na ordem correta a partir unicamente dos produtos públicos de uma eleição e conhecimento superficial do código-fonte, também de acesso público aos partidos políticos;
   Recomendações: Erradicar o Registro Digital do Voto e empregar um mecanismo que forneça a possibilidade real de verificação independente de resultados, como o voto impresso verificável pelo eleitor. Caso o registro digital seja constitucional, os autores recomendam no mínimo a eliminação das posições vazias do arquivo em seu formato final, como forma de dificultar a busca exaustiva no espaço de sementes possíveis.
2) **Cifragem inadequada:** A mesma chave criptográfica é utilizada para cifrar as mídias de todas as urnas eletrônicas. Fazendo uso de uma analogia clássica de um cadeado como abstração da técnica criptográfica, isto é equivalente a proteger meio milhão de cadeados com uma mesma chave, visto este ser o número aproximado de urnas em operação. Além disso, a chave que decifra todas as mídias é armazenada às claras na porção decifrada das mídias. Fazendo uso da mesma analogia, isto é equivalente a esconder a chave do cadeado embaixo do tapete e confiar no segredo dessa localização como fonte de segurança (segurança por obscuridade).
   Recomendações: Armazenar a chave de cifração no módulo de segurança em hardware ou, preferencialmente, em dispositivo criptográfico seguro externo ao ambiente da urna eletrônica.

3) **Utilização de algoritmos obsoletos:** A função de resumo criptográfico (Seção 5.1.8) SHA-1 empregada na urna, não oferece a segurança desejada para o software em verificação de integridade. Esta aplicação específica da função escolhida não é mais recomendada há pelo menos 6 (seis) anos.

   Recomendações: Fazer uso de um gerador de números pseudo-aleatórios de qualidade criptográfica e uma função de resumo criptográfico padronizada e resistente a colisões, como as pertencentes à família SHA-2. Em caso do comprimento da cadeia de caracteres produzidos como saída da função de resumo seja considerada crítica para a conferência, basta empregar uma função de resumo com segurança superior a necessária e trancar o resultado.

4) **Formulação equivocada do modelo de atacante:** Há ênfase demasiada apenas na existência de atacantes externos ao projeto de mecanismos resistentes, não levando em consideração a atuação interna de agentes maliciosos.

   Recomendações: Adotar mecanismos de segurança que resistam a agentes externos e, em particular, a agentes internos que os conhecem em seus mínimos detalhes.

5) **Processo de desenvolvimento defeituoso:** De encontro às boas práticas de segurança, o processo permite a inserção acidental ou maliciosa de vulnerabilidades ao projeto de software, sendo claro que o processo de desenvolvimento empregado pelo TSE é frágil do ponto de vista de segurança.

   Recomendações: Reduzir o volume de código a partir de técnicas de reuso e componentização. Evitar intervenções no código-fonte externo ao TSE e isolar as porções de código de sistema operacional e aplicação para facilitar a auditoria interna do software.

6) **Verificação insuficiente da integridade:** O software da urna verifica sua própria integridade durante o processo de inicialização, mas toda a informação necessária para subverter esse mecanismo encontra-se armazenada nas próprias urnas eletrônicas, com dificuldades distintas para um ataque, dependendo da presença do módulo de segurança em hardware. Em urnas sem esse recurso, o problema de verificação é reduzido a si próprio, sem fonte externa de confiança. Os autores também atentam a

versão do código observado, no qual apresenta como desativada a verificação da integridade por parte do software contido na urna, evidenciando as limitações intrínsecas da técnica.

Recomendações: Aplicar a verificação ativa do conteúdo da BIOS pelo módulo de segurança em hardware. De forma geral, recomenda-se transferir a pressão da verificação de integridade do software para a verificação independente dos resultados produzidos pelo software. Utilizar ferramentas sofisticadas de análise de código para minimizar o impacto de erros de programação que produzem vulnerabilidades, respeitando as boas práticas para desenvolvimento de software de missão crítica.

7) **Outros desafios:** Não obstante aos problemas técnicos apresentados em (ARANHA, 2014), a urna brasileira também sofre com os problemas intrínsecos a um projeto de máquinas de 1ª Geração – DRE (Seção 2.4.2), como: falsa ideia de segurança absoluta; dificuldade na análise e detecção de fraudes eleitorais; impossibilidade de materialização do voto, o que acarreta na falta de integridade ao processo eleitoral como todo; descarte da possibilidade de auditoria por parte do eleitor e auditoria universal; entre outros.

   Recomendações: Emprego de mecanismos que possibilitem a materialização do registro do voto, evoluindo o projeto da urna brasileira para uma urna de 3ª geração – E2E, como é proposto no modelo apresentado neste trabalho.

Outros pontos são relevantes no que diz respeito aos problemas existentes no modelo brasileiro de votação. Em um texto produzido pelo Prof. Walter Del Picchia em (DEL PICCHIA, 2014), são mencionados diversos argumentos, entre eles:

1) **Jurídicos que evidenciam a inadequação da urna eletrônica brasileira:** Estão defasadas, pois ainda são de primeira geração porque registram o voto apenas em via digital e, assim:
   - **a)** Não atendem o princípio da publicidade, que concede ao eleitor comum o direito de entender e conferir o processamento do seu voto;

b) Não atendem o princípio da independência do software (Seção 3.1), que diz que erros ou adulterações não detectadas no software não podem causar erros indetectáveis no resultado.

2) **Técnicos que demonstram a insegurança da urna eletrônica brasileira:**
   a) Adulterações nos programas podem provocar o desvio de votos sem deixar rastros;
   b) Adulterações nos programas podem permitir a identificação sistemática do voto (o número do título eleitoral é digitado na urna);
   c) É impossível verificar, na prática, se os programas das 400 mil urnas são corretos.
3) **São procedimentos insuficientes para garantir a segurança (passíveis de serem burlados):**
   a) Emissão da Zerézima (suposta demonstração de que a urna estaria sem votos);
   b) Votação Paralela (simulada) no dia da eleição;
   c) Auto-verificação de assinaturas digitais pelo próprio programa das urnas.
4) **A propaganda do TSE (Tribunal Superior Eleitoral) sobre suas próprias urnas eletrônicas:**
   a) Sistematicamente ignora e nega os inúmeros problemas ocorridos;
   b) Usa jargão que confunde o eleitor.
5) **Em relação à confiabilidade:**
   a) A urna eletrônica brasileira não permite conferência externa da apuração;
   b) O TSE impede uma investigação independente;
   c) O TSE mantém secretos relatórios que apontam falhas importantes.
6) **As urnas biométricas (com leitura da impressão digital do eleitor) também são inseguras:**
   a) Tem custo proibitivo (equipamentos, programas e conferências);
   b) Não impedem fraudes do mesário (colocar votos por eleitores ausentes);
   c) Não impedem a compra de abstenção ou de votos (feita com filmagem pelo celular);

d) Cria-se alguma dificuldade, mas não impedem o cadastro de eleitores fantasmas;

e) Não são aceitas em todo o mundo porque permanecem os riscos de violação sistemática de votos por manipulação do software

7) **Visão do exterior sobre a urna eletrônica brasileira:**

a) Foi rejeitada por TODOS os mais de 70 países que vieram conhecê-la;

b) Foi abandonada e até proibida em dezenas de países por não materializar o voto para conferência pelo eleitor (exemplo: Alemanha, Holanda, Reino Unido, Bélgica, Rússia, Índia, 40 estados dos EUA, Argentina, México, Equador, Venezuela e Paraguai);

c) Até o inventor da Assinatura Digital condena a ausência da materialização do voto.

8) **O TSE (Tribunal Superior Eleitoral) detém superpoderes. Em relação às eleições, ele:**

a) Executa/administra;

b) Legisla/regulamenta (a fiscalização permitida é feita sob-regras criadas pelo próprio fiscalizado);

c) Julga, muitas vezes ignorando as próprias regras;

d) Recebe as denúncias contra si mesmo (o administrador eleitoral);

e) Protela ou as arquiva;

f) Ou julga-se e absolve-se.

9) **Propostas para dar confiabilidade ao sistema eleitoral eletrônico brasileiro:**

a) Adotar a tripartição dos poderes no processo eleitoral, reservando ao TSE a função judiciária;

b) Adotar o princípio da Independência do software em sistemas eleitorais por meio do voto em papel (impresso ou escaneado) conferido pelo eleitor para permitir a auditoria independente da apuração eletrônica. Esse mecanismo é proposto neste trabalho no Capítulo 6;

c) Não identificar o eleitor na mesma máquina na qual ele vota.

CAPÍTULO 5

"O começo de todas as ciências é o espanto de as coisas serem o que são."

Aristóteles

Criptografia em SEVs

Definidos por Shannon em (SHANNON, 1949), os sistemas criptográficos convencionais são conhecidos como um conjunto de transformações unicamente inversíveis de mensagens em um conjunto de criptogramas. Cada transformação diz respeito a um processo de codificação com uma chave exclusiva, que deve ser transportada através de meios de comunicação protegidos contra interceptação da origem até o seu destino. O conjunto de transformações unicamente inversíveis serve para que a decriptação somente seja possível quando a chave for revelada.

Estudos voltados para a criptografia se constituem num dos principais agentes impulsionadores de pesquisas quanto à segurança de SEVs. Os grandes desafios de segurança desse tipo de sistema se entrelaçam em vários momentos com construções criptográficas, que tem como objetivo fornecer resultados reais e factíveis dos requisitos que visam garantir a segurança na utilização de sistemas eletrônicos de votação.

Nas seções a seguir são abordados os principais modelos criptográficos utilizados em projetos de SEVs, bem como o funcionamento da criptografia visual, que é um dos principais componentes deste trabalho.

5.1. Principais modelos criptográficos utilizados em SEVs

Os grandes desafios da atualidade para fornecer os principais requisitos (Seção 2.2) de um SEVs, tendem a amenizar os anseios de toda sociedade democrática, além de impulsionar diversos pesquisadores da área de computação,

em que se direcionam esforços para o desenvolvimento de métodos para a melhor implementação de SEVs.

O cenário atual favorece um ambiente de incertezas quanto à reputação dos SEVs, que está diretamente ligada a inúmeras dúvidas em relação aos resultados de uma eleição, além de não conhecer a fundo como esses sistemas são preparados para coibir fraudes através de software malicioso, por exemplo, que venha a sujar os alicerces de segurança, favorecendo assim algum candidato em especial. Dado esse cenário, torna-se notório a cobrança sob as autoridades eleitorais, que tem por obrigação agregarem transparência ao processo, seja através de auditorias ou mecanismos que possibilitem a averiguação de fraudes.

Na área de votação eletrônica, esses desafios têm como principal base de solução diversos modelos criptográficos, principalmente os esquemas que são descritos nas próximas seções.

5.1.1. ElGamal

O modelo de cifra El Gamal foi apresentado inicialmente em 1985 pelo pesquisador Taher Elgamal (ELGAMAL, 1985), e trata-se de uma construção direta do algoritmo de troca de chaves Diffie-Hellman (DIFFIE, 1976), tendo como base a sua segurança na utilização dos cálculos de logaritmos modulares de números grandes. O esquema descrito funciona basicamente segundo o Quadro 10.

Valores públicos	p α	Valor primo de grande dimensão Elemento primitivo módulo p
Chave Privada **Chave Pública**	a β	p > 0 $\alpha^a \bmod p$
Cifra	$C = \{c_1, c_2\}$	Valor aleatório secreto k < p -1 $c_1 = a^k \bmod p$ $c_2 = P \cdot \beta^k \bmod p$
Decifra	$P = c_2 \cdot (c^a{}_1)^{-1} \bmod p$	

Quadro 10 – Funcionamento básico do modelo de cifra El Gamal

Dada a complexidade intrínseca ao cálculo de logaritmos discretos de números com grandes dimensões, não é possível que de *β* consiga-se obter a chave privada *a* e que de c_1 consiga-se obter *k* em tempo rápido suficiente para que a informação cifrada ainda tenha valor. Dessa forma, o valor de *k* deve ser gerado de forma aleatória para cada cifra e, para não permitir sua divulgação,

deverá ser descartada logo em seguida. A decrifagem só poderá ser efetuada por quem conhecer $(c^{a}_{1})^{-1}$, sendo ainda necessário conhecer antes a chave privada *a*.

5.1.2. Redes de Misturadores e Canais Anônimos

Com objetivo de preservar as cédulas individuais e dar suporte na construção da escrita dos votos, os modelos criptográficos empregados em processos eleitorais fazem uso do anonimato das informações, e essa característica geralmente é fornecida por meio de modelos de redes de misturadores e canais anônimos.

O processo das redes de misturadores, inicialmente descrito por Chaum em (CHAUM, 1989), baseia-se no envio de mensagens com múltiplas cifras ainda no emissor, após isso a mensagem é enviada para o primeiro módulo mix, que, a partir da primeira cifra, ordena a mensagem; em seguida, a mensagem é enviada para o segundo módulo mix, onde, seguindo o mesmo princípio, utiliza a segunda cifra para obter a mensagem, e o processo se repete até que a mensagem chegue ao seu destino. Este modelo é amplamente utilizado em SEVs, com o principal objetivo de garantir o requisito da privacidade, pois o registro do voto é sempre computado de forma embaralhada e anônima.

O sistema Helios Voting (Seção 3.4), por exemplo, empregou o protocolo Sako-Kilian descrito por Kazue Sako e Joe Kilian em (SAKO, 1995), considerado o primeiro modelo de redes de misturadores baseada em re-encriptação El-Gamal. Segundo o mantenedor do projeto Helios, Ben Adida (ADIDA, 2008), este procedimento foi usado, apesar de existirem outros mecanismos mais complexos e robustos, por conta da sua simplicidade e facilidade de compreensão, propriedades que permitem atingir o objetivo final do projeto com melhor desempenho e sem infringir o requisito de integridade.

No caso dos canais anônimos, é possível que a partir do emissor seja possível enviar mensagens para o receptor, garantindo que esse último não consiga identificar o autor da mensagem. Nesse modelo, o emissor cifra apenas uma vez a mensagem correspondente à chave do primeiro módulo da rede de misturadores; este em seguida, decifra a mensagem e modifica-a com um identificador único. Após isso, a mesma mensagem é cifrada com a chave da próxima rede e repete-se este processo até que a mensagem chegue ao seu destino. Este modelo é semelhante a redes de misturadores, pois tem como

objetivo garantir a propriedade da privacidade, porém trata-se de um mecanismo mais robusto, pois disponibiliza a bi-direcionalidade. Em SEVs este modelo é geralmente desenvolvido para prover comunicação entre diferentes módulos do sistema eleitoral.

5.1.3. Assinatura cega

Tanto o anonimato do eleitor, quanto a qualidade de seu sufrágio, são propriedades extremamente sensíveis em um pleito eleitoral, pois não se admite sob hipótese alguma, efetuar a associação entre a intenção real do eleitor e a qualidade de seu voto. Uma fralde que explora a propriedade de anonimato do votante tende a oferecer recursos para a prática de comercialização dos votos e fere o requisito de incoercibilidade do eleitor (Seção 2.2.3).

Proposto pela primeira vez por David Chaum em (CHAUM, 1982) para emprego na área financeira e pelos pesquisadores Fujioka, Okamoto e Ohta em (FUJIOKA, 1992) para emprego na área de votação eletrônica, o esquema de assinaturas cegas permite que o usuário obtenha a assinatura digital de uma determinada entidade, sem que a mesma tenha conhecimento do que está assinando, sendo possível então conter informações que identifiquem o eleitor. Com base nesse esquema que garante a propriedade do anonimato, uma variedade de SEVs estão sendo projetados.

Para adquirirmos um entendimento global sobre o esquema, vamos exemplificar de forma didática e análoga, propondo o uso de duas folhas *X* e *Y* e um papel químico. Então supomos que Bob deseja que a entidade *A* assine cegamente a folha *X*, que está preenchida com informações. Desta forma, Bob coloca o papel químico sobre a folha *X* e o sobrepõe com a folha *Y*, e esse conjunto é entregue para a entidade *A* efetuar a assinatura. A entidade *A* então assina sobre a folha *Y* que está em branco e, portanto, não permite que *A* veja o conteúdo em *X*. A entidade *A* então devolve o conjunto para Bob e este retira a folha *Y* e o papel químico, passando a ter na folha *X*, a assinatura da entidade *A* por conta do papel químico que transferiu para a folha *X* a assinatura. Na Figura 16 é ilustrado o esquema empregado em assinaturas cegas.

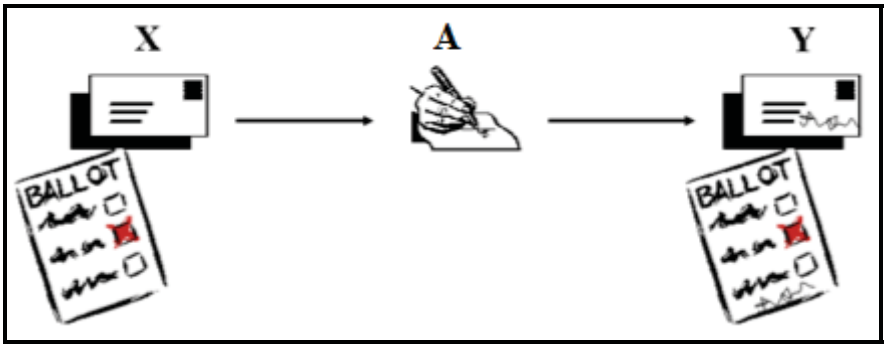

Figura 16 – Esquema empregado em assinaturas cegas

Quanto aos aspectos computacionais, e fazendo uso de criptografia assimétrica, a entidade A possui uma chave pública *e*, uma chave privada *d* e o módulo *n*. Bob envia uma mensagem *m* para ser assinada por *A*, mas antes adiciona um fator de cegamento aleatório *r* na mensagem, deixando-a com o seguinte formato: $msg = mr^e \ mod \ n$. A entidade A recebe a mensagem e a assina, retornando para Bob $msg^d = (mr^e) \ mod \ n$. Bob, ao receber, executa o processo de descegar msg^d usando $msg^d/r \ mod \ n$, que resulta em $m^d \ mod \ n$.

Nos modelos clássicos de SEVs, existe uma entidade responsável por controlar o número de vezes que os eleitores votam, garantindo assim a propriedade da democracia. Nos SEV baseados em assinaturas cegas (CHAUM, 1982) é natural que a entidade que faz este controle assine o voto do eleitor para depois verificar que este é válido. Este mecanismo permite a esses SEVs garantias quanto à propriedade da democracia, sem que haja quebra do sigilo do voto.

5.1.4. Cifra com recifra aleatória

O mecanismo de recifra aleatória possibilita que a partir da alteração de *M'*, a cifra de uma mensagem *M*, em *M''*, de forma que $M' \neq M''$ mas que a decifragem de *M''* é *M*. O esquema é detalhado a seguir e pode ser representado conforme Figura X.

$$C_k(M) = M' \rightarrow D_{k'}(M') = M$$
$$F(M') = M'' \rightarrow D_{k'}(M'') = M$$

Onde

K é a chave pública

K' é a chave privada

C_k é a função de cifra chaveada com a chave ***K***

$D_{k'}$ é a função de cifra chaveada com a chave ***K'***

F é a função de recifra

M é a mensagem em claro

M' é a mensagem cifrada que resulta da aplicação da função de cifra $C_{k'}$ ***a M***

M'' é a mensagem cifrada que resulta da aplicação da função ***F a M'***

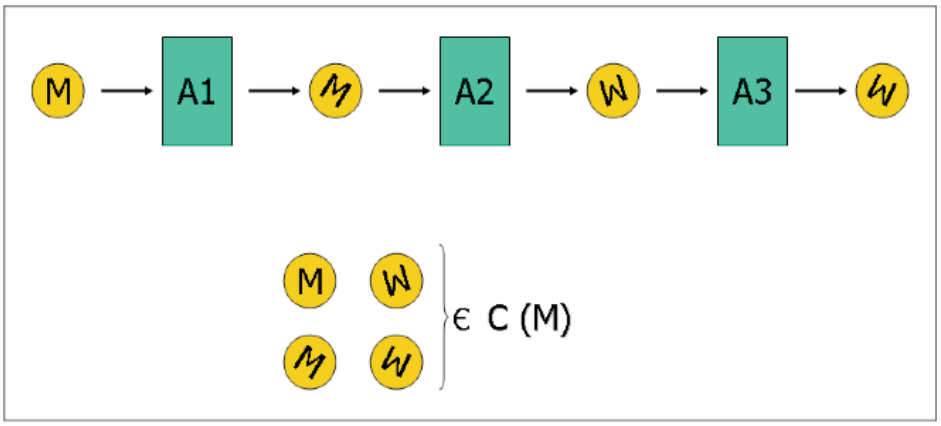

Figura 17 – Cifra com recifra aleatória

O emprego dessa técnica surge a partir da necessidade de introduzir maior entropia na geração das chaves, sendo que apenas o responsável pela geração da cifra sabe o seu conteúdo, podendo ser evidenciada através do sistema de prova de conhecimento nulo que é visto na próxima seção.

5.1.5. Prova de conhecimento zero

Os sistemas de prova de conhecimento zero foram introduzidos em 1985 por Goldwasser, Micali e Rackoff em (GOLDWASSER, 1989) e tornaram-se um dos conceitos mais relevantes na criptografia moderna. O método consiste em uma técnica criptográfica utilizada como um mecanismo para comprovação de que se conhece algo, mas que não seja possível revelá-lo. Um exemplo clássico encontrado na literatura para descrever o conceito é a gruta de Ali Baba.

O objetivo principal do exemplo é o Ali Baba comprovar ao seu amigo que conhece o segredo que lhe permite mover a pedra que bloqueia uma gruta. Ali Baba então entra na gruta sem que o amigo veja e escolhe um dos caminhos

possíveis, então o amigo da entrada da gruta pede ao Ali Baba para sair por um dos tuneis possíveis, esquerdo ou direito, se o Ali Baba sair por onde ele escolheu é dada então a prova de que o segredo é realmente conhecido. A ideia parte de que na primeira escolha a prova de conhecimento é parcial, visto que o amigo tem apenas 50% de certeza que Ali Baba conhece o segredo, no entanto o processo pode ser repetido várias vezes até que o mesmo fique convencido. A Figura 17 ilustra o modelo descrito.

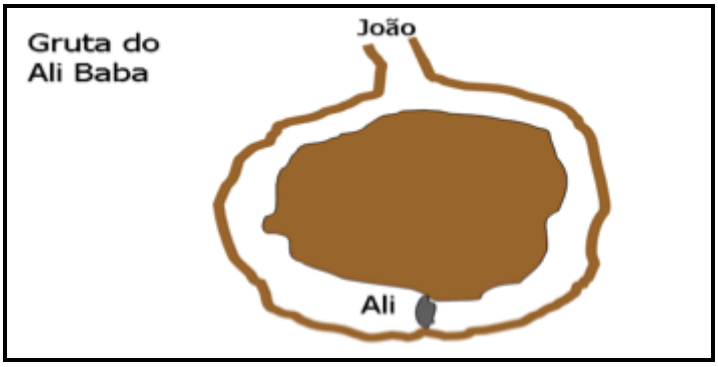

Figura 18 – A gruta do Ali Baba

Na prática, estas provas servem para garantir a correção de alguma confusão introduzida nos dados, como por exemplo, a cifra com recifra aleatória (Seção 5.1.4). Através desse mecanismo os SEVs conseguem garantir os requisitos de exatidão e verificabilidade do voto.

5.1.6. Cifra de múltipla decifra (*Threshold Decryption*)

Segundo Schilcher (SCHILCHER, 2004), a cifra de múltipla decifra consiste em um mecanismo que visa dispor de uma chave pública para a cifra de uma mensagem e, em vez de existir uma única chave privada, existem diversas. Ou seja, é gerada uma chave *(t, n)* em que *t* representa o número mínimo de partes da chave necessárias para realizar a decifra, e n consiste no número de partes da chave que são geradas. Dessa forma, uma mensagem cifrada pela chave pública só pode ser decifrada por quem possuir *t* partes da chave privada.

Geralmente esse esquema é empregado fazendo a distribuição das *n* partes da chave privada por *n* entidades diferentes, evitando assim que qualquer coligação de *t-1* entidades consiga efetuar a quebra da cifra e ter acesso à mensagem. A Figura 18 ilustra o esquema descrito.

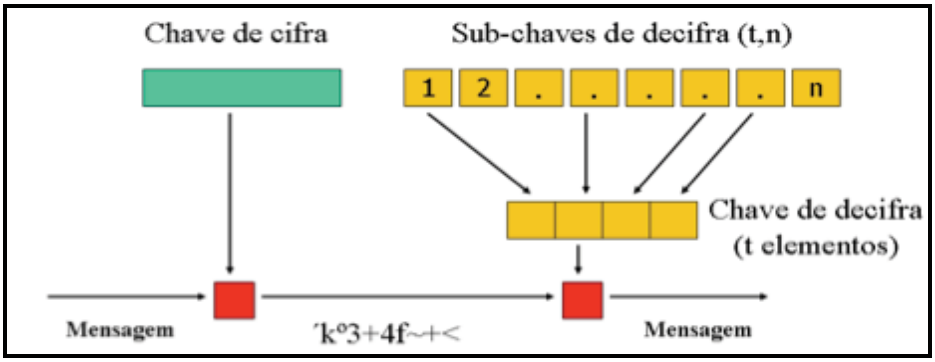

Figura 19 – Cifra de múltipla decifra (*Threshold Decryption*)

Os SEVs que utilizam esse mecanismo permitem a verificação e correção da contagem dos votos, pois existem combinações possíveis de entidades para decifrar os votos. Além de se empregar também uma maior proteção contra fuga de resultados parciais, visto que o agrupamento destes não depende só de uma entidade mais sim de *t* entidades.

5.1.7. Encriptação homomórfica

Descrita inicialmente por Rolf Haenni, Eric Dubuis e Ulrich em (HAENNI, 2008), o mecanismo de encriptação homomórfica baseia-se na aplicação de operações aritméticas a números cifrados sem que estes sejam decifrados previamente. O resultado final pode ser revelado a partir da decrifragem adotando uma chave privada, no entanto não possibilitando a decifragem dos números individualmente com essa mesma chave privada.

Uma função é dita homomórfica em relação às operações de multiplicação *"⊗"* e adição *"⊕"* se para todo o *x* e *y* temos:

$$f(x) \otimes f(y) = f(x \oplus y).$$

As funções de encriptação homomórfica, como por exemplo, a variação homomórfica da função de cifra ElGamal (Seção 5.1.1), podem ser empregadas para revelar o resultado de uma eleição sem revelar diretamente cada voto em si, assegurando dessa forma o requisito de anonimato do eleitor em relação ao seu voto.

Um exemplo da utilização desse mecanismo é descrito por Benaloh em (BENALOH, 2006), onde cada eleitor partilha uma fração do seu voto com diversas autoridades de voto, sendo que as frações devem ser cifradas com a chave pública

da autoridade receptora, autenticada, que publicará a fração. No final do processo de votação, as autoridades juntam as suas frações para gerar a apuração. Como forma de obter robustez no processo, é utilizado o esquema de encriptação homomórfica, onde são necessárias apenas *t* autoridades para combinar as suas frações e, então os resultados podem ser verificáveis universalmente.

O principal desafio na utilização deste tipo de cifra está na grande limitação ao formato dos boletins de voto, geralmente restritos a uma escolha “Sim” ou “Não”. A limitação ao número de candidatos que um voto deste formato possui é ultrapassada normalmente recorrendo a utilização de um voto Sim/Não por candidato, mas nunca ultrapassando a desvantagem de só possibilitar votos de um só bit. Outra limitação importante, é que embora estruturalmente simples, esse esquema possui um custo elevado em termos de comunicação, pois cada eleitor terá de submeter seu voto através de *n* canais.

5.1.8. Resumo criptográfico (*Hash*)

Uma função de resumo criptográfico (*Hash*) é uma transformação matemática que opera sobre uma mensagem de tamanho variável e produz um resultado de tamanho não variável (fixo). Esse tipo de função tem que ser unidirecional, ou seja, não deve ser factível inverter o resultado e obter a mensagem original. Embora seja uma função não injetora, onde mensagens diferentes podem gerar o mesmo resumo, uma função de hash deve garantir que seja muito custoso computacionalmente encontrar uma colisão.

Funções de hash utilizam basicamente operações de lógica booleana, deslocamentos e rotações, agindo de forma encadeada sobre os blocos gerados a partir da mensagem original.

Existem diversas implementações que empregam essa técnica, as mais usadas são o *Message-Digest Algotithm 5 (MD5)*, que gera como resultado um hash de 128 bits, e o *Secure Hash Algorithm (SHA)*, que produz hashes de 160 bits.

5.2. Criptografia visual

Proposta inicialmente por Naor e Shamir (NAOR, 1995), um sistema de criptografia visual (VCS) é um modelo que tem como diferencial a possibilidade de

executar a decriptação de mensagens sem que haja a necessidade do uso de um sistema computacional (hardware e software), todo o processo de decifragem é feito a partir da visão humana.

O esquema basicamente faz uso de um material (papel) para impressão do texto encriptado e outro material especial (papel) transparente, que servirá como chave. O processo de decriptação acontece quando ambas as partes são sobrepostas, o que possibilita a revelação da mensagem original. Muito embora haja ruídos no resultado da operação, torna-se tolerável, pois ainda assim qualquer pessoa capaz pode compreender a mensagem.

Como definição, a criptografia visual deve ser considerada um modelo especial de encriptação, que tem como objetivo esconder a informação em textos processados em imagens, e quando do uso da chave correta, torna-se possível a decriptação através do sistema visual humano. Na técnica proposta por Naor e Shamir (NAOR, 1995), o texto processado como imagem é separado em duas camadas distintas, o que torna possível a revelação do segredo, ou seja, sem uma das camadas é praticamente impossível obter o resultado correto. A forma mais trivial de desenvolver o modelo é realizando a impressão das duas camadas em material especial, no caso folhas transparentes. Podemos visualizar uma implementação simples escrita em Javascript desse modelo em (BAIRD, 2006), ou ainda baixar um Visual Crytography Kit para linguagem Python em (STAJANO, 1998). A Figura 19 ilustra um exemplo do mecanismo básico utilizado pelo método de criptografia visual.

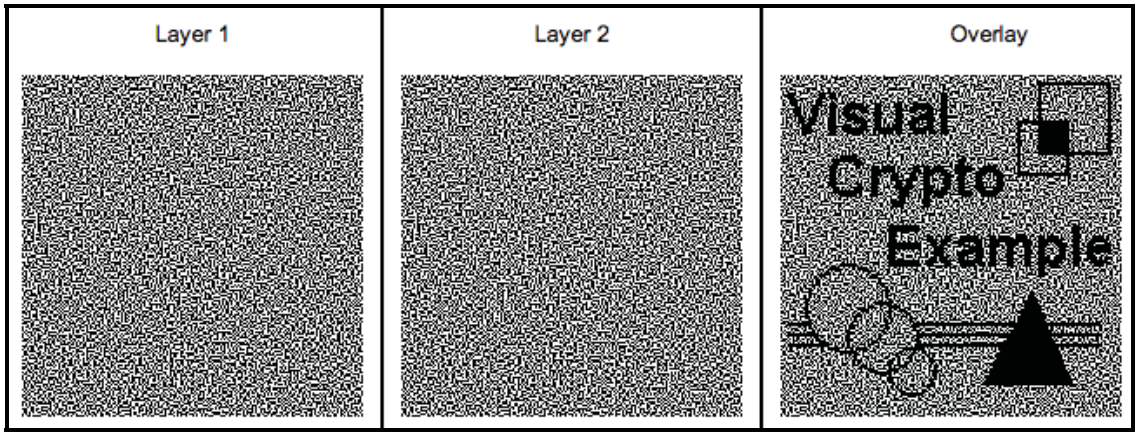

Figura 20 – Exemplo do mecanismo para criptografia visual

A criptografia visual tende a oferecer um nível considerável de segurança, dados outros modelos existentes, além de possuir um custo razoavelmente baixo de implementação. Outros sistemas criptográficos baseados em hardware e software, geralmente necessitam de maiores e caros recursos para executarem o processo de encriptação e decriptação de uma mensagem. Outra grande vantagem do modelo de criptografia visual sobre outros métodos é sua linha de aprendizado, na qual não se faz necessário conhecimento profundo em técnicas computacionais para cifragem e decifragem de dados.

Para uma melhor compreensão da criptografia visual, são descritos nas próximas seções os principais mecanismos existentes para construção do modelo (Secret Sharing; One-time Pad; Método de Naor e Shamir; Random Grids), além de tratarmos das principais aplicações da criptografia visual.

5.2.1. *Secret Sharing*

Proposto inicialmente por Adir Shamir em (SHAMIR, 1979), o método de compartilhamento de segredo, descreve uma solução para o problema proposto por Chung L. Liu em (SHAMIR, 1979), onde se imaginou hipoteticamente que, se onze cientistas trabalhassem no mesmo projeto secreto e se os mesmos desejassem trancar os documentos em um armário de tal forma que ele só poderia ser aberto se, e somente se, seis ou mais dos cientistas estivessem presentes. A solução sugerida pelo autor foi que para tanto o número mínimo de trancas seria 462 trancas e o número mínimo de chaves seria 252 para cada cientista.

Na prática, a solução proposta para o problema de Chung L. Liu (LIU, 1968) é totalmente inviável. Adir Shamir então propôs uma solução generalizada, usando uma abordagem criptográfica baseada em computação, onde: considerado *D* o dado secreto, então o dividimos em D_1, D_2, D_3, ..., Dn, de modo que: 1) o conhecimento de *k* ou mais pedaços D_i, permite que *D* seja computável com facilidade; 2) o conhecimento de *k-1* pedaços de *D*, permite que *D* seja totalmente indeterminado. Neste caso, os valores possíveis de *D* são igualmente prováveis;

Esse modelo ficou conhecido como *threshold scheme (k, n)*, em que se fundamenta no conceito de interpolação de polinômios, onde: dado um polinômio de grau *k-1*, *k* pontos distintos da função poderão ser usados para sua reconstrução. Dessa forma, *D* é selecionado para ser o termo constante do polinômio, enquanto os *k* pontos da função revelarão *D*.

5.2.2. *One-time Pad (OTP)*

O método de *One-time Pad (OTP)* é bastante simples e trata-se de um dos principais algoritmos de encriptação simétrica. A função básica da sua implementação trata-se de uma simples operação de Exclusive or (*XOR*) entre a chave e o texto que se deseja encriptar. A chave no caso precisa ser do mesmo tamanho que o texto e deve ser gerada a partir da seleção de uma cadeia de bits pseudoaleatórios. O tamanho da chave cria uma limitação ao mecanismo de *OTP*, no entanto se a chave for realmente mantida em segredo, gerada de forma pseudoaleatória e nunca reutilizada, o sistema pode garantir um nível alto de segurança.

Sugerindo que uma mensagem *M* deve ser cifrada pelo mecanismo *OTP*, então basta computar o *XOR* bit a bit com a chave *K*, gerando assim um cifrotexto *C*. Para a decifragem, basta realizar o calculo inverso da função, exemplo: para cifrar a mensagem: *C = M XOR K*; para decifrar a mensagem: *M = C XOR K = M XOR K XOR K = M*. A Figura 20 ilustra um exemplo do funcionamento de um mecanismo de *One-time Pad (OTP)*.

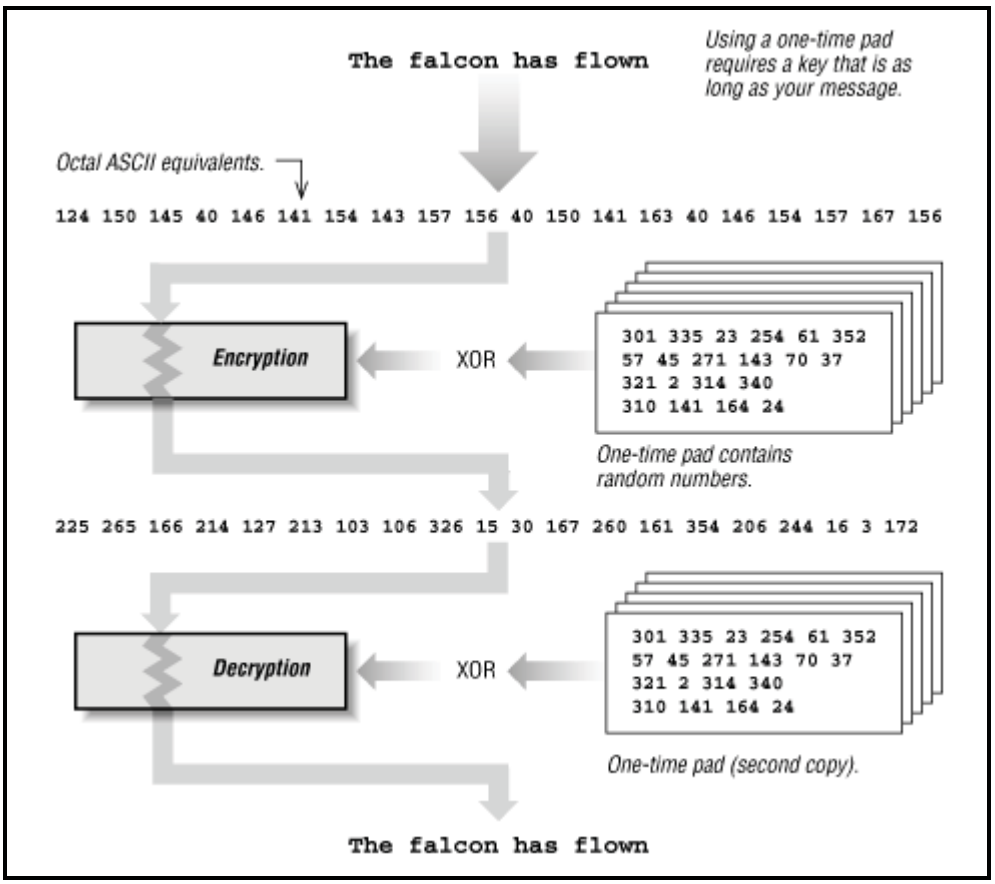

Figura 21 – Exemplo do funcionamento de um mecanismo OTP

5.2.3. O Método de Naor e Shamir

No método apresentado por Naor e Adi Shamir (NAOR, 1995), onde se demonstrou o emprego de duas camadas, onde: 1) uma das transparências apresenta o conteúdo encriptado que pode ser enviada através de correio ou até mesmo usando um aparelho de telecópia (fax); 2) a outra transparência serve como chave para decriptação do conteúdo cifrada na primeira. O conteúdo (purotexto) deve ser revelado quando da sobreposição de ambas as partes é executada. É importante lembrar que nenhuma das duas transparências pode revelar o conteúdo sobre a imagem impressa de forma isolada. O mecanismo é parecido com o one-time-pad (LIU, 1968), onde se utiliza um sistema criptográfico simétrico simples, em que a chave usada trata-se de uma string de bits pseudoaleatórios que deve possuir exatamente o mesmo tamanho da mensagem original. No caso do método proposto por Naor e Shamir (NAOR, 1995), o tamanho da mensagem também é do tamanho da chave, e ela é também é gerada pseudoaleatoriamente, e cada página de crifrotexto é decriptada com uma transparência diferente. Esse esquema também segue os princípios da *secret sharing* abordado em (SHAMIR, 1979), em que para se possa revelar o segredo, faz-se necessário pelo menos a participação de duas pessoas (partes distintas).

Tecnicamente esse modelo considera que a mensagem representada através de uma imagem, é uma coleção de pixels brancos e pretos. Cada pixel deve ser tratado separadamente e aparecerá de uma forma específica em cada uma das *n* transparências geradas. Cada transparência é uma coleção de m pixels pretos e brancos, em que são impressos muito próximos fazendo com que a visão humana realize uma média das contribuições individuais de cada pixel preto e branco, revelando assim o segredo. A construção básica é uma matriz *n x m* booleana $S = [s_{ij}]$, em que $s_{ij} = 1$ se, e somente se, o j-ésimo subpixel da i-ésima transparência é preto. Quando *k* transparências são sobrepostas de forma a posicionar alinhadamente os subpixels correspondentes, forma-se então uma imagem onde os subpixels pretos são representados pela operação “OR” das linhas correspondentes as *k* transparências na matriz *S*. Conjuntos de subpixels pretos e brancos posicionados muito próximos são interpretados com tons de cinza pelo sistema visual humano, com o nível de cinza sendo variável de acordo com a proporção dos pixels.

Ainda segundo Naor e Shamir (NAOR, 1995), a solução para o compartilhamento de segredos *k out of n* consiste em dois conjuntos C_0 e C_1 de matrizes booleanas. Para realizar o compartilhamento de um pixel branco seleciona-se, aleatoriamente, uma das matrizes de C_0 e para compartilhar um pixel preto seleciona-se, aleatoriamente, uma das matrizes de C_1. A matriz selecionada define a cor de *m* subpixels em cada uma das *n* transparências existentes.

Para qualquer subconjunto $\{i_1, i_2, \ldots i_q\}$ de $\{1, 2, \ldots n\}$ com $q < k$, as duas coleções de matrizes $q \times m$ D_t para $t \varepsilon \{0,1\}$ obtidas restringindo cada matriz $n \times m$ de C_t $(com\ t \varepsilon \{0,1\})$ as linhas $i_1, i_2, \ldots i_q$ são indistinguíveis. Esta construção garante que não é possível decidir se cada pixel é branco ou preto unindo menos de *k* transparências; ou seja, não é possível reconstruir o segredo com menos de *k* transparências.

Os autores (NAOR, 1995) também descreveram o problema da divisão do segredo em duas transparências, de forma que somente com ambas a partes seja possível revelar o segredo. A possibilidade de resolvê-lo baseia-se no mapeamento de cada pixel da imagem original em dois novos pixels em cada transparência, como podemos visualizar no Quadro 12. Esse método é conhecido como algoritmo *2 out of 2* de Naor e Shamir.

Pixel Original	Probabilidade	Subpixel 1	Subpixel 2	Subpixel 1 or Subpixel 2
□	0,5	■□	■□	■□
□	0,5	□■	□■	□■
■	0,5	■□	□■	■■
■	0,5	□■	■□	■■

Quadro 11 – Mapeamento da imagem original em 2 subpixels

O fato é que, no algoritmo *2 out of 2*, a encriptação faz com que o pixel fique esticada causando distorção do resultado final, portanto, é mais indicado processar cada pixel em um conjunto de quatro novos pixels em cada transparência, como podemos visualizar no Quadro 13.

Pixel Original	Probabilidade	Subpixel 1	Subpixel 2	Subpixel 1 or Subpixel 2
	0,5			
	0,5			
	0,5			
	0,5			

Quadro 12 – Mapeamento da imagem original em quatro subpixels

No momento da sobreposição das transparências, é executada a operação “OR” pixel a pixel, ou seja, o posicionamento de um pixel preto com qualquer outro pixel resultará sempre em um pixel preto e o posicionamento de dois pixels brancos retorna um pixel branco.

No processo ilustrado pelo Quadro 13, podemos ver que a imagem encriptada terá duas vezes o tamanho da imagem original, mas manterá suas proporções. É possível notar também que um pixel branco da imagem original após processado, se transforma em um conjunto de dois pixels brancos e dois pixels pretos na imagem encriptada. A partir de técnicas de pontilhamento, esse contraste de pixels aproximados tem a tonalidade cinza, fazendo com que a imagem encriptada seja compreendida pela visão humana. O ruído inserido na imagem encriptada garante a segurança do mecanismo, visto que de posse de apenas uma das transparências é comprovadamente impossível inferir da análise de um conjunto de pixels, o conjunto correspondente na imagem impressa.

5.2.4. *Random Grids*

No modelo de Naor e Shamir (NAOR, 1995), podemos evidenciar uma segurança significativa, além de ser um sistema eficaz, no entanto como o sistema baseia-se na expansão do pixel, é notória a necessidade de um tempo mais elevado de processamento e transição. Como uma alternativa a esse modelo existe os algoritmos baseados em *Random Grids*.

Proposto pelos pesquisadores Kafri e Keren (KAFRI, 1987), o algoritmo consiste na divisão da imagem *I* em duas transparências *T1* e *T2* com as mesmas dimensões de *I*. *T1* é uma coleção de bits pretos e brancos selecionados aleatoriamente, enquanto *T2* é construída a partir de *T1* e da imagem *I*. No caso de

um pixel de coordenadas *(i, j)* é branco em *I*, o pixel correspondente em *T2* será idêntico ao pixel da mesma coordenada de *T1*. No caso de um pixel de coordenadas *(i, j)* seja preto, os pixels correspondentes de *T1* e *T2* devem ser complementares. No formato geral, os pixels de *T1* e *T2* são selecionados conforme representação ilustrada no Quadro 14.

Pixel em I	Pixel em T_1	Probabilidade	Pixel em T_2	Pixel em T_1 or Pixel em T_2
□	□	0,5	□	□
□	■	0,5	■	■
■	□	0,5	■	■
■	■	0,5	□	■

Quadro 13 – Seleção dos pixels de T_2 de acordo com os pixels em I e T_1

Podemos ver que um pixel preto na imagem original *I* permanecerá preto ao se unir *T1* e *T2*, porém, um pixel branco em *I* se tornará preto em 50% das vezes, podendo gerar uma diferença expressiva entre *I* e a imagem gerada por *T1* e *T2* quando *I* possuir mais de 50% de pixels na cor branca.

5.2.5. Criptografia visual e suas aplicações

O emprego da criptografia visual em aplicações reais vem sendo proposto por diversos autores, que apresentam desde modelos conceituais até ideias práticas para a utilização do modelo. Além desses, empresas que desenvolvem produtos comerciais, começam a adotar a criptografia visual como mecanismo para garantir requisitos de projeto.

Uma das primeiras propostas da aplicação de criptografia visual foi com o intuito de prover garantias quanto à proteção de marcas, em que algumas empresas já adotam. No caso a empresa Trustcopy, situada em Cingapura, oferece alguns serviços, entre eles um serviço denominado Trustmark, desenvolvido para prevenir a falsificação, cópia ou outro tipo de uso não autorizado de marcas e produtos. Segundo a fabricante, o maior avanço tecnológico é o uso da marca d'agua com até 20 camadas encriptadas independentes e incorporadas no rótulo. Conforme descrito por Giuliano Marques, Vinicius Ribeiro e Jorge Zabadal em (MARQUES, 2008), a Trustcopy (www.trustcopy.com) faz uso de métodos de criptografia visual, como forma de não necessitar da utilização de software e

hardware para decriptar o segredo, facilitando assim o processo de autenticação. Tecnicamente o processo requer que o comprador utilize um mecanismo chamado *"Lens Key"*, que se trata de uma peça confeccionada em plástico e é usada como a chave impressa. Ao posicioná-la na área que contém a marca d'agua impressa no rótulo do produto, o segredo será revelado. A Figura 21 ilustra um exemplo do mecanismo implementado pela Trustcopy, aplicado em uma garrafa de uísque, onde o proprietário da marca pode autenticar o número de lote da produção, posicionando a "Lens Key" sobre a área invisível designada a marca d'agua.

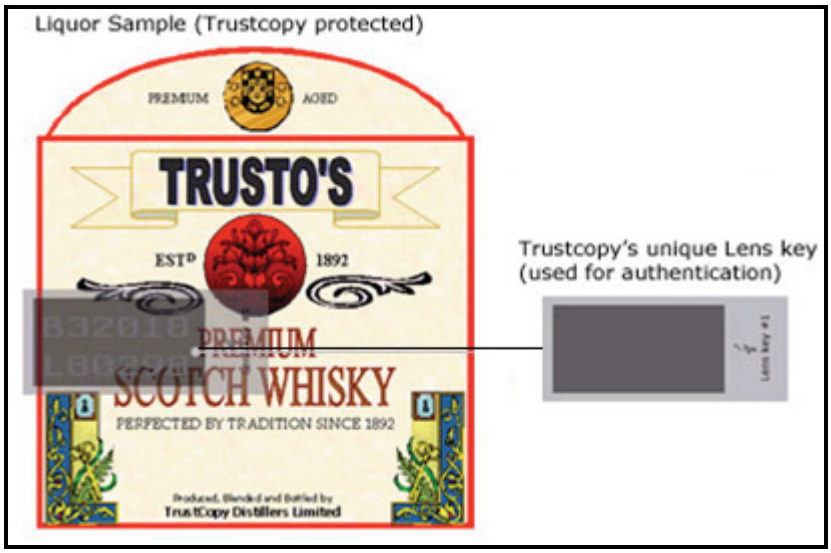

Figura 22 – Autenticação do número de um lote de fabricação pela Trustcopy (MARQUES, 2003)

Outra proposta relevante para utilização da criptografia visual é para autenticidade de documentos. Algumas empresas já desenvolvem este serviço, fornecendo uma solução que inclui um fluxo seguro de entrega de documentos, a partir de técnicas de anti-falsificação e anti-cópia.

A empresa Trustcopy (www.trustcopy.com) através do serviço denominado TrustDelivery oferece um serviço para autenticação de tickets, que prediz a compra on-line e impressa do bilhete. Como forma de evitar tickets eletrônicos falsificados, o sistema faz controle da impressão de forma que a numeração correta seja realizada apenas nos tickets originais.

5.2.6. Criptografia visual em SEVs

O pesquisador David Chaum foi o pioneiro em sugerir a aplicação da criptografia visual em SEV. O trabalho (CHAUM, 2002) descreve um sistema que

permite a verificabilidade do voto por parte do eleitor através da materialização do voto, sem que isso infrinja a propriedade do sigilo do voto.

O pesquisador propôs os seguintes mecanismos para o funcionamento do sistema:

1) O eleitor registra suas escolhas a partir de uma urna eletrônica, então é gerada uma impressão que será considerada como um recibo do voto. No recibo deve constar o nome do candidato selecionado, juntamente com a filiação partidária e o cargo que ele concorre. A impressão também pode incluir gráficos, da escolha manuscrita do eleitor, símbolos do partido, ou até fotografias dos candidatos. A Figura 22 ilustra um exemplo de um recibo gerado por esse mecanismo;

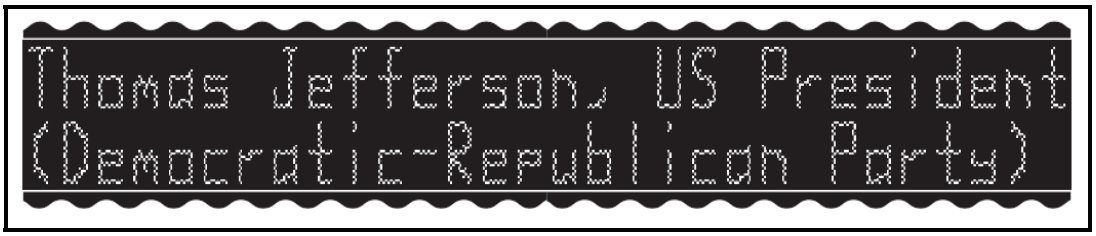

Figura 23 – Exemplo de recibo gerado pelo mecanismo sugerido por Chaum (CHAUM, 2002)

2) Após a impressão do voto, a máquina solicita uma verificação da impressão por parte do eleitor, que poderá aceitá-la ou não, no caso de uma negativa, o sistema dá a oportunidade de alterá-la e regera uma nova impressão;

3) No caso de haver a concordância com o voto impresso, a máquina solicita que o eleitor aponte qual das partes: superior ou inferior da camada será mantida como recibo. Esse mecanismo é necessário, pois a impressão é realizada nas duas camadas juntas e alinhadas, como pode ser visto na Figura 23. Após a escolha, o recibo é impresso.

Figura 24 – Impressão do recibo com as camadas juntas (CHAUM, 2002)

4) O eleitor então toma as duas camadas e as separa. A parte escolhida como recibo pode conter uma mensagem legível, como por exemplo: “Voter keeps this privacy-protected receipt layer”. Enquanto que a outra pode ter a mensagem: “Voter must surrender this layer to poll worker”. A Figura 24 ilustra um exemplo das camadas separadas.

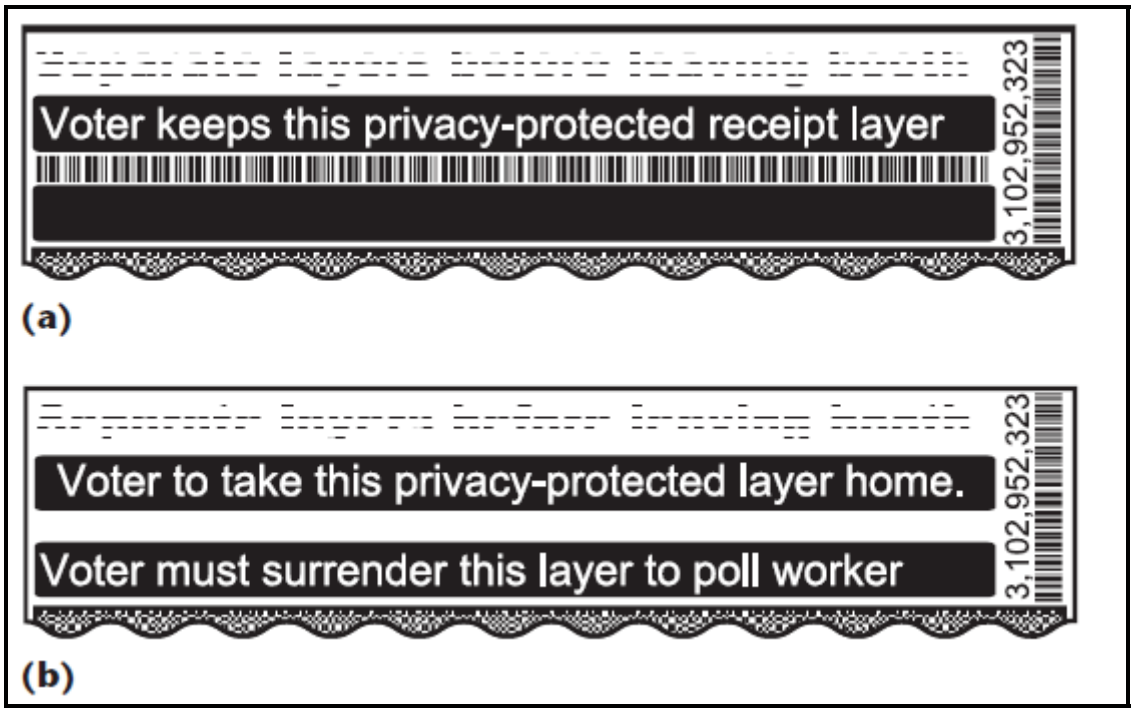

Figura 25 – Impressão das camadas. (a) Recibo que o eleitor retém; (b) Parte que é destruída

5) Antes de sair do local da votação, os agentes responsáveis pela seção eleitoral recebem uma das camadas e a destrói, enquanto a outra camada é levada pelo eleitor. O voto fica registrado eletronicamente na máquina e será transmitido via Internet para futuras verificações. Os bits na camada picada também devem ser “picados” por um processo eletrônico;

6) Ao término da votação, os votos digitais são enviados por um canal de comunicação de dados ou por mídias de armazenamento;

7) Após um período pré-determinado, o eleitor poderá verificar o seu voto em uma página Web disponibilizada pela instituição organizadora. Para tanto, deverá usar o número de identificação gerado na camada que está sob sua custódia.

Outra proposta relevante da aplicação de criptografia visual em sistemas de votação foi descrita por Nathanael Paul em (PAUL, 2003). Esse trabalho apresenta um sistema de votação via Internet fazendo uso de mecanismos de criptografia visual para autenticar o eleitor.

O sistema parte do princípio que os oficiais devem gerar as transparências encriptadas e as envia juntamente com uma lista de endereços de eleitores para um agente transporte, os correios, por exemplo, este órgão por sua vez envia para cada eleitor uma transparência selecionada aleatoriamente, em conjunto a um pacote de informações que incluem instruções de voto e uma senha. Em posse da encomenda, o eleitor acessa a página Web e digita a senha que recebeu; o sistema então solicita outras informações pessoais e, após a autenticação dos dados, o sistema apresenta na tela a outra parte da transparência, chamada de share. Nesse momento, o eleitor sobrepõe sua transparência na tela e a nova senha é revelada. Esse mecanismo garante a autenticação do eleitor que agora poderá efetuar seu voto. Além disso, os autores garantem que não ocorre aumento drástico no custo para realização de uma eleição. A Figura 25 mostra o funcionamento básico desse mecanismo.

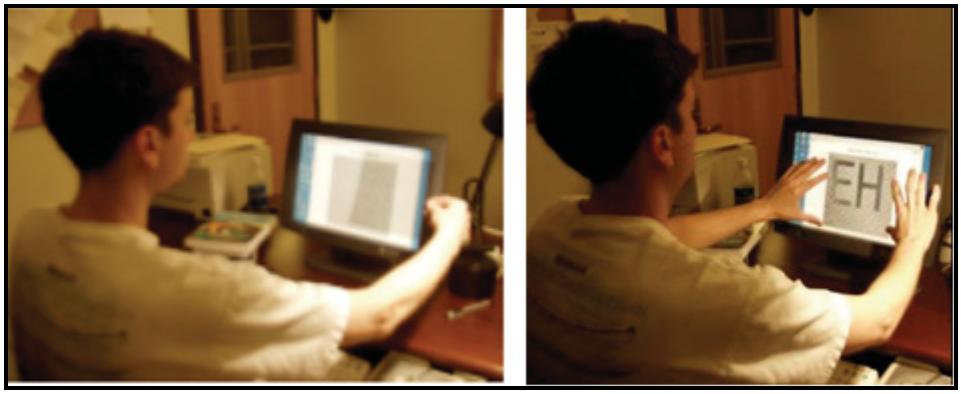

Figura 26 – Processo de sobreposição das transparências do sistema proposto em (PAUL, 2003)

5.2.7. Fraudes e prevenções em criptografia visual

É fato que qualquer informação considerada secreta pode se tornar confidencial a partir da aplicação da criptografia. Os sistemas criptográficos convencionais foram inicialmente descritos por Claude Shannon em (SHANNON, 1949), como um conjunto de transformações inversíveis de mensagens em um conjunto de criptogramas. Em que cada transformação obedece a um processo de

codificação usando uma chave específica. As transformações são inversíveis para que a decodificação seja possível a partir do conhecimento da chave.

Como complemento aos estudos sobre os sistemas criptográficos, que inicialmente demonstravam diversos padrões de cifras e métodos de decrifragem, Shannon descreveu a estrutura matemática e as propriedades desses sistemas, através de um artigo (SHANNON, 1949) considerado por Diffie e Hellman (DIFFIE, 1979) como essencial para o entendimento da criptografia, por descrever a base da teoria da informação para a criptoanálise clássica, além de distinguir os sistemas criptográficos perfeitos e detalhar a construção de alguns padrões de cifras.

A teoria de Claude Shannon (SHANNON, 1949) prevê que o criptoanalista possui capacidade computacional ilimitada. Por isso, Martin Hellman em (HELLMAN, 1977) considerou que o principal emprego desta teoria estaria no alcance de percepções qualitativas para o entendimento de sistemas criptográficos. Porém, ela não poderia ser diretamente aplicada na implementação prática de novos sistemas criptográficos. Em contraposição às definições de Martin Hellman (HELLMAN, 1977), o sistema criptográfico descrito por Felix Klein (KLEIN, 2003) é considerado pela *National Security Agency (NSA)* como um dos mais relevantes da história da criptografia e como um sistema perfeito, conforme a definição de Claude Shannon (SHANNON, 1949).

Ainda conforme Claude Shannon (SHANNON, 1949), cada chave usada no processo de proteção das informações deve ser transmitida sob canais seguros contra interceptação de terceiros da origem até o destino. A proteção das chaves usadas na encriptação de uma mensagem deve ser alcançada a partir da utilização de métodos especiais. Um sistema de armazenamento das chaves deve mantê-las em locais protegidos da memória, visto que incidentes podem ocasionar na perda da chave. É importante também manter outras cópias com entidades confiáveis ou em locais seguros. Frente à necessidade de armazenar de forma segura essas chaves, George Blakley (BLAKLEY, 1979) sugeriu a seguinte problemática: “se um determinado sistema de armazenamento de chaves gera múltiplas cópias, torna-se difícil evitar a perda. No entanto, se o sistema cria um número reduzido de cópias, todas poderão ser destruídas”.

Adir Shamir apresentou em (SHAMIR, 1979), uma forma viável de armazenar chaves criptográficas. No trabalho foi considerado que este é um desafio que está diretamente relacionado com o compartilhamento de um segredo

(Seção 5.2.1), que pode ser realizado através da divisão de um dado secreto *D* em n partes $D_1, ..., D_n$, de forma que o conhecimento de determinada quantidade $q >= k$ dessas partes tornaria *D* facilmente calculável, e plenamente indeterminado caso $q < k$. Este método foi definido pelo autor como um *Threshold Scheme (k, n)* e é ideal em aplicações compostas por um grupo de indivíduos paralelamente suspeitos, com interesses contraditórios, mas que devem cooperar entre si. Ou seja, um *Threshold Scheme (k, n)* é relevante quando alguma informação deve ser replicada ou dividida por *n* participantes ou locais, e protegida contra *k – 1* violações de segurança, devido à fragilidade dos dados ou desconfiança entre os participantes.

Com relação à fragilidade dos dados ou desconfiança entre os participantes, os pesquisadores Tompa e Woll em (TOMPA, 1989) acresceram a seguinte propriedade ao *Threshold Scheme (k, n)*, onde é real a possibilidade de que qualquer *k – 1* participantes $P_1, ..., P_{k-1}$ possam construir novas partes $D'_1, ..., D'_{k-1}$ com o objetivo de enganar o *k-ésimo* participante P_k. Determinar também que P_k foi enganado significa evidenciar que o dado secreto *D'*, reconstruído pela união das partes falsas $D'_1, ... D'_{k-1}$ e a parte original D_k, foi considerado legal, apesar de ser incorreto, visto que $D \neq D'$. Com a inclusão dessa propriedade, os autores (TOMPA, 1989) concluíram que o *Threshold Scheme (k, n)* é vulnerável a fraudes.

Dados os desafios e o cenário relatado acima, Naor e Shamir em (NAOR, 1995) desenvolveram uma abordagem visual da criptografia sobre o esquema *Threshold Scheme (k, n)* e definida por eles como *Visual Cryptography Scheme (k, n)*. Onde, a partir de uma imagem secreta, composta por pixels pretos e brancos, é possível gerar *n* transparências, de maneira que essa imagem se revela quando a quantidade $q >= k$ dessas transparências forem sobrepostas e plenamente indecifráveis caso $q < k$. Um trabalho relevante que descreve o relacionamento entre *Threshold Scheme (k, n)* e o *Visual Cryptography Scheme (k, n)* foi produzido por Stinson em (STINSON, 1999).

O *Visual Cryptography Scheme (2, 2)* é considerado a estrutura mais simples em Criptografia Visual e pode ser usada como um sistema criptográfico convencional na encriptação de materiais impressos como imagens, documentos e até textos escritos à mão. Um sistema baseado no *Visual Cryptography Scheme (2, 2)* é composto basicamente por uma página que contém a imagem impressa do criptograma e por uma transparência que constitui a imagem impressa da chave.

As imagens impressas na página e na transparência não definem, nem revelam qualquer informação sobre a imagem original, que pode ser reconstruída somente a partir de um processo de sobreposição das partes. Esse esquema apresenta grande simplicidade, pois pode ser usado por qualquer pessoa sem conhecimento prévio de mecanismos criptográficos e sem a utilização de qualquer tipo de componente computacional para efetuar a reconstrução do segredo, tão somente o sistema visual humano.

De acordo com Naor e Shamir em (NAOR, 1996), um *Visual Cryptography Scheme (k, n)* entrega a segurança incondicional, conforme as definições de Shannon em (SHANNON, 1949). A partir de um comparativo traçado com o sistema de Vernam descrito em (VERNAM, 1926), os autores chegaram à conclusão que a única diferença está na operação booleana empregada, onde um *Visual Cryptography Scheme (k, n)* se baseia na operação *OU*, enquanto a cifra de Vernam é baseada na operação *XOR.* Porém é possível notar que somente o *Visual Cryptography Scheme (2, 2)* oferece a segurança incondicional, definida por (SHANNON, 1949), visto que um *Visual Cryptography Scheme (k, n)* com outras configurações de *k e n*, mais especificamente quando *k = 2* e *n > 2* são consideradas vulneráveis a fraudes por (TOMPA, 1989) e aplicada no âmbito da criptografia visual por Gwoboa Horng, Tzungher Chen e Du-Shiau Tsai em (HORNG, 2006). Os autores validaram que *n – 1* participantes desonestos são capazes de fraudar a imagem secreta em um *Visual Cryptography Scheme (2, n > 2)* quando estes trabalham em conluio com o intuito de enganar o participante honesto.

Contudo a fraude pode ser evitada, se o *n-ésimo* participante for capaz de suspeitar que as transparências dos outros n – 1 participantes não são originais ou que a imagem revelada logo após a sobreposição das partes não é verdadeira. Ainda de acordo com (HORNG, 2006), a solução natural para o problema está no conceito de autenticação em Criptografia Visual, elaborado por Naor e Pinkas (NAOR, 1997), e conhecido como *Authentication Based Cheating Prevention Scheme (ABCPS)* e fornece aos participantes a possibilidade de validar a integridade das outras transparências antes que o processo de reconstrução do segredo seja realizado.

Podem-se compreender algumas vantagens e desafios em um *Authentication Based Cheating Prevention Scheme (ABCPS).*

Vantagens apresentadas por Cimato e Yang (CIMATO, 2011):

1) A verificação da integridade das transparências é opcional e pode ser efetuada apenas quando algum dos participantes suspeita de alguma fraude.
2) A geração das transparências de verificação deve ser efetuada após a geração das transparências originais. Por conta disso, qualquer estrutura de acesso pode se transformar num esquema de prevenção contra fraudes.

Desafios apresentadas por Cimato e Yang (CIMATO, 2011) e (LIU, 2011):

1) De acordo com (LIU, 2011), um *Authentication Based Cheating Prevention Scheme (ABCPS)* necessita de transparências extras para verificação, o que inevitavelmente causa um aumento de carga sobre os participantes.
2) Já conforme descrito em (CIMATO, 2011), não é possível realizar uma prova formal de segurança para o esquema.

Outros mecanismos também foram usados em esquemas de prevenção contra fraude. Entre eles o esquema descrito por Hu e Tzeng (HU, 2007) e Prisco e Santis (PRISCO, 2006), que sugere o aumento na expansão do pixel como forma de incorporar informações adicionais de autenticação. Num dos esquemas de (HORNG, 2006) gera-se um número maior que *n* transparências com o objetivo de reduzir o conhecimento que os participantes desonestos possuem referente à distribuição dos pixels na transparência da vítima.

Outra pesquisa relevante foi descrita por Tsai, Chenh e Horng (TSAI, 2007) onde foi desenvolvido um algoritmo genético para codificar imagens secretas homogêneas.

CAPÍTULO 6

"A menos que modifiquemos a nossa maneira de pensar, não seremos capazes de resolver os problemas causados pela forma como nos acostumamos a ver o mundo."

Albert Einstein

Modelo Proposto

Conforme descrito na Seção 5.2.6, o pesquisador David Chaum (CHAUM, 2002) foi o precursor em sugerir a aplicação de criptografia visual em Sistemas Eletrônicos de Votação (SEV) e após análise realizada nos esquemas propostos pelo autor, tornou-se possível conceber e sugerir uma implantação dessa técnica no sistema eletrônico de votação brasileiro, com o propósito de garantir maior transparência em todo o processo eleitoral para o principal ator desse sistema, o eleitor brasileiro.

A ideia global da proposta é fazer uso de um modelo que tem como objetivo específico assegurar as principais propriedades críticas de um SEV (Seção 2.2), enfatizando a aplicabilidade dos requisitos de: 1) verificabilidade do voto para o eleitor: onde algum tempo após o lançamento do voto, o mesmo pode confirmar se este foi "recolhido como elencado"; 2) verificabilidade universal: onde qualquer pessoa interessada no processo pode verificar que os votos foram "contados como recolhidos", ou seja, o registro processado através do software da urna é correto com relação ao registro público dos recibos postados em uma urna convencional.

Para atingir os requisitos citados, o modelo sugere basicamente mecanismos que proporcionam a materialização do voto através de sua impressão e sem que haja probabilidades mínimas de oferecer a quebra do sigilo do voto ou ainda favorecer a ação de um agente coercitivo com a intenção de comprometer um sufrágio através da compra de votos, por exemplo.

Um dos pontos altos da pesquisa está na evidência de que a partir da utilização das técnicas sugeridas por David Chaum (CHAUM, 2004) e Carlos Eduardo (SARAIVA, 2012), torna-se plenamente possível a conservação de quase todo o processo eleitoral já existente e empregado ao longo dos anos no Brasil, conforme foi descrito no Capítulo 4, fazendo com que a migração do processo ocorra com o menor trauma e desprendimento possível. Todos os ajustes propostos ocorreriam durante a fase de votação do processo eleitoral brasileiro, conforme visto na Seção 4.2.2, corroborando o menor impacto na operação, além de fornecer baixo acréscimo aos gastos eleitorais.

É importante frisar que o modelo proposto é apenas uma construção intelectual do processo e que ainda deve ser projetado, implementado, testado e implantado, seguindo as metodologias da engenharia e desenvolvimento de um software. Futuras pesquisas serão priorizadas, como forma de obter maior aprofundamento dos estudos e a contemplação de testes de prototipação e/ou implementação computacional desse modelo.

6.1. Trabalhos relacionados

Os Sistemas Eletrônicos de Votação surgiram como opção aos sistemas tradicionais, no entanto, uma série de problemas de seguranças vem sendo evidenciados ao longo dos anos, lançando assim severas desconfianças quanto à pura e simples informatização de um processo eleitoral.

Na América e Europa, por exemplo, órgãos governamentais e civis vêm buscando organizar diversos eventos, com o intuito de impulsionar as pesquisas de soluções que aprimoram o uso de um sistema de votação em seus países, no sentido de mitigar possíveis vulnerabilidades e ameaças, além de fornecer mecanismos que disponibilizam os requisitos de um projeto de SEV.

Entre as principais propostas de SEV, pode-se citar o idealizado por Peter Ryan (RYAN, 2009), denominado *Prêt à Voter.* Esse sistema é considerado um sistema de votação E2E e, têm como principal objetivo, fornecer garantias na contagem de votos sem que haja a quebra do sigilo do voto, atendendo ao princípio da independência do software (Seção 3.1). Em particular o sistema *Prêt à Voter* permite que os eleitores possam confirmar que seu voto foi corretamente contabilizado durante a contagem e, fazendo isso sem que haja a possibilidade da atuação de uma agente coercitivo.

Sua ideia chave está cunhada na codificação do voto usando listas aleatórias de candidatos. O *mix* da lista de candidatos em cada boletim de voto, garante o sigilo do voto e também elimina a probabilidade da fixação de uma ordem dos candidatos dentro da cédula.

O valor impresso na parte inferior do recibo é a chave para a extração da votação. A criptografia aplicada neste valor é a informação necessária para reconstruir a ordem dos candidatos e assim obter o voto codificado no recibo. Essas informações são devidamente encriptadas com as chaves secretas compartilhadas através de um número de caixas. Dessa forma, somente o conjunto de contadores que atuam juntos são capazes de revelar o voto codificado. O método garante que nenhum agente individual ou qualquer máquina envolvida no processo possa ligar um eleitor a um voto decriptado em particular. Logo após a eleição, os eleitores ou representantes podem verificar o *Web Bulletin Board (WBB)* e confirmar se seus registros aparecem corretamente.

Conforme descrito por Ron Rivest e equipe em (RIVEST, 2007), foi possível propor um modelo que fornece uma contraprova do voto, utilizando um sistema de votação tradicional (Seção 2.4.1) baseado em papel com o uso de três cédulas idênticas, em que os candidatos são apresentados em linhas organizadas pelo cargo. Na frente da identificação de cada candidato, há um círculo para marcação do voto, e este pode ser lido por um sistema de leitura óptica.

Para selecionar o candidato pretendido, o eleitor deve marcar o círculo da identificação do candidato em duas das três cédulas. Os outros candidatos não selecionados receberão uma marcação aleatória única em uma das três cédulas. Esse procedimento deve então ser repetido para os demais cargos existentes na cédula.

Após o preenchimento das cédulas, o eleitor deve entregá-las ao mesário responsável, que submeterá as cédulas para validação de um equipamento do tipo *Mark Sense*, onde dispositivos sonoros indicarão se a cédula está preenchida dentro do padrão esperado. Caso esteja tudo correto com o preenchimento, o eleitor poderá receber a cópia de qualquer uma das cédulas como seu recibo de votação. Então, o equipamento que verifica as cédulas, fixará uma tarja vermelha no rodapé da cédula escolhida, cobrindo assim a área em que está o ID da cédula, indicando que a cédula já foi usada.

O processo de depósito das cédulas na urna é realizado logo após a divisão das cédulas. Salientando que a máquina de validação não mantém nenhum registro desse processo, tão somente informa o preenchimento correto da cédula, podendo também gerar uma autenticação e imprimir o recibo.

Ao fim do processo de votação, o eleitor poderá conferir via Internet se o seu voto foi computado no processo de apuração, efetuando a comparação da cédula que levou consigo como contraprova do voto, com uma cópia da mesma publicada no boletim de votos apurados na Web. A partir disso, é possível verificar se a qualidade do voto e o ID da cédula conferem.

É fato que esse sistema agrega condições de auditoria por parte do eleitor e terceiros, visto que a lista de votantes é divulgada em conjunto com a contraprova do voto. Esse mecanismo permite ao eleitor validar a contagem do seu voto dentro da totalização. No entanto, há desvantagens herdadas pelo modelo, relacionadas principalmente ao uso de um sistema tradicional (Seção 2.4.1). É factível que a proposta do autor pode ser implementada, mas corre o risco de não fornecer grande agilidade ao processo de votação manual, levando em consideração também que no sistema brasileiro existe um grande número de cargos, o que deixaria a cédula de votação extremamente grande.

Roberto Araújo em (ARAUJO, 2010), descreve um protocolo para verificabilidade do voto baseado em Farnel. No trabalho em questão, os autores apresentam uma nova versão do sistema de votação Farnel (DEVEGILI, 2001); um sistema eletrônico de votação que fornece componentes para materialização do voto. Além disso, os autores enfatizam uma falha existente no esquema *ThreeBallot* apresentado acima (RIVEST, 2007).

O esquema introduz uma nova maneira de verificar o voto, onde: o eleitor não verifica seu próprio voto, mas copias de um subconjunto dos votos lançados até o momento. Mais precisamente, o eleitor recebe cópias de alguns IDs de voto. Estes são utilizados mais tarde para realizar uma comparação com os IDs das cédulas publicados no quadro de boletim dos votos.

A versão em papel usa uma cédula em formato simples. Exigindo apenas que o eleitor compare identificações e marque as opções existentes. Porém, o esquema depende de uma caixa de cédulas que executará o embaralhamento das cópias dos IDs. Além disso, a segurança do sistema depende dos parâmetros de voto.

No caso, os autores usaram uma versão em papel para modelo a versão eletrônica. O trabalho atingiu o esperado pela equipe, no entanto, acabou não sendo prático e gerou alguns inconvenientes, pois requer componentes adicionais, como por exemplo, uma urna especial para executar a mistura corretamente. Além disso, o eleitor deve comparar um monte de informações.

David Chaum em (CHAUM, 2004) também propôs um modelo de SEV que fornece ao eleitor um recibo como contraprova do seu voto. Diferente do modelo sugerido anteriormente, este se trata de um esquema plenamente direcionado para Sistemas Eletrônicos de Votação (SEV) e realiza encriptação da cédula através de funções baseadas em criptografia visual (NAOR, 1995).

O modelo proposto (CHAUM, 2004) leva em consideração os seguintes aspectos:

1) A área da cédula em que o eleitor vota, é composta por duas faces, a frontal e a de fundo, sendo ambas produzidas em material especial de plástico transparente;
2) O registro do voto é impresso em ambas as faces da cédula, empregando a técnica de criptografia visual propostas por Naor e Shamir (Seção 5.2.3). No momento em que as faces são sobrepostas de forma alinhada, é possível visualizar o voto em texto claro;
3) A visualização das faces separadas não revela a qualidade do voto do eleitor em decorrência do processo criptográfico usado;
4) A contraprova do voto é dada pela cópia de uma das faces que o eleitor escolherá.

Para que seja possível existir a contraprova do voto, o eleitor deverá escolher entre uma das faces que será levada como recibo, a outra parte deverá ser destruída pela Autoridade Eleitoral na presença do mesmo. A partir da escolha do eleitor, o sistema imprime em cada face informações representando qual a face selecionada e qual face que deverá ser destruída.

Logo após a votação, a conferência do recibo é realizada a partir da publicação dos resultados na Internet, onde é divulgada uma cópia idêntica do recibo, fornecendo ainda ao eleitor a impressão desse recibo e possibilitando o alinhamento das partes, de forma a verificar se os pixels pretos formam a imagem

ou texto do recibo que o mesmo possui. Ressaltado ainda que o ID da cédula também deve ser validado.

A grande vantagem do modelo é, sem dúvida, pelo fato da contraprova ser baseada em algoritmos de criptografia visual, o que reflete diretamente na dificuldade da construção de fraudes eleitorais, que visam comprometer a integridade do sistema. Mesmo se tratando de um recibo codificado e que permite a revelação da informação do voto, o uso de múltiplas chaves para a decodificação (faces da cédula) inviabiliza qualquer tentativa de quebra do processo criptográfico usado, além de garantir o sigilo do voto.

Embora com todas suas vantagens, podem-se citar pontos negativos ao modelo, como: 1) a necessidade do uso de uma impressora e material de impressão não convencional, que acaba por aumentar os custos de uma eleição; 2) uma das faces, a que não foi escolhida pelo eleitor, deve ser descartada ainda no local da votação por algum sistema de destruição do papel ou algo similar, como forma de garantir que não ocorra a reconstrução do recibo. Porém, se o sistema de descarte utilizado for falho, a reconstituição do material pode ser realizada. Além disso, a necessidade de manter um equipamento como esse em cada seção, pode causar aumento nos custos de uma eleição.

Outro trabalho relevante foi descrito por C.E.R. Saraiva em (SARAIVA, 2012), onde foi enfatizado o entendimento detalhado de todo o processo eleitoral brasileiro, como forma de evidenciar possíveis desafios ao SEV desse país, ocorrendo desde as fases preliminares de preparação até a apuração e totalização dos votos. Pode-se ressaltar também o estudo aprimorado dos esquemas de criptografia visual realizados pelo autor, com o objetivo de sugeri-los como forte componente às possíveis soluções dos desafios da urna brasileira.

Ainda segundo o autor, o principal ganho desse trabalho está na análise realizada sobre as fases de alistamento, votação e apuração/totalização dos votos. Bem como a aplicação de esquemas de criptografia visual no sistema eletrônico brasileiro, ocorrendo apenas durante a fase de votação e contando com o acréscimo de uma auditoria eleitoral:

O trabalho (SARAIVA, 2012) sugere as seguintes mudanças no sistema brasileiro:

- **Na votação:** O eleitor continuaria utilizando a mesma urna eletrônica, procedendo normalmente com a escolha dos candidatos, no entanto, depois do registro, o mesmo poderia optar pela impressão do voto em duas cédulas. O processo é semelhante ao sugerido por (CHAUM, 2004), ou seja, teria uma parte transparente com as opções do candidato encriptadas com funções de criptografia visual e um número de identificação. Além disso, uma região em branco para receber uma marca oficial, como forma de prevenir fraudes eleitorais. Após a impressão das cédulas, o eleitor realizaria a conferência do seu voto, sobrepondo alinhadamente as cédulas. No caso de haver discrepância, ele então cancelaria o seu voto e o registraria novamente; em caso positivo, ele depositaria uma das cédulas numa urna tradicional e a outra seria levada ao mesário para receber a marca oficial.
- **Autenticação:** No trabalho também foi sugerido uma forma de adicionar autenticação ao processo, onde a cédula poderia ser dividida em nove áreas distintas, sendo possível escolher em qual delas seria impresso o voto, bastando o eleitor digitar no próprio teclado numérico da urna, um número variando entre 1 e 9 correspondente ao espaço na cédula;
- **Auditoria:** O processo de auditoria sugerido pelo autor ocorreria dias após as eleições, em um período pré-definido pelo TSE. No dia escolhido, uma empresa ficaria responsável pela conferência dos lacres na presença de terceiros. Após isso, os votos seriam retirados das urnas tradicionais e colocados em ordem numérica por seção e entregues aos eleitores. Estes, por sua vez, seriam encaminhados ao local de conferência, portando a cédula (comprovante). Após efetuar sua identificação e receberem a outra parte da cédula, iriam até um local seguro e executariam sobreposição das partes, realizando assim a conferência do voto. Em seguida, depositariam as partes unidas em uma urna para auditada do processo, a ser executada pelos oficiais eleitorais em outro momento e na presença de terceiros.

Ainda conforme (SARAIVA, 2012), o modelo apresenta uma série de vantagens e desafios, começando pelo aumento dos gastos eleitorais como já havia sido enfatizado em (CHAUM, 2004). No entanto, os ganhos da aplicação de criptografia visual no sistema eletrônico de votação brasileiro são visíveis,

principalmente no que diz respeito à transparência do processo, sem que ocorram possibilidades da quebra do sigilo do voto.

6.2. O emprego da criptografia visual no SEV brasileiro

Conforme descrito na Seção 5.2.6 e segundo os modelos especificados em (CHAUM, 2004), o emprego da criptografia visual num SEV é algo concreto. Após a análise dessas técnicas, em paralelo ao entendimento do sistema eletrônico de votação brasileiro visto no Capítulo 3, tornou-se possível conceber a sua aplicação na urna eletrônica brasileira.

Os tópicos a seguir descrevem detalhadamente todo o processo responsável em propor o fornecimento do requisito de verificabilidade E2E (Seção 3.2) dentro do sistema eletrônico de votação brasileiro.

6.2.1. Visão geral do modelo

Dentro do modelo deverá existir impreterivelmente um mecanismo para geração e impressão do recibo para contraprova do voto, no qual chamo de Cédula de Registro de Voto (CRV). A geração da CRV seguiria um processo semelhante ao sugerido por David Chaum em (CHAUM, 2004), ou seja, a cédula deverá ser visivelmente destacável a partir de duas vias impressas em papel especial (transparente) contendo as informações do candidato selecionado durante a fase de votação (Seção 4.2.2). Essas informações deverão estar devidamente encriptadas, utilizando técnicas de criptografia visual (Seção 5.2), semelhantes ao *Visual Cryptography Scheme (2, 2)*, por exemplo, e exibindo também um Código de Confirmação do Voto (CCV) e um Número Identificador Singular (NIS), que poderão ser usados posteriormente numa auditoria do sufrágio. Além disso, na CRV deverá existir uma região em branco responsável pelo recebimento de uma marca d'água do Selo Nacional do Brasil, registrada de forma manual pelo fiscal responsável antes mesmo do eleitor deixar a seção de votação, conforme sugerido em (SARAIVA, 2012). Essa medida visa dificultar possíveis fraudes de falsificação das CRVs por indivíduos mal intencionados.

As Figuras 22 e 23 ilustram respectivamente o Selo Nacional do Brasil, que deverá ser registrado no campo reservado da CRV e um exemplo das duas vias de uma Cédula de Registro do Voto (CRV), correspondente ao modelo proposto.

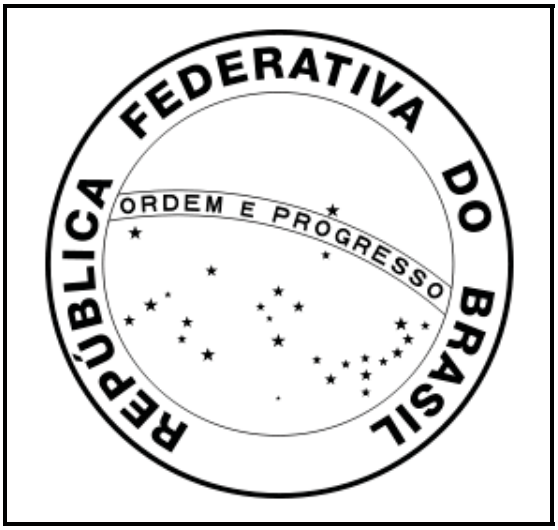

Figura 27 – Selo Nacional do Brasil

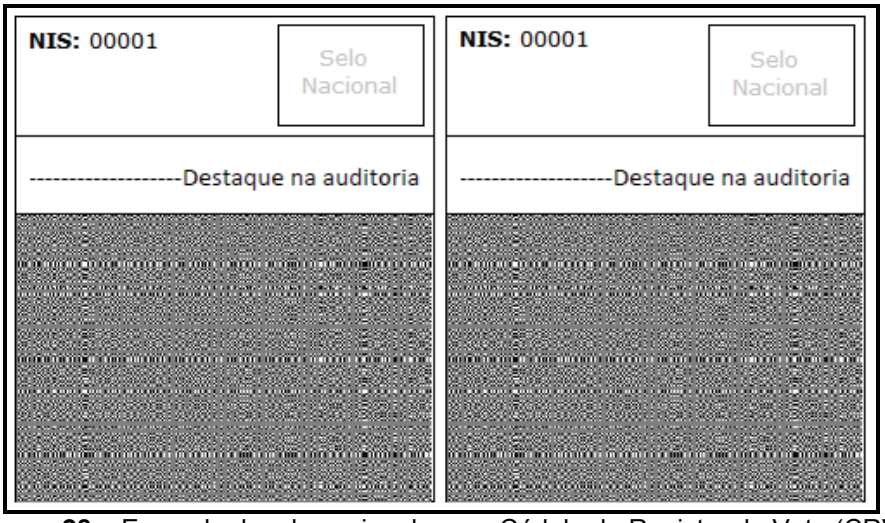

Figura 28 – Exemplo das duas vias de uma Cédula de Registro do Voto (CRV)

Durante a fase de votação do sistema brasileiro (Seção 4.2.2), o eleitor deverá se dirigir até a “cabine indevassável” de votação, que no caso do Brasil, ainda é considerada como um dos principais recursos para a garantia do sigilo do voto. Então o eleitor registra seu voto de acordo com o processo eletrônico já estabelecido e amplamente divulgado, e ao fim do sufrágio, o software da urna processará e apresentará ao eleitor um questionamento sobre a materialização (Impressão) do voto, nesse momento o eleitor poderá optar pela impressão ou não da CRV. No caso de uma negativa, o processo de votação se encerra e é dado prosseguimento de acordo com os procedimentos já instaurados, ou seja, o eleitor finaliza seu voto e sai da sua seção eleitoral sem qualquer contraprova do voto. No caso do eleitor optar pela impressão da CRV, o sistema deverá implementar alguns mecanismos, que estão descritos na Seção 6.2.2.

Após o processo de votação (Seção 4.2.2), o eleitor também poderá verificar a integridade de seu voto na Internet, através de uma página web desenvolvida especificamente para esse propósito. Um processo de verificabilidade universal também é fornecido pelo modelo, onde é possível auditar os votos depositados em uma urna tradicional, confrontando o registro físico com o registro digital contabilizado pela urna eletrônica e atualmente empregado como a principal base de dados para apuração e totalização dos votos respectivamente (Seções 4.2.3 e 4.2.4).

6.2.2. Arquitetura do modelo

O modelo em questão pode ser representado por uma arquitetura (Figura 28), onde, caso o eleitor opte pela impressão da CRV, conforme mencionado na Seção 6.1.1, o sistema deverá fornecer os respectivos mecanismos que implementam a proposta em questão:

1) **Geração e impressão da CRV:** Utilizando como base os mecanismos de encriptação visual sugeridos por David Chaum em (CHAUM, 2004), o sistema brasileiro deverá imprimir as vias de uma CRV. Ou seja, a CRV deverá ser visivelmente destacável e existirão duas vias impressas em papel especial (transparente) contendo as informações do candidato selecionado durante a fase de votação (Seção 4.2.2). A Figura 27 ilustra um exemplo das duas vias de uma Cédula de Registro do Voto (CRV);
2) **Geração do CCV na CRV:** Utilizando como base os mecanismos de encriptação aplicados em diversos sistemas eletrônicos de votação (Seção 5.1), o sistema brasileiro deverá gerar como saída para o eleitor o CCV, resultado da aplicação de um algoritmo de dispersão (Ex. XYZ) sob os dados previamente selecionados (o NIS, por exemplo). As seguintes características deverão ser garantidas pelo processo de geração do CCV:
    a) O código deve ser único dentro de cada CRV. Como dito, isso pode ser garantido a partir da utilização de uma função de dispersão (Seção 5.1.8) confiável e de conhecimento público;
    b) O CCV correspondente deve ser mantido em segredo para o eleitor até o que se efetue o processo de sobreposição das vias impressas de uma CRV;

3) **Geração do NIS na CRV:** Os CCVs poderão ser gerados a partir do NIS, que por sua vez também será gerado pelo sistema (Ex. 00001) e, por conseguinte impresso na Cédula de Registro do Voto (CRV), ou ainda a partir de outro parâmetro que seja comprovadamente único. As seguintes características devem ser garantidas pelo processo de geração dos NIS em cada CRV:
    a) O número deve ser único dentro de cada CRV. Essa unicidade pode ser garantida a partir da aplicação de uma função que contemple a pseudoaleatoriedade da geração desses números. Pode-se aplicar nesse caso o modelo usado pelo sistema Wombat abordado na Seção 3.6, que faz uso de um sistema de criptografia de chave pública: $Enc_{pk}(c, s)$, onde *s* é uma semente pseudoaleatória;
    b) O número não deve fornecer a mínima probabilidade de vínculo com o registro eletrônico do voto;
    c) O número não deve retratar a sequência de uma votação.
4) **Sobreposição das partes de uma CRV:** Conforme descrito anteriormente, tendo como base as funções de encriptação visual sugeridas por David Chaum (CHAUM, 2004), o sistema brasileiro deverá imprimir as duas vias de uma CRV. Em ambas, deverá constar o NIS correspondente à CRV e, quando devidamente sobrepostas, o eleitor deverá visualizar o CCV, juntamente com outras informações que comprovem que a CRV expressa verdadeiramente o voto capturado e registrado pelo software da urna eletrônica. Conforme ilustrado na Figura 25 (Direita) Essas informações podem ser, por exemplo:
    a) A identificação da eleição: Ex. Presidente;
    b) O nome do candidato: Ex. Fulano de tal;
    c) O número do candidato: Ex: 202020
5) **Conferência do registro eletrônico do voto:** No momento da sobreposição das vias encriptadas e impressas pela urna, o eleitor poderá conferir se as informações contidas na CRV compreendem o seu registro eletrônico. Nesse momento, o eleitor também poderá anotar em algum papel, ou mesmo na sua via da CRV, o resumo criptográfico (Hash) que foi revelado (CCV). É importante lembrar que apenas de posse desse resumo criptográfico (Hash), o eleitor não poderá sofrer ataques de um agente

coercitivo ou, ainda que intencionalmente, revelar o seu registro, visto que para comprovação íntegra do voto seria necessário efetuar a sobreposição das vias, que foram devidamente impressas em papéis especiais (transparente) a partir da aplicação da criptografia visual (Seção 5.2). Caso ocorra algum erro na conferência, como por exemplo, não ser possível visualizar o CCV, ou ainda se for o desejo do eleitor, o sistema deverá permitir o retorno ao processo inicial de votação, conforme ilustrado na Figura 28;

6) **Depósito da CRV numa urna tradicional:** Se não houver nenhum erro gerado durante a sobreposição das vias de uma CRV, o eleitor então depositará uma das vias numa urna tradicional (Seção 2.4.1). Esse processo tem como objetivo principal garantir uma futura auditoria dos votos, caso haja necessidade. O processo de auditoria e verificabilidade universal dos votos estão descritos na Seção 6.2.3.
7) **Marca d'água e finalização da votação:** Após a inserção de uma das vias da CRV numa urna tradicional, o eleitor deverá se dirigir até o responsável pela seção eleitoral, que estará responsável pela aplicação da marca d'água do Selo Nacional do Brasil (Figura 26) no local reservado da via da CRV escolhida pelo eleitor, finalizando assim o processo de votação.

A Figura 28 representada a seguir ilustra a arquitetura geral do modelo proposto e suas respectivas etapas.

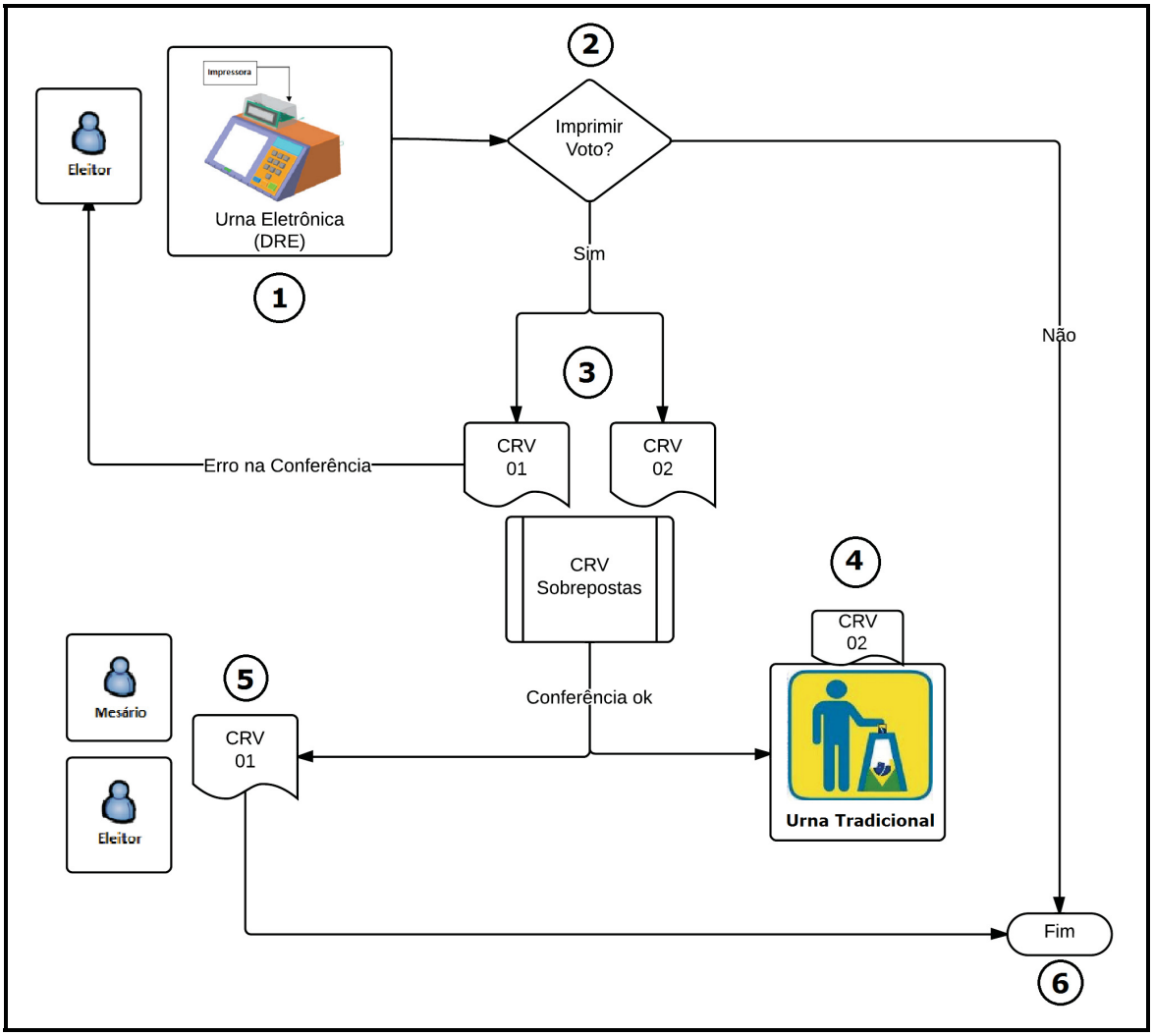

Figura 29 – Arquitetura geral do modelo proposto

Etapas do modelo proposto:

1) Voto do eleitor na urna eletrônica (DRE);
2) Escolha do eleitor pela impressão do registro do voto;
3) Processo de sobreposição e conferência das vias de uma CRV;
4) Depósito de uma das vias da CRV em uma urna tradicional;
5) Carimbo do selo nacional na outra via da CRV;
6) Fim da Votação.

É importante lembrar ainda que o processo de sobreposição das vias de uma CRV deverá ser efetuado pelo eleitor durante o processo de votação ainda dentro da “cabine indevassável” e, nesse momento, o sistema possibilitará a comprovação do registro eletrônico do voto. A Figura 29 ilustra um exemplo do

resultado da sobreposição das duas vias de uma Cédula de Registro do Voto (CRV), contendo as possíveis informações a serem utilizadas para a confirmação do registro eletrônico do voto.

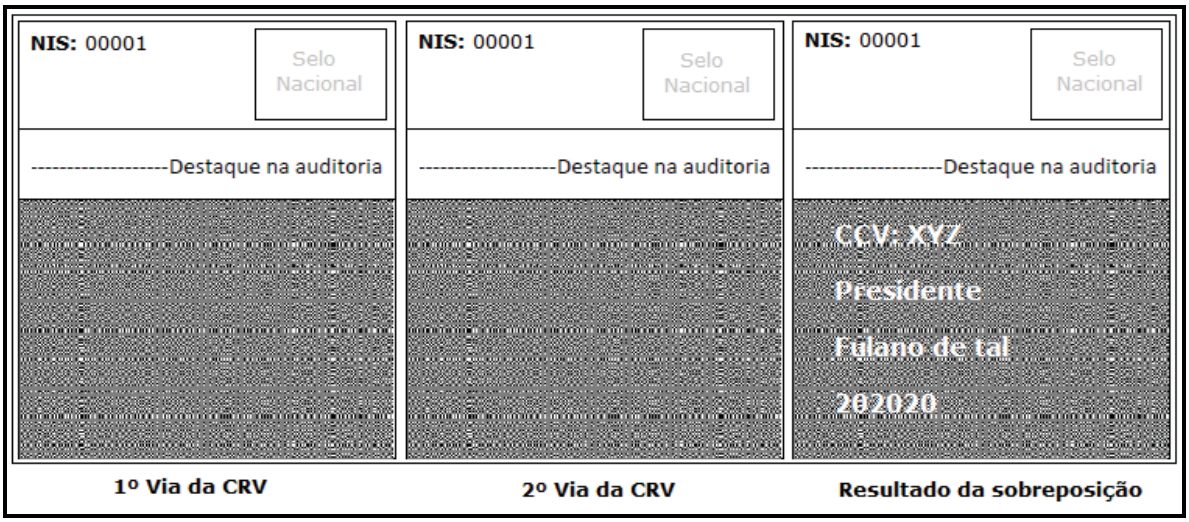

Figura 30 – Exemplo do resultado da sobreposição das duas vias de uma CRV

6.2.3 Concepção física do modelo

Para atender o modelo proposto, algumas alterações seriam necessárias na atual estrutura física da urna eletrônica brasileira. No caso, deverá ser instalado um equipamento responsável pela impressão das vias de uma CRV. Esse componente adicional poderia está posicionado sobre a urna, utilizando ou não um encaixe especial, e sua caixa seria preferivelmente produzida com material transparente, com o objetivo de prover maior visibilidade aos participantes no que se refere o processo de impressão e seus componentes.

A impressão das vias de uma CRV em papel especial (transparente) pelo sistema brasileiro, conforme especificado na Seção 6.1.1, é plenamente viável, pois atualmente a urna eletrônica brasileira já possui um módulo de impressão acoplado ao seu hardware. Além disso, existem empresas especializadas, como a Hewlett-Packard (HP), por exemplo, que já fabricam modelos capazes de operacionalizar esse tipo de impressão, incluindo neles o uso da criptografia visual (Seção 5.2).

Conforme descrito em (CHAUM, 2004), pode se considerar outras possibilidades para execução da impressão, onde, no caso, seria necessário o emprego de uma impressora especial. O fato é que a decisão pelo uso desse tipo de impressora elevaria inevitavelmente os gastos do processo. A Figura 30 ilustra uma possível concepção física do modelo proposto.

Figura 31 – Concepção física do modelo proposto

6.3. Processos de verificabilidade E2E

A Seção 2.1 relata a incessante busca pelo aumento da segurança e confiabilidade dos sistemas eletrônicos de votação, prezando por dois princípios ativos: o da publicidade e o do sigilo do voto. A partir disso, nota-se que os SEVs com verificabilidade E2E permitem que os eleitores auditem seus votos em quase todas as fases do processo eleitoral, proporcionando assim uma votação transparente, passando por uma apuração democrática, até um processo de auditoria capaz de garantir conferência para a sociedade.

Mais formalmente, o que tem sido invariavelmente chamado de E2E (do inglês, “End-to-End” ou Fim-a-Fim), votos codificados, criptografia, ou auditoria de sistemas abertos de voto, são os sistemas que preservam o sigilo eleitoral e que proporcionam: verificabilidade do eleitor e verificabilidade universal**.**

6.3.1. Verificabilidade do Eleitor

Na Seção 2.2.4, foi visto que a verificabilidade do eleitor é um requisito que tende em fornecer a possibilidade de que algum tempo após o lançamento do voto, cada participante possa confirmar que seu voto foi recolhido como elencado, verificando a preservação da privacidade de recepção da informação contra um registro público de recibos postados pelos funcionários eleitorais.

O modelo proposto garante esse requisito ao sistema brasileiro, pois no momento em que o eleitor registra seu voto eletronicamente na urna e opta pela impressão da CRV, é possível executar o processo de sobreposição das vias de

uma CRV, fornecendo assim ao eleitor a real possibilidade de confrontar seu registro eletrônico com o voto materializado na cédula.

É importante lembrar ainda que o processo de conferência ocorre somente durante a sobreposição das vias da CRV, que estarão devidamente impressas a partir de um mecanismo de criptografia visual (Seção 5.2), isso faz com que não seja possível ocorrer a revelação intencional ou não do voto, pois os responsáveis pelo processo eleitoral devem garantir que o eleitor apenas saia da seção de posse de uma das vias da CRV como contraprova do voto. A Figura 31 ilustra o possível procedimento de sobreposição das vias de uma CRV e a conferência do voto pelo eleitor, além de um exemplo do resultado dessa sobreposição.

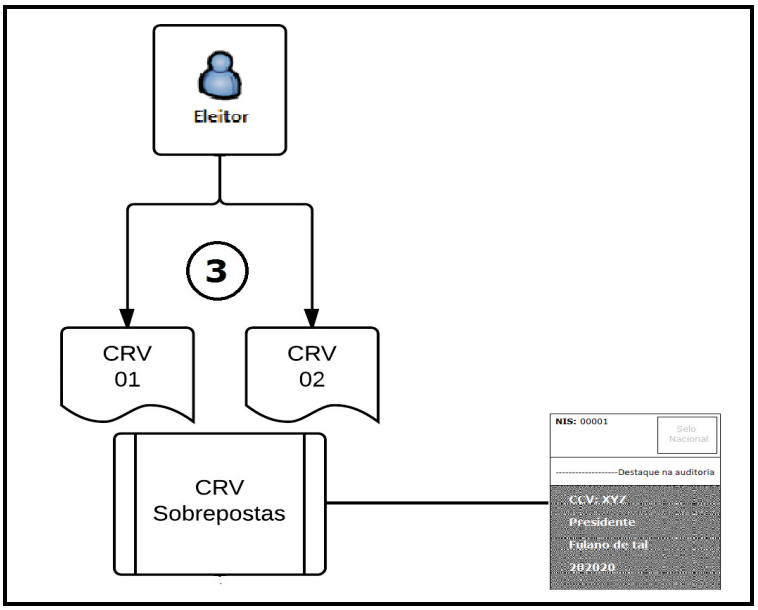

Figura 32 – Procedimento de sobreposição das vias de uma CRV e conferência do voto pelo eleitor

As autoridades responsáveis pelo processo eleitoral brasileiro também deverão informar ao eleitor sobre a possibilidade de anotar o CCV revelado durante a sobreposição, em uma das vias da cédula que ficará sob sua tutela, ou ainda em outro papel devidamente autorizado. Dessa forma, é possível efetuar posteriormente a verificação da integridade do seu registro em um sistema Web. O processo de verificação da integridade está detalhado na Seção 6.2.2.

Um fato relevante a respeito da anotação do CCV por parte do eleitor, é que esses mecanismos ainda precisam ser aprimorados no que tange sua usabilidade, visto que a grande maioria dos eleitores brasileiros não possui conhecimento básico do processo para geração de *hashes* criptográficos (Seção 5.1.8). Além

disso, qualquer caractere alfanumérico representado na CRV e anotado de forma errônea pelo eleitor poderá comprometer o processo de verificabilidade na Internet (Seção 6.2.2). Nos trabalhos futuros descritos na Seção 7.2, é enfatizada a necessidade de se estudar mais a fundo os algoritmos de dispersão que forneçam um melhor entendimento de seus resultados por parte do usuário final.

6.3.2. Verificação da integridade na Internet

Algumas pesquisas da atualidade que visam munir os SEVs da propriedade de verificabilidade E2E, sugerem também a adoção de um mecanismo que disponibilize a verificação do voto através de uma aplicação Web, onde o eleitor após algum tempo pode acessá-la e, de posse de informações públicas materializadas durante o processo de votação, efetua a conferência da integridade do registro do seu voto. Podemos citar como exemplo, o sistema Scantegrity II estudado na Seção 3.3.

No caso dessa proposta, para que seja possível garantir o requisito da verificabilidade pela Internet, o eleitor deverá acessar através de um navegador Web, uma aplicação responsável pela verificação do voto, inserindo em um campo de entrada o NIS emitido na CRV (Ex. 00001). Esse sistema deverá processar e apresentar como saída o CCV expresso por um resumo criptográfico (Seção 5.1.8), a partir desse código exibido em tela, o eleitor poderá conferi-lo de acordo com o que foi previamente anotado em uma das vias da CRV durante o processo de sobreposição (Figura 31). Esse mecanismo sugere a entrega de garantias aos eleitores de que seu voto foi registrado corretamente pelo software da urna e que o CCV gerado pela urna e revelado na CRV é integro a partir do uso do NIS.

A aplicação Web sugerida deverá implementar características importantes, entre elas, a aplicabilidade do mesmo algoritmo de dispersão utilizado para geração do CCV, visto que para o eleitor, o procedimento será nada mais que inserir o NIS que consta na CRV e receber como saída o mesmo código hash da CRV outrora anotado. A Figura 32 ilustra um possível protótipo de tela da aplicação que seria responsável pelo fornecimento da verificabilidade pela Internet.

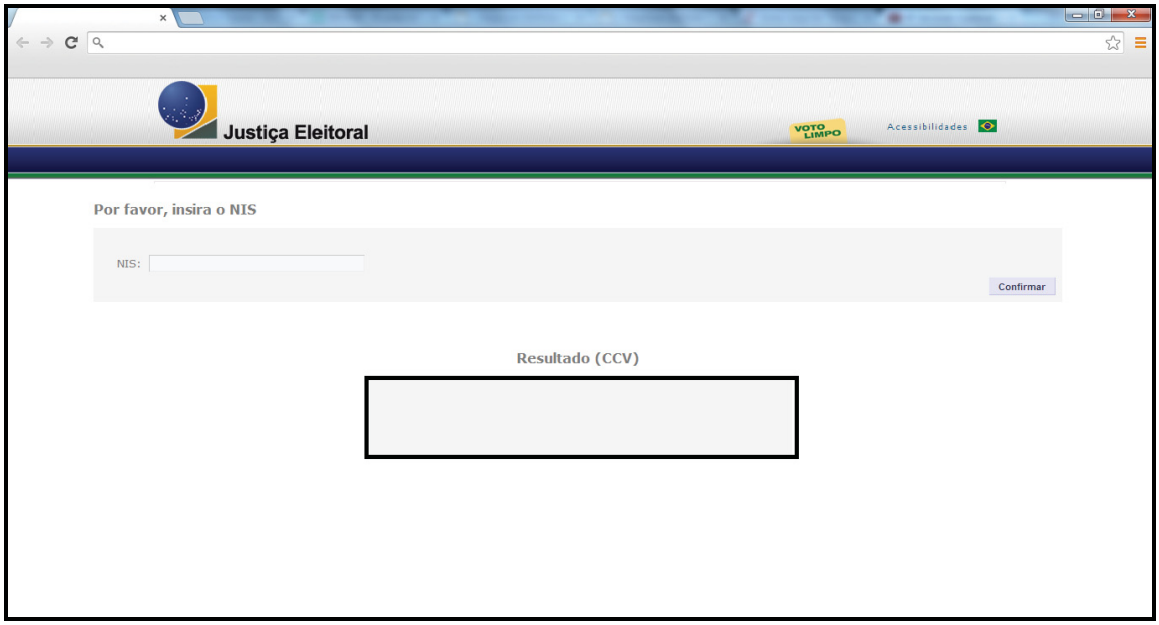

Figura 33 – Protótipo de tela da aplicação para verificabilidade pela Internet

Conforme já mencionado na seção anterior, a verificabilidade pela Internet só poderá existir a partir do momento que o eleitor opta em copiar o número CCV gerado pelo sistema em uma das vias da CRV, caso isso não aconteça, todos os esforços abnegados serão em vão.

Uma forma de minimizar o impacto negativo ou resistência na utilização desse recurso seria um trabalho massivo de divulgação através de cartilhas e mídias de comunicação, além de fornecer um possível treinamento online que orientasse o uso desse mecanismo.

6.3.3. Auditoria e verificabilidade universal

Foi visto na Seção 2.2.4, que a verificabilidade universal é um requisito que fornece a possibilidade de que qualquer pessoa pode verificar que os votos foram contados como recolhidos, ou seja, uma forma de provar que a correspondência postada é correta com relação ao registro público dos recibos postados.

O modelo proposto sugere garantias desse requisito ao sistema brasileiro, a partir de um processo que pode ocorrer dias após as eleições, em um período pré-definido pelo Tribunal Superior Eleitoral (TSE).

Seguindo o processo sugerido por C.E.R. Saraiva em (SARAIVA, 2012), na auditoria, deve-se dispor de uma equipe especializada para realizar a conferência da integridade dos lacres das urnas tradicionais, estas devem ser mantidas

organizadas por seção até o dia da auditoria, como forma de garantir que as CRVs sejam reutilizadas pelos eleitores. Com o emprego desse mecanismo não existe riscos para a quebra do sigilo dos votos no caso de qualquer pessoa ver uma das vias da CRV, pois o voto está devidamente encriptado por um mecanismo de criptografia visual e só é possível ser revelado de posse das duas chaves (vias da CRV). Após esses procedimentos, será efetuado o rompimento dos lacres das urnas tradicionais na presença das partes interessadas nesse processo, como por exemplo, os fiscais de diversos partidos.

Os votos representados por uma das vias da CRV devem ser retirados das urnas seguindo cada seção, sendo então colocados em ordem sequencial a partir do NIS, e posteriormente entregue aos eleitores selecionados por um sistema de amostragem. Conforme mencionado, o processo de sequenciamento das vias é possível graças ao NIS que apesar de ser um número pseudoaleatório, é singular. Conforme mencionado, deve-se, no entanto, focar para a definição de uma amostragem razoável de vias da CRV para conferência, sem que ocorra grande impacto na evolução do processo, mas que se mantenha um nível elevado de assertividade na auditoria.

Após isso, os eleitores selecionados irão até o local oficial levando consigo a sua via da CRV, lá serão devidamente identificados pelos oficiais eleitorais, que entregarão a respectiva via da CRV outrora depositada na urna tradicional (Seção 2.4.1) pelo respectivo eleitor. Nesse momento, o eleitor será encaminhado novamente a uma cabine indevassável para que ninguém veja seu registro e nem seja possível haver a quebra do sigilo de seu voto. Efetuando novamente o processo de sobreposição das duas vias da CRV para revelação do voto (Figura 31), o eleitor então confere o mesmo, destaca em ambas as vias a parte impressa com o NIS, que deve ser descartada (Figura 29) e as conecta utilizando algum mecanismo, como por exemplo, grampos ou cola. Em seguida o eleitor deposita as vias em outra urna que será posteriormente auditada pelos oficiais eleitorais na presença dos interessados. Caso o eleitor evidencie alguma discrepância durante a sobreposição das vias da CRV, o mesmo deverá comunicar ao responsável pelo processo, que executará os procedimentos necessários e pré-definidos para o processo de auditoria. Lembrando que qualquer discrepância evidenciada pelo

eleitor durante a conferência das vias, não revelará o voto, visto que apenas o conjunto real da CRV apresentará o sufrágio.

É importante reforçar que a auditoria é feita por amostragem, definida pelo órgão competente e não é necessário que todos os eleitores produzam seus recibos. Conforme sugerido por (SARAIVA, 2012) e como é comum em alguns sistemas, um percentual entre 2% a 5% já é considerado suficiente para determinar se houve ou não fraude na eleição. Dessa forma, levando em conta que pessoas com necessidades especiais ou idosas, por exemplo, geralmente consideram o método complicado, elas poderiam ser dispensadas da amostra. Entretanto é importante também frisar que pelo menos 10% dos eleitores precisam gerar as CRVs, para o caso de perdas, furtos, ou vias danificadas que precisem ser anuladas, por isso o sistema de divulgação do processo de verificabilidade do eleitor (Seção 6.2.1) é considerado tão relevante.

6.4. Principais vantagens e desafios encontrados

O modelo proposto emprega uma série de melhorias ao SEV brasileiro, principalmente no que tange o requisito de verificabilidade E2E. Outras propriedades também são mantidas, mesmo havendo certo conflito entre elas, como por exemplo, a possibilidade de prover verificabilidade sem que haja a quebra no sigilo do voto e nem o favorecimento na atuação de um agente coercitivo, conforme foi detalhado na Seção 2.2.3.

Mesmo contando com um número relevante de ganhos ao processo, não se pode deixar de relatar que o modelo ainda carece de evolução, principalmente no que diz respeito aos desafios para implementação e testes reais de utilização desse sistema, bem como a melhorias na usabilidade de alguns mecanismos de criptografia empregados. No Quadro 15 estão descritas as principais vantagens e desafios da utilização do modelo, levando-se em consideração os estudos realizados até o momento.

Principais vantagens	Principais desafios
• Garante maior transparência em todo o processo eleitoral; • Assegura a aplicabilidade do requisito de verificabilidade do voto; • Assegura a aplicabilidade do requisito de verificabilidade universal; • Assegura a aplicabilidade do requisito de verificabilidade na Internet; • Entrega mecanismos para o princípio da independência do voto eletrônico; • Conservação de quase todo o processo eleitoral já existente e empregado ao longo dos anos no Brasil; • Menor impacto na operação, além de proporcionar baixo acréscimo aos gastos do processo eleitoral.	• Aumento dos gastos com impressoras; • Acréscimo no tempo do processo de votação; • Os CCV não são amigáveis; • Causa certa dificuldade para pessoas com necessidades especiais, idosas e outras.

Quadro 14 – Vantagens e desafios do modelo proposto

7. CONCLUSÃO E TRABALHOS FUTUROS

7.1. Contribuições do trabalho e visão do futuro

As principais contribuições desta dissertação estão listadas a seguir:

- **A análise e contextualização dos sistemas de votação:** Essa análise foi primordial para a compreensão dos principais sistemas de votação, buscando pelo entendimento e evolução dos requisitos para implementação de um projeto de SEV, além de evoluir no entendimento dos principais desafios que ainda impactam no projeto. Outro ponto relevante foi os estudos das possíveis gerações que contemplam os modelos desse tipo de sistema;
- **O estudo de alguns dos principais sistemas eletrônicos de votação de 3ª Geração:** Foram minunciosamente estudados e detalhados quatro sistemas de votação de terceira geração, que no caso servem como projetos que contribuem consideravelmente com a evolução desses sistemas. O estudo envolveu principalmente a compreensão dos mecanismos de criptografia usados pelos sistemas, o que fez com fosse possível conceber a proposta;
- **O estudo do sistema eleitoral brasileiro:** Como já havia sido realizado por Carlos Eduardo Saraiva em (SARAIVA, 2012), o estudo aprofundado do sistema eleitoral brasileiro, proporciona um conhecimento relevante de seus desafios, como isso, torna-se possível conceber modelos que visam ajustar possíveis falhas no processo como um todo, garantindo assim o estado democrático desse país;
- **A evolução nos estudos da criptografia visual:** Dentre outros mecanismos de criptografia detalhados neste trabalho, a criptografia visual foi dada como prioridade, pois a partir disso foi possível munir o sistema brasileiro para entregar propriedades críticas (Seção 2.2) de um SEV, como por exemplo, a verificabilidade E2E. Analisar e propor a aplicabilidade esse método não convencional de encriptação, também favorece sua expansão;
- **Detalhamento de uma proposta da aplicação de criptografia visual no SEV brasileiro:** Esta deve ser considerada como a principal contribuição

deste trabalho, onde, a partir da compreensão geral do sistema brasileiro (Capitulo 4) e de mecanismos de criptografia visual (Seção 5.2), tornou-se plenamente possível sugerir um modelo que visa atender as principais propriedades de um Sistema Eletrônico de Votação ao sistema eleitoral brasileiro. Além disso, é de extrema importância oferecer ao provo brasileiro uma alternativa ao processo instaurado hoje no Brasil.

7.2. Trabalhos futuros

Como possíveis trabalhos futuros, pode-se apontar:

- **Célula de estudos para votação eletrônica no CIN/UFPE:** A partir do crescimento nas pesquisas de sistemas eletrônicos de votação, inevitavelmente teremos uma maior procura de pesquisadores para essa área, com isso a intenção de formar uma célula especifica para essa área, como forma de organizar eventos para divulgação dos resultados das pesquisas;
- **Estudo ainda mais aprofundado da criptografia em SEV:** A imersão nos estudos referentes a modelos criptográficos para SEV é algo relevante e que será dado como foco em futuras pesquisas, visto que a partir desses mecanismos é possível prover soluções aos principais desafios desse tipo de sistema. Além disso, enfatizo a necessidade de se estudar mais a fundo os algoritmos de dispersão para que forneçam um melhor entendimento de seus resultados por parte do usuário final;
- **Implementar um SEV com base no modelo proposto:** Realizar a implementação de um protótipo do modelo proposto, como forma de evidenciar sua aplicação em um SEV de primeira geração. Além de realizar testes para avaliação de sua funcionalidade e confiabilidade. Nesse sentido, também será realizado estudos para solucionar os desafios ligados a utilização de um código *hash* como produto verificador, em que torna o processo de verificação mais complicado para seus utilizadores, bem como os problemas relacionados a possíveis ataques ao modelo, como por exemplo, a possibilidade de um atacante tirar cópia do recibo do eleitor e

então subornar um dos ficais para tirar cópia da outra parte a fim de confirmar seu voto.

- **Empregar o SEV em uma eleição real:** Após a avaliação realizada a partir protótipo, existe a intenção de empregar esse sistema em alguma eleição real. Visando inicialmente atingir pequenos processos eleitorais, como ocorre para a seleção de sindicatos, por exemplo.

7.3. Conclusão

A democracia de um país só pode ser levada em consideração no momento em que o mesmo fornece possibilidades reais de que o povo pode exercer seus poderes de escolha. No Brasil, essa definição está descrita e instaurada na Constituição Federal. No que tange o cenário eleitoral, o Brasil tem por obrigação favorecer a participação indireta do povo, que exerce esse direito democrático a partir do voto em seus representantes.

Muito embora o processo eleitoral brasileiro seja considerado fácil e rápido principalmente no que diz respeito à apuração e totalização dos votos, muitas premissas de segurança ainda são obscuras na visão do eleitor, como por exemplo, os questionamentos sobre onde vai parar o voto registrado pelo software da urna eletrônica, que no caso brasileiro atende por uma máquina de primeira geração, considerada por muitos como defasada. Realmente não existem garantias quanto à computação do voto, visto que é uma limitação inerente a um processo puro e simplesmente computacional. Faz-se necessário então revisar uma série de pontos desse sistema, contando com a parceria imparcial do TSE e outros profissionais que estão diretamente envolvidos com o processo, com isso será possível prover uma maior confiabilidade das eleições ao eleitor.

Em meio às diretrizes de segurança estabelecidas e empregadas pela comunidade internacional, este trabalho destaca o *Princípio da Independência do Software* (Seção 3.1) em sistemas eleitorais, visto que este conceito vem sendo defendido como a principal forma de possibilitar a conferência do resultado de uma eleição, sem que haja a total dependência de tecnologia e possibilitando que cada eleitor possa ser um auditor do seu próprio sufrágio.

Os mecanismos para materialização do voto são considerados por muito como a principal solução de garantias a democracia, fazendo com que a sociedade possa comprovar seu registro eletrônico de voto, a partir da entrega de um requisito conhecido como verificabilidade fim-a-fim. Nesse contexto a aplicação de modelos criptográficos é fundamental, sendo mais especifico o uso de mecanismos de criptografia visual como ferramenta principal que faz a integração entre a tecnologia e a transparência de uma eleição, primando pelo aumento da segurança.

Conforme visto no Capitulo 6, o emprego da criptografia visual em sistemas eletrônicos de votação é plenamente possível, e sua inserção para o processo eleitoral brasileiro é essencial para a manutenção de uma sociedade democrática. E, apesar de alguns desafios, deve-se considerar a utilização da computação a favor da grande massa e não com o objeto de aliená-la, com isso a computação deve servir como recurso propulsor a segurança e transparência do voto.

REFERÊNCIAS

ADIDA, B.; NEFF, A. **Ballot Casting Assurance**. In: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop, EVT'06, pp. 7-7, Berkeley, CA, USA, 2006.

ADIDA, B. **Web-based Open-Audit Voting**. In: Proceedings of the 17th Usenix Security Symposium (USENIX Security 2008), San Jose, CA, Jul 28 – Agosto 1, pp. 335-348, 2008.

ADIDA, B.; NEFF, A. **Efficient Receipt-Free Ballot Casting Resistant to Covert Channels**. In: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2009 on Electronic Voting Technology Workshop, EVT/WOTE'09, Montreal, Canada, 2009.

ARANHA, D. F. et al. **Software Vulnerabilities in the Brazilian Voting Machine**. UnB, 2012. (Relatório Técnico).

ARANHA, D. F. et al. **Vulnerabilidades no Software da Urna Eletrônica Brasileira**. [S.l.]: UnB, 2012. 36 p. – Disponível em: <http://goo.gl/5SSYgm>. Acesso em: 09 de junho de 2014.

ARAUJO, R.; CUSTODIO, R. F.; GRAAF, J. V. **A Verifiable Voting Protocol Based on Farnel.** Towards Trustworthy Elections. Lecture Notes in Computer Science Vol. 6000, 2010, pp. 274-288.

BAIRD, L. **Código de Criptografia Visual Escrito em JavaScript**. Disponível em: <http://goo.gl/84TfNX>. Acesso em: 02 de fevereiro de 2014.

BENALOH, J. **Simple Verifiable Elections**. In: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop, EVT'06, pp. 5-5, Berkeley, CA, USA, 2006.

BLAKLEY, G. R. **Safeguarding Cryptographic Keys**. In: Proceedings of the 1979 National Computer Conference, volume 48 of AFIPS Conference Proceedings, pp. 313-317, New York, USA, 1979. AFIPS Press.

BRUNAZO, A. **Modelos e Gerações dos Equipamentos de Votação Eletrônica**. Disponível em: <http://goo.gl/28R0kJ>. Acesso em: 09 de junho de 2014.

CHAUM, D. **Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms**. Commun. ACM, pp. 24(2):84-88, 1981. Universidade da California, Berkeley, 1981.

CHAUM, D. **Blind Signatures for Untraceable Payments**. In: D. Chaum, R. L. Rivest, and A. T. Sherman, editors, advances in Cryptology - Crypto '82, pp. 199 - 204. Plenum Publishing, 1982.

CHAUM, D. **Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA**. In: Proceendings of Advances in Crytology – EUROCRYPT'89, pp. 177-182, 1989.

CHAUM, D. **Secret-Ballot Receipts and Transparent Integrity**. Palo Alto Workshop on Information Dynamics in the Networked Economy, 2002.

CHAUM, D. **Secret Ballot Receipts: True Voter-Verifiable Election**. IEEE Security and Privacy, Janeiro/Fevereiro 2004, pp. 38-47.

CHAUM, D. et al. **Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems Using Invisible Ink Confirmation Codes**. Disponível em: <http://goo.gl/B8lDq9>. Acesso em: 09 de junho de 2014.

CIMATO, S.; YANG, C. N, editores. **Visual Cryptography and Secret Image Sharing**. Digital Imaging and Computer Vision. CRC Press, New York, USA, 2011.

COMITE MULTIDISCIPLINAR INDEPENDENTE (CMIND). **Relatório da Observação de Eleição na Argentina com Sistema de Voto Eletrônico de 2ª Geração**. Versão 1.0. Cidade de Residência. Disponível em: <http://goo.gl/W7JYFc>. Acesso em: 09 de junho de 2014.

COSTA, R. G. **Sistema Seguro de Votação Eletrônica Multi-cédulas**. Dissertação de mestrado. Pontifícia Universidade Católica do Paraná, Curitiba, 2008.

COSTA, R.; OBELHEIRO, R.; FRAGA, J. **RPM: Comunicação Anônima em Redes Par a Par**. 26º SBRC. Departamento de Automação e Sistemas. Universidade Federal de Santa Catarina, 2008.

DEL PICCHIA, W. **Cartilha Básica do Voto-E no Brasil**. Disponível em: <http://goo.gl/rIhLZb>. Acesso em: 09 de junho de 2014.

DEVEGILI, A. J.; CUSTODIO, R. F. **Farnel: Uma Proposta de Protocolo Criptográfico para Votação Digital**. Universidade Federal de Santa Catarina. Centro Tecnológico, 2001.

DIFFIE, W.; HELLMAN, M. **New Direction in Cryptography**. IEEE Transactions on Information Theory, Novembro 1976.

DIFFIE, W.; HELLMAN, M. E. **Privacy and Authentication: An Introduction to Cryptography**. Proceedings of the IEEE, pp. 67(3):397-427, Março 1979.

DOUGLAS, W. J.; BARBARA, S. **Broken Ballots: Will Your Vote Count in the Electronic Age?** Library of Congress. Caraloging-in-Publication Data, 2012.

ELGAMAL, T. **A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms**. Information Theory, IEEE Transactions on, pp. 31(4):469-472, 1985.

ESTEHGHARI, S.; DESMEDT, Y. **Exploiting the Client Vulnerabilities in Internet E-voting Systems: Hacking Helios 2.0 as an Example**. In: Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections, EVT/WOTE'10, pp. 1-9, Berkeley, CA, USA, 2010.

FERREIRA, P.; JOAQUIM, R.; RIBEIRO, C. **The Design of an End-to-End Verifiable Internet Voting System**. 2009.

FUJIOKA, A.; OKAMOTO, T.; OHTA, K. **A Practical Secret Voting Scheme for Large Scale Elections**. Proc. of Advances in Cryptology – AUSCRYPT '92, LNCS 718, pp. 244-251, 1992.

GOLDWASSER, S.; MICALI, S.; RACKOFF, C. **The Knowledge Complexity of Interactive Proof Systems**. SIAM Journal of Computing, pp. 18(1):186-208, 1989.

HAENNI, R.; DUBUIS, E.; ULTES-NITSCHE, U. **Research on E-voting Technologies**. Technical Report, Berner Fachhochschule Berne University of Applied Sciences, Engineering and Information Technology, 2008.

HELLMAN, M. E. **An Extension of the Shannon Theory Approach to Cryptography**. IEEE Transactions on Information Theory, pp. 23(3):289-294, Maio 1977.

HIRT, M.; SAKO, K. **Efficient Receipt-Free Voting Based on Homomorphic Encryption**. Advances in Cryptology – EUROCRYPT 2000. Lecture Notes in Computer Science Volume 1807, 2000, pp. 539-556, Maio 2000.

HORNG, G.; CHEN, T.; TSAI, D. S. **Cheating in Visual Cryptography**. Designs, Codes and Cryptography, pp. 38(2):219-236, Fevereiro 2006.

HU, C. M.; TZENG, W. G. **Cheating Prevention in Visual Cryptography**. IEEE Transactions on Image Processing, pp. 16(1):36-45, Janeiro 2007.

JACOBS, B.; PIETERS, W. **Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment**. Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures. Springer LNCS 5705, pp. 121-144, 2009.

JOAQUIM, R.; RIBEIRO, C.; FERREIRA, P. **VeryVote: A Voter Verifiable Code Voting System**. E-Voting and Identity. Lecture Notes in Computer Science Vol. 5767, 2009, pp. 106-121.

JOAQUIM, R.; FERREIRA, P.; RIBEIRO, C. **EVIV: An End-to-End Verifiable Internet Voting System**. Computers & Security. ISSN 0167-4048. Vol. 32, pp. 170-191, 2013.

KAFRI, O.; KEREN, E. **Encryption of Pictures and Shapes by Random Grids**. Optics Letters, 1987.

KÜSTERS, R.; TRUDERUNG, T.; VOGT, A. **Clash Attacks on the Verifiability of E-Voting Systems**. University of Trier, Alemanha, 2012. Disponível em: <http://goo.gl/DwBeRH>. Acesso em: 09 de junho de 2014.

LIU, C. L. **Introduction to Combinatorial Mathematics**. McGraw-Hill, Nova Iorque, 1968.

LIU, F.; WU, C.; LIN, X. **Cheating Immune Visual Cryptography Scheme**. IET Information Security, pp. 5(1):51-59, Março 2011.

MARQUES, D.; NEVES, J. **Criptografia Visual**. Dissertação de mestrado. Universidade de Campinas, Instituto de Computação, Mestrado Profissional, 2003.

MARQUES, G. B.; RIBEIRO, V. G.; ZABADAL, J. R. **Impactos Computacionais de Uma Implementação de Criptografia Visual**. Revista Eletrônica de Sistemas de Informação, V. 7, Nº. 1, artigo 1, 2008. Disponível em: <http://goo.gl/7is9V8>. Acesso em: 09 de junho de 2014.

MERCURI, R. **Electronic Vote Tabulation Checks & Balance**. Ph.D. Dissertation, defended October 27, 2000 at the School of Engineering and Applied Science of the University of Pennsylvania, Philadelphia, PA. Disponível em: <http://goo.gl/qIfC85>. Acesso em: 09 de junho de 2014.

MONTEIRO, A. et al. **Sistemas Electrónicos de Votação**. Faculdade de Ciências da Universidade de Lisboa, 2001.

MORAN, T.; NAOR, M. **Receipt-Free Universally Verifiable Voting witch Everlasting Privacy**. Advances in Cryptology – CRYPTO 2006. Lecture Notes in Computer Science. Volume 4117, 2006, pp. 373-392.

NAOR, M.; SHAMIR, A. **Visual Cryptography**. Em Advances in Cryptology – EuroCrypt '94, volume 950 of Lecture Notes in Computer Science, pp. 1-12, Perugia, Itália, 1995. Springer.

NAOR, M.; SHAMIR, A. **Visual Cryptography II: Improving the Contrast Via the Cover Base**. In: Security Protocols Workshop, volume 1189 of Lecture Notes in Computer Science, pp. 197-202, Cambridge, Reino Unido, 1996. Springer.

NAOR, M.; PINKAS, B. **Visual Authentication and Identification**. In: Advances in Cryptology - CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, pp. 322-336, California, USA, 1997. Springer.

PAUL, N. et al. **Authentication for Remote Voting.** Workshop on Human-Computer Interaction and Security Systems, Abril 2003.

PERES, G. – DEPUTADO. **Audiências na CCJC sobre Urnas Eletrônicas**. [S.l.]: Câmara dos Deputados, 2008. 5 p. Disponível em: <http://goo.gl/dzAX2N>. Acesso em: 09 de junho de 2014.

PRASA, H. K. et al. **Security Analysis of India's Electronic Voting Machines**. 17th ACM Conference on Computer and Communication Security (CCS '10). Chicago, 2010.

PRISCO, R.; SANTIS, A. **Cheating Immune (2, n)-threshold Visual Secret Sharing**. Em Security and Cryptography for Networks, volume 4116 of Lecture Notes in Computer Science, pp. 216-228, Maiori, Itália, 2006. Springer.

RADWIN, M.; KLEIN, P. (1995). **An Untraceable, Universally Verifiable Voting Scheme**. Seminar in Cryptology, Dezembro 1995.

REZENDE, P. **Podemos Classificar Sistemas de Votação**. Universidade de Brasília (UnB), 2012. Disponível em: <http://goo.gl/Qv1ysf>. Acesso em: 29 de maio de 2014.

RIVEST, L. R.; WACK, J. P. **On the Notion of "Software Independence" in Voting Systems**. [S.l.]: National Institute of Standards and Technology (NIST), 2006. 11 p. Disponível em: < http://goo.gl/AZ1FRc>. Acesso em: 21 de abril de 2014.

RIVEST, R.; SMITH, W. **Three Voting Protocols: ThreeBallot, VAV, and Twin**. USENIX/ACCURATE Electronic Votinh Technology Workshop, 16 th USENIX Security Symposium, 2007.

ROCHA, R.; SIMÕES, F.; ANTUNES, P. **Estudo dos Requisitos para um Sistema de Votação Electrónica**. Departamento de Informática, Faculdade de Ciências da Universidade de Lisboa, Março de 2004

RYAN, P. Y. A. et al. **The Prêt a Voter Verifiable Election System**. IEEE Transactions on Information Forensics and Security. pp. 662-673, 2009.

SAKO, K.; KILIAN, J. **Receipt-free Mix-type Voting Scheme – A Practical Solution to the Implementation of a Voting Booth**. In: EUROCRYPT´95, pp. 393-403, 1995.

SARAIVA, C.E.R. **A Criptografia visual e suas aplicações na melhoria da segurança do sistema brasileiro de votação eletrônica**. Dissertação de mestrado. Centro de Informática, Universidade Federal de Pernambuco, Mestrado Acadêmico, Setembro 2012.

SCHILCHER, F. **Key Management and Distribution for Threshold Cryptography Schemes**. Janeiro 19, 2004.

SCHOENMAKERS, B. **Compensating for a Lack of Transparency**. In: Proceedings of the Tenth Conference on Computers, Freedom & Privacy. (CFP'00), 2000.

SHAMIR, A. **How to Share a Secret**. Communication of the ACM, Vol. 22, Nº 11, Novembro 1979.

SHANNON, C. E. **Communication Theory of Secrecy Systems**. Bell Systems Technical Journal, v. 28, pp. 656-715, Outubro 1949.

SINGH, S. **O Livro dos Códigos**. Rio de Janeiro: Record, 2001.

STAJANO, F. **VCK: the Visual Cryptography Kit**. Olivetti Oracle Research Laboratory & University of Cambridge Computer Laboratory, 1998. Disponível em: <http://goo.gl/J5pxEB>. Acesso em: 09 de junho de 2014.

STEFAN, K. **Explanation of the German Voting System**. Disponível em: <http://goo.gl/UlKTvv>. Acesso em: 28 de agosto de 2014.

STINSON, D. **Visual Cryptography and Threshold Sch**emes. Potentials, IEEE, pp. 18(1):13-16, Fevereiro/Março 1999.

TOMPA, M.; WOLL, H. **How to Share a Secret with Cheaters**. Journal of Cryptology, pp. 1:133-138, Agosto 1989.

TSAI, D. S.; CHEN, T. H.; HORNG, G. **A Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Secret Images**. Pattern Recognition, pp. 40(8):2356-2366, 2007.

WIKSTRON, D. **How to Implement a Stand-alone Verifier for the Verificatum Mix-Net**. KTH Stockholm, Suécia, 2011. Disponível em: <http://goo.gl/65rgTd>. Acesso em: 09 de junho de 2014.

ZMOGINSKI, F. **TSE terá urna biométrica em 61 cidades**. Info Online. Disponível em: <http://goo.gl/JffooI>. Acesso em: 09 de junho de 2014.