UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

RICARDO LUÍS LICHTLER

Um Sistema Seguro Para Votações Digitais

Dissertação apresentada como requisito parcial
para a obtenção do grau de
Mestre em Ciência da Computação

Prof. Dr. Raul Fernando Weber
Orientador

Porto Alegre, outubro de 2004.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Lichtler, Ricardo Luís.

Um Sistema Seguro Para Votações Digitais / Ricardo Luís Lichtler. Porto Alegre: Programa de Pós-Graduação em Computação, 2004.

53 f.: il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Ciência da Computação, Porto Alegre, BR-RS, 2004. Orientador: Raul Fernando Weber

1. Votações digitais. 2. Criptografia. 3. Protocolos. I. Weber, Raul. II. Título.

DEDICATÓRIA

qANQR1DDDQQDAwIrQfO5IOF0oWDJae0ILy6zsFlrqKT0Z0rtdytvRJ58eTXbony6
C38xFskqjh4TaLrRuA0j3/yr0RHAPNRwutjfAUQRdvenajEszUdZrxlx7CwW/vX7
+ZxMwuxLYhqwBS8nVoXIt3rooklSRgpi1lIoLBP40Q==
=zf5i”2404”
.

AGRADECIMENTOS

Ao meu orientador, pela pessoa única que é.
Aos meus colegas e amigos do GSeg.
Aos meus amigos da faculdade, especialmente
Henrique, Ingrd, Rafael, Maíra e Paulo.
E finalmente, mas não menos importante, ao Luís Fernando.

SUMÁRIO

LISTA DE ABREVIATURAS

CA	Central de Apuração
CC	Central de Cadastramento
CV	Central de Votação
DES	*Data Encryption Standard*
PGP	*Pretty Good Privacy*
RSA	Rivest Shamir Adleman
SDK	*Software Developer´s Kit*
TSE	Tribunal Superior Eleitoral

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

O papel das eleições tem crescido de importância na sociedade moderna. Se, por um lado, é necessário garantir a universalização do voto, por outro lado é fundamental garantir a qualidade e a lisura do processo eleitoral.

Neste sentido, muitos trabalhos têm sido apresentados com o objetivo de usar recursos computacionais no processo eleitoral. Computadores podem facilitar o acesso dos eleitores aos sistemas e processos de votação, como também aceleram a apuração dos resultados.

Entretanto, redes de computadores são alvos de ataques sistemáticos. Esses ataques podem afetar a disponibilidade do processo e, além disso, interferir nos resultados da eleição ou afetar seus fundamentos. Garantir que os princípios exigidos para uma eleição segura sejam respeitados é a finalidade dos sistemas baseados em protocolos criptográficos.

Muitas propostas de sistemas têm sido feitas. Algumas utilizam certo grau de obscuridade de funcionamento como garantia contra ataques; outras utilizam técnicas amplamente conhecidas, embora com grau elevado de complexidade.

O presente trabalho apresenta a proposta de um sistema completo para execução de uma votação digital segura. O sistema é baseado em um protocolo simples, porém completo, que utiliza técnicas criptográficas amplamente conhecidas. O protocolo é descrito gradativamente, e é provada a sua eficiência contra os ataques possíveis.

O texto ainda apresenta alguns outros protocolos criados para esse mesmo propósito. Finalmente, é apresentado o protótipo de um sistema de software que emprega o protocolo considerado.

Palavras-chave: votação segura, protocolo, criptografia.

A Secure System for Electronic Voting

ABSTRACT

The role of the elections has grown of importance in the modern society. If it is necessary to guarantee the universalization of the vote, on the other hand it is basic to guarantee the quality and the correctness of the electoral process.

In this direction, many works have been presented with the objective to use computational resources in the electoral process. Computers can facilitate to the access of the voters to the voting systems and processes, as also they speed up the verification of the results.

However, computer networks are target of systematic attacks. These attacks can affect the availability of the process and, moreover, intervene with the results of the election or affect its fundamentals. To guarantee that the principles demanded for a safe election are respected is the purpose of the systems based on cryptographic protocols.

Many proposals of systems have been made. Some use certain degree of functional obscurity as warranty against attacks; others use widely known techniques, even so with high degree of complexity.

The present work presents the proposal of a complete system for execution of a secure digital voting. The system is based on a simple protocol, however complete, that uses widely known cryptographic techniques. The protocol is gradually described, and its efficiency against the possible attacksis proven.

The text still presents some other protocols created for this same purpose. Finally, the prototype of a software system that uses the considered protocol is presented .

Keywords: secure voting, protocol, cryptography

1 INTRODUÇÃO

O presente trabalho objetiva apresentar os estudos realizados e os resultados obtidos referentes a um sistema de votação seguro para uso em redes de computadores. Dessa forma, são abordados dois aspectos relevantes da vida contemporânea, em evidência sobretudo no atual momento: o sigilo sobre a informação e eleições com resultados confiáveis.

1.1 Motivação

A criptografia surgiu como uma técnica militar, elaborada para permitir a transferência segura e sigilosa de informações de estado. Assim, era utilizada sobretudo em períodos de guerra, quando conspirações e estratégias de ataque e defesa deviam ser rigorosamente mantidas em segredo.

Durante muito tempo, a criptografia exigia o emprego de especialistas, pois os sistemas de cifragem e, por conseqüência, de decifragem, eram métodos trabalhosos e, freqüentemente, também deviam fazer parte do segredo. Na Segunda Guerra Mundial, a técnica ganhou um novo impulso, com a automação dos métodos, através de aparatos eletromecânicos. O mais notável deles foi a máquina chamada Enigma (SINGH, 2001), empregada pelos alemães.

De outro lado, as técnicas para quebrar um criptossistema receberam a significativa contribuição de Allan Turing. Dessa forma, também a criptoanálise era aprimorada e automatizada.

Atualmente, tem-se uma rede mundial de computadores, a *Internet*. Nesse contexto, os segredos militares já não são mais a principal demanda da criptografia, pelo menos em quantidade. Há a necessidade de se efetuar transações comerciais com segurança e privacidade; transferências pecuniárias em contas bancárias; autenticação de ingresso em redes privativas de computadores.

Paralelamente, há discussão sobre os sistemas utilizados em eleições. Fraudes eleitorais são tanto antigas quanto atuais. Dois episódios, entretanto, merecem destaque por abordarem temas relacionados ao presente trabalho.

Nas eleições presidenciais dos Estados Unidos da América, no ano de 2000, houve a questão sobre a legitimidade do presidente dado como eleito . Em um sistema de cédulas marcadas manualmente, a contagem mecânica parece ter provocado não apenas uma sensível distorção dos resultados finais, mas a completa alteração do candidato eleito. Então, a confiabilidade em um sistema eleitoral é fundamental: o voto depositado deve ser adequadamente computado.

No Brasil, há a discussão permanente acerca das urnas eletrônicas. O sistema operacional instalado em tais máquinas é proprietário. O software propriamente dito fica disponível para verificação durante cinco dias apenas. Soma-se à obscura confiabilidade uma obscura privacidade: não há garantia de que o voto não fique vinculado ao eleitor,

pois o número do seu título é previamente digitado no microterminal para habilitar o procedimento de voto no terminal do eleitor.

Considerando-se tais aspectos, é notória a necessidade da vinculação da transparência com a automação, reduzindo o risco de fraudes e ampliando as possibilidades de auditoria e recontagem. Dessa forma, a criptografia computadorizada fornece ferramentas adequadas para atender às demandas de um processo eleitoral automatizado e seguro.

1.2 Conceitos Básicos

A seguir são apresentadas algumas definições. Elas estão agrupadas de acordo com o tema relacionado, facilitando assim comparações e análises. Entretanto, não é objetivo desta seção fazer explanações exaustivas ou detalhadas, mesmo porque, alguns tópicos podem já ser de amplo domínio.

1.2.1 Criptografia

Criptografia é a arte ou ciência de tornar informações confusas, ilegíveis àqueles que não podem ou não devem ter acesso a elas. O processo empregado, o ato e o efeito de se usar criptografia são chamados de **encriptação** ou mesmo de criptografia. Uma mensagem original, antes de passar pelo processo de encriptação, é chamada **texto claro**, **texto original** ou ainda **texto plano**. Depois de passar pelo processo, o resultado obtido é o **texto encriptado** ou ainda **texto criptografado**.

A pessoa (ou entidade) que envia uma mensagem é chamada **remetente**, da mesma forma que a pessoa que recebe a mensagem é chamada **destinatário**.

Quando o destinatário recebe uma mensagem encriptada, ele deve ser capaz de reverter o processo, ou seja, obter a mensagem original. Essa tarefa é chamada **decriptação**. O texto criptografado é, então, **decriptado**, produzindo o texto original.

Existem diversas técnicas de criptografia. As duas principais são as cifras e os códigos. **Código** é o processo que altera, de alguma forma, as palavras ou morfemas da mensagem. Normalmente, esse processo é feito através da substituição de palavras por outras e, por tal motivo, é dito que faz uso de dicionários, tanto no processo de encriptação quanto no de decriptação. **Codificar**, **decodificar**, **codificação** e **decodificação** são as ações e efeitos da aplicação de códigos. **Cifra** é o processo que altera, de alguma forma, pequenas quantidades de informação, menores do que morfemas, como caracteres ou *bytes*. Esse processo pode usar substituição de letras por outras, ou transposição das letras, ou ainda combinações de substituições e transposições. **Cifrar**, **decifrar**, **cifragem** e **decifragem** são os atos e efeitos da aplicação de cifras.

O resultado do processo de criptografia depende não somente do texto original, mas também de um segundo parâmetro, chamado **chave**. A chave pode ser, e normalmente é, uma senha, representada por uma seqüência de bits significando um número, uma frase ou alguma outra informação digital.

O conjunto formado pelo método de encriptação, chave, texto original e texto encriptado é denominado **criptossistema**. A **premissa de Kerckhoffs** (SINGH, 2001) diz que a robustez de um criptossistema não deve ser baseada no segredo sobre o método de criptografia empregado, mas apenas no sigilo sobre a chave utilizada. Obviamente, quanto mais chaves distintas puderem ser empregadas em um criptossistema, mais robusto ele será.

Atacante é a pessoa que não é nem remetente tampouco destinatário da mensagem, mas tenta descobrir informações sobre o criptossistema. Para tanto, ele faz uso de técnicas estudadas na criptoanálise. **Criptoanálise** é a arte ou ciência que estuda formas de descobrir o método de encriptação empregado, ou a mensagem original, ou a chave utilizada, ou ainda qualquer combinação dessas informações. É dito que o objetivo da criptoanálise é quebrar um criptossistema.

Criptografia e criptoanálise são campos de estudo de uma ciência chamada **criptologia**.

Quando um criptossistema utiliza a mesma chave, tanto na cifragem quanto na decifragem, ele é chamado de sistema de **criptografia simétrica**. Em criptossistemas simétricos, o algoritmo de decifragem é o contém as operações inversas na ordem inversa das respectivas operações do algoritmo de cifragem.

Exemplos de criptossistema simétrico são os algorimos DES (*Data Encryption Standard*), IDEA (*International Data Encryption Algorithm*) e o Rijndael, o novo padrão AES (*Advanced Encryption Standard*) adotado pela NIST (*National Institute of Standards and Technology*) dos Estados Unidos da América.

Entretanto, um criptossistema pode usar duas chaves distintas, uma específica para cifragem, e outra específica para a decifragem. Nesse caso, é chamado de sistema de **criptografia assimétrica**. Essas chaves são, via de regra, matematicamente relacionadas. Assim sendo, cada usuário tem um **par de chaves**, uma para cifrar e outra para decifrar. É fácil observar que, para cada usuário, a única chave que necessita ser guardada em sigilo é a chave de decifrar. Por esse motivo é chamada de **chave privada** (ou secreta). A chave de cifrar de cada usuário pode ser de conhecimento público, e por isso é chamada **chave pública**. Para cifrar uma mensagem a um determinado usuário, o remetente usa a chave pública do destinatário. Para decifrá-la, o destinatário usa sua própria chave secreta.

Exemplo de criptossistema assimétrico são os algoritmos RSA (Rivest Shamir Adleman) e Diffie-Hellman.

A criptografia contemporânea e computadorizada utiliza sobretudo cifras. De um lado, criptossistemas simétricos fazem uso de transposição, substituição, compactação e expansão de caracteres. Já os criptossistemas assimétricos são baseados em operações matemáticas complexas, como exponenciais, fatorações, logaritmos e operações em aritmética em módulo.

1.2.2 Assinatura

Assinatura é uma marca ou sinal que identifica a autoria de algo. Ela deve indicar quem assinou um documento, mensagem ou registro, e deve ser difícil para outra pessoa reproduzi-la sem autorização; dessa forma é feita a autenticação do assinante. Dessa forma, uma assinatura é uma prova de evidência, de cerimônia, de aprovação e de eficiência (ABA, 1996).Por outro lado, uma assinatura deve identificar o que é assinado, tornando impraticável falsificar ou alterar, tanto o documento quanto a assinatura, sem detecção; dessa forma é feita a autenticação do documento.

O conceito de **assinatura digital** foi abordado inicialmente por Whitfield Diffie e Martin Hellman em 1976 (SIMMONS, 1992), e obteve uma grande receptividade junto à comunidade, que buscava aplicações da idéia em problemas práticos de segurança de informações. Assinaturas digitais devem garantir os seguintes princípios (SCHNEIER, 1996):

- A assinatura é autêntica: A assinatura convence o destinatário do documento de que o assinante assinou deliberadamente o documento.

- A assinatura não é falsificável: A assinatura é a prova que o assinante, e não outro, deliberadamente assinou o documento.
- A assinatura não é reusável: A assinatura é parte de um documento, e ela não pode ser copiada ou movida para outro documento.
- Um documento assinado é inalterável: Depois de um documento ser assinado, seu conteúdo não pode ser alterado.
- A assinatura não pode ser negada: A assinatura e o documento são provas materiais. O assinante não pode negar depois que assinou o documento.

É importante ressaltar que a finalidade de uma assinatura não é tornar secreto o conteúdo de um documento. Assim, documentos assinados não são necessariamente cifrados. Além do mais, documentos assinados e não cifrados devem ser facilmente lidos pelas partes interessadas.

A publicação do algoritmo RSA em 1978 mostrou que existem métodos práticos de implementar o conceito, que desde então, vêm sendo estudados e aperfeiçoados. Existe uma propriedade encontrada na maioria dos criptossistemas assimétricos: o que é cifrado com uma chave (qualquer uma) pode ser decifrado com a outra. Essa complementação produz um resultado muito útil: a assinatura.

Para **assinar** uma mensagem, o remetente a cifra com sua própria chave secreta. A mensagem cifrada deve, então, ser decifrada com o uso da outra chave, que é pública. Ou seja, qualquer usuário pode verificar que a cifragem foi produzida com a chave secreta do remetente. Portanto, é dito que a mensagem está **assinada** pelo remetente, ou que contém a sua assinatura.

1.2.3 Funções de Resumo

Uma **função de resumo** (ou ***hash***) é uma transformação matemática que opera sobre uma mensagem de qualquer tamanho e produz um resultado de tamanho fixo. Uma função desse tipo é unidirecional, ou seja, não é invertível, por não ser injetora (documentos originais diferentes podem gerar o mesmo resumo). Embora não seja injetora, uma função de resumo deve garantir que seja muito difícil, computacionalmente trabalhoso, conseguir dois documentos distintos que produzam o mesmo resumo, ou ainda, mais improvável, obter um documento que gere um determinado resumo.

Funções de resumo usam basicamente operações de lógica booleana, deslocamentos e rotações, trabalhando de forma encadeada sobre os blocos nos quais o documento original foi dividido.

Dois dos algoritmos mais usados são o MD5, que gera um resumo de 128 bits, e o SHA, que cria resumos de 160 bits.

1.2.4 Protocolos

Segundo (HOUAISS, 2001), **algoritmo** é seqüência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas. Ou seja, um processo de cálculo, um encadeamento das ações necessárias ao cumprimento de uma tarefa, ou ainda, o processo efetivo, que produz uma solução para um problema num número finito de etapas.

Da mesma fonte, a definição de **protocolo** é o conjunto de normas reguladoras que de atos públicos, especialmente nos altos escalões de governo e na diplomacia. Também pode ser a característica do que segue normas rígidas de procedimento, formalidade.

No contexto de criptografia, um protocolo é a especificação de um conjunto completo de passos que realizam atividades criptográficas, incluindo a especificação explícita de como proceder em casos de contingência (MERTZ, 2004). Dessa forma, um algoritmo é muito mais o procedimento envolvido na transformação de dados digitais.

Protocolos são, portanto, regras mais gerais, em um nível de abstração mais elevado. Protocolos criptográficos empregam, normalmente, um ou mais algoritmos criptográficos, mas a segurança, assim como outros objetivos da criptografia, é resultado de um protocolo inteiro (IBM, 2002). Não basta serem empregados algoritmos criptográficos seguros se o protocolo envolvido tiver pontos fracos.

Por exemplo, um protocolo hipotético no qual o remetente cifra sua mensagem com um algoritmo criptográfico simétrico inquebrável. O protocolo determina que remetente deve enviar a mensagem para o destinatário. Como o algoritmo empregado é simétrico, a chave de encriptação deve ser enviada conjuntamente, mas em claro. Obviamente uma captura do pacote contendo a mensagem e a chave por um atacante acaba com a segurança do sistema. A fraqueza, nesse caso, é do protocolo empregado, não do algoritmo.

1.3 Estrutura do Documento

No próximo capítulo, são colocados os requisitos de uma votação segura, e como eles podem ser satisfeitos.

No terceiro capítulo, há uma descrição dos protocolos criptográficos existentes, bem como sobre a situação da urna eletrônica brasileira. São feitas considerações sobre cada um, analisando suas vulnerabilidades.

No quarto capítulo, é apresentado o protocolo que fundamenta este trabalho, tanto no nível descritivo quanto analítico frente aos requisitos apresentados no capítulo anterior.

As soluções tecnológicas possíveis e a escolhida, assim como o protótipo desenvolvido são descritos no quinto capítulo.

No sexto e último capítulo, apresenta-se a conclusão, com análise do que foi realizado e propostas para trabalhos futuros.

2 ELEIÇÕES

O termo eleições que aqui se aplica não se refere somente ao tipo usual de eleições. Por eleições deve ser entendida qualquer votação, indicação, referendo, plebiscito, etc. Na verdade, no contexto deste trabalho, eleição significa qualquer procedimento em que uma ou várias pessoas devem se manifestar, de forma anônima, de tal modo que sua manifestação - ou melhor dizendo, o registro dela - seja de alguma forma computado.

Esse procedimento, portanto, não é necessariamente uma eleição no sentido específico da palavra, nem tampouco uma votação. Por exemplo, pode-se imaginar uma situação em que pessoas devem se manifestar sobre algum dado familiar sigiloso, como em um censo sanitário. As pessoas não precisam se identificar por terem determinada doença, mas é importante que o governo saiba quantas pessoas tem determinadas doenças, e em que regiões elas estão.

2.1 Características de uma Eleição

Uma eleição tradicional, não automatizada, possui certas características fundamentais que, com grande freqüência, influenciam também a estruturação de sistemas de votação eletrônicos. Algumas dessas características são os participantes e as fases em que o processo pode ser dividido (RIERA, 1998).

Quanto aos participantes, podem ser divididos basicamente entre votantes, também chamados eleitores, e autoridades. Os votantes constituem obviamente o público alvo do processo eleitoral; são eles que determinam, através de seus atos e escolhas, qual é o resultado de uma eleição. As autoridades são entidades ou pessoas envolvidas no processo, para garantir sua evolução; sua atividade é exercida no transcorrer da eleição e suas escolhas e atos não devem influir no resultado da mesma.

Esquemas de eleição simples podem possuir apenas uma autoridade. Dependendo de como o sistema é montado e a quais requisitos satisfaz, essa autoridade deve possuir maior ou menor grau de confiabilidade. Isso acontece pelo poder que essa única autoridade pode ter em alterar o resultado; em que momentos e por quais meios pode fazê-lo. Esquemas mais complexos podem exigir um maior número de autoridades. Nesse caso, ainda que se faça necessária alguma confiança, o poder de influência no processo, ou seja, a possibilidade de alterar o resultado, é diluído entre essas autoridades. Assim, uma fraude exige a combinação dessas autoridades envolvidas, e como todas são e devem ser, por definição e princípio, confiáveis, reduz-se substancialmente as oportunidades de alteração do resultado.

Em relação às fases da eleição, podem ser distinguidas basicamente três. Quem participa de cada uma depende de como o esquema é estruturado, ou seja, qual o protocolo utilizado. A primeira fase constitui-se no registro. Nessa fase, de uma população de possíveis eleitores, apenas alguns, de acordo com critérios estabelecidos, são credenciados para serem, de fato, eleitores. Esse procedimento deve ser feito por

uma autoridade e é possível que seja desejável o conhecimento público dos eleitores credenciados.

Na fase de votação, cada eleitor recebe uma cédula e a marca, transformando-a em um voto. Esse voto deve ser entregue a uma autoridade. Dependendo de como o esquema é estruturado, pode haver mais de uma autoridade envolvida nessa fase.

A terceira e última fase constitui-se na contagem dos votos, também chamada escrutínio. Terminado o recebimento de votos, a autoridade responsável por essa fase faz a contabilização dos votos, calcula os resultados e os publica.

Adicionalmente, pode ser realizada uma classificação quanto ao meio, isto é, o documento que é gerado durante o processo por cada eleitor e que, quando contabilizado, é um dos determinantes do resultado. Esse documento é normalmente único para cada votante, mas possui funcionalidades bem distintas. Em um certo momento é apenas uma cédula. Ela pode ter garantias quanto à sua autenticidade, como, por exemplo, um timbre ou rubricas da autoridade envolvida. Entretanto, uma cédula não tem valor no resultado da eleição. É apenas quando ela passa pelo eleitor, que a transforma em voto, que realmente ganha influência no resultado. Um voto é o segundo papel que esse documento pode ter e, devido à sua importância, uma série de garantias e cuidados devem ser tomados, a fim de satisfazer certas restrições e impedir alterações indevidas.

2.2 Requisitos Gerais

Uma eleição segura apresenta vários princípios fundamentais (RIERA, 1999). São eles:

I. Exatidão. Uma eleição é exata se (1) não for possível alterar votos válidos, se (2) não for possível eliminar votos válidos da contagem final e, finalmente, se (3) votos inválidos não forem considerados.

II. Democracia. Uma eleição é democrática se (1) permitir que somente eleitores cadastrados votem e se (2) cada eleitor puder votar uma única vez.

III. Privacidade. Uma eleição é privada se (1) a autoridade envolvida na fase de votação não conseguir rastrear um eleitor a partir de seu voto; se (2) nenhum eleitor conseguir provar qual foi seu voto e se (3) os votos permanecerem em segredo até o final do processo de contagem.

IV. Verificabilidade. Uma eleição é verificável se (1) cada eleitor pode verificar individualmente se o seu voto foi computado adequadamente.

O primeiro requisito do princípio de privacidade é conhecido com anonimato e o segundo como propriedade de não-coação.

A combinação dos princípios acima produz requisitos gerais (SCHNEIER, 1996), que são explanados a seguir.

1) Somente pessoas autorizadas podem votar. Isso significa que nem todas as pessoas tem o direito de participar de uma determinada votação. Deve ser possível barrar pessoas que não têm o direito de voto.
2) Ninguém pode votar mais de uma vez. Esse requisito é conhecido como *uma pessoa, um voto*. Isso significa que, a menos que seja explicitamente acordado o contrário, cada pessoa tem o mesmo peso decisório que cada uma de todas as outras pessoas votantes. Também significa que o eleitor deve fazer, em um único voto, a melhor escolha ou definição possível; ele não pode dar um voto a cada opção que o agrade.
3) O voto é secreto. Este é um dos requisitos fundamentais da democracia moderna. O eleitor pode manifestar sua opinião antes e depois do processo eleitoral, mas de

fato ninguém pode comprovar o que realmente contém o voto de um determinado eleitor. O voto, depois de recolhido pela urna, passa a ser completamente desvinculado do eleitor que o fez e deve ser impossível reconhecer a identidade do eleitor pela inspeção do voto.

4) Ninguém pode duplicar o voto de ninguém. Isso significa que cada voto é único e tem valor único, não podendo ser duplicado ou multiplicado. Não pode haver meios de se copiar um voto.
5) Ninguém pode alterar o voto de ninguém. Uma vez depositado o voto, ele não pode ser alterado, em qualquer parte do processo, seja por outro eleitor, seja pela junta apuradora, seja por quem for. O voto depositado deve ser inviolável.
6) Cada eleitor deve poder verificar se o seu voto foi computado. Esse é um requisito essencial, mas nem sempre implementado. Significa que o eleitor tem o direito, e o sistema deve garantir isso, de poder verificar o seu voto no cômputo final dos votos. E ele deve poder fazer isso de uma maneira que ainda tenha garantido o item 3, que determina o sigilo do voto.

Adicionalmente, eleições seguras podem permitir que as pessoas saibam quem votou e quem não votou. Esse requisito, entretanto, não é fundamental e depende do contexto da eleição em si.

2.3 A Eleição no Brasil

O sistema de eleições no Brasil é regido pela Legislação Eleitoral (TRIBUNAL, 2004). De um modo geral, ela define regras para todos os requisitos acima, inclusive o adicional, já que o voto é obrigatório e o eleitor deve comparecer a uma seção eleitoral quando da ocorrência de eleições e, se não o fizer, sua ausência é depois punida com o que for cabível aplicar.

Dessa forma, através do caderno de presença da seção eleitoral, fica-se sabendo quem votou e quem não votou. Mas o sistema eleitoral brasileiro tem mais um requisito: o eleitor deve poder comprovar de que participou de determinada eleição.

Assim, sempre que vota, o eleitor ganha um pequeno recibo, com código de barra e as Armas Nacionais, identificando o pleito do qual ele participou. Esse comprovante pode ser exigido em diversas circunstâncias na vida do eleitor, como na obtenção de empregos, de diplomas ou em outras situações.

O sistema de votação tradicional, com voto em cédulas de papel e apuração humana, tinha vários pontos críticos. A maior parte deles se encontrava no momento de apuração dos votos (BRUNAZZO FILHO, 2003). Alguns deles eram:

1) As cédulas eram facilmente falsificáveis. Mesmo que rubricadas pelos mesários, algum eleitor bem preparado conseguiria forjar as cédulas.
2) No momento da apuração e da constatação de cédulas adicionais, a menos por fraude grosseira, era difícil ou mesmo impossível descobrir as cédulas falsas. O ato corriqueiro, nessa situação, era impugnar a urna inteira.
3) Os escrutinadores tinham tarefa difícil para validar e contar os votos, muitas vezes rasurados, e ao mesmo tempo, tinham poder para poder fraudar a contabilização ou adulterar votos, marcar votos em branco, etc. Não se afirma que essa fosse a prática corrente, mas o sistema permitia essa brecha. Devido a isso, o escrutínio sempre era acompanhado pelo maior número possível de fiscais de partido.

Diante dessas situações, os requisitos 2, 4, 5 e seis não eram completamente satisfeitos, a menos que se acreditasse na reputação completamente ilibada de todos os mesários, escrutinadores e fiscais de partidos envolvidos.

O advento da urna eletrônica trouxe melhoras substanciais ao processo. Embora ainda se levantem algumas suspeitas a respeito de seu funcionamento (BRUNAZZO FILHO, 2004), o método parece bem mais confiável. Os principais pontos suspeitos são:

- O eleitor ainda não consegue perceber que seu voto está realmente sendo computado. Parece haver falta de garantias sobre o algoritmo apresentado, e falta de garantias de que o algoritmo apresentado seja, de fato, o que é usado nas urnas eletrônicas.
- O eleitor é identificado, no terminal da urna eletrônica, com seu título de eleitor. Isso poderia facilitar a inspeção do voto do mesmo.

Embora esses pontos possam parecer exagerados, já que são obtidos de uma desconfiança sobre o trabalho do TSE, eles merecem ser mais amplamente discutidos.

Adicionalmente, um ponto falho do sistema anterior de votação ainda permanece na votação eletrônica: o requisito 2. Sob a complacência de mesários - o que não é difícil, se levarmos em conta os vários cantões do Brasil - um eleitor pode votar mais de uma vez, fazendo-se passar por eleitores faltosos ou falecidos. Inclusive os próprios mesários podem praticar esse delito.

Não se deve considerar que tais desconfianças sejam preconceituosas contra o Brasil. Corrupção eleitoral e fraudes acontecem em toda a parte do mundo. Um dos pontos realmente críticos em votações no mundo todo é a complacência de mesários, quando até eleitores mortos podem votar (SCHNEIER, 2000).

De acordo com a legislação eleitoral brasileira, que torna o voto obrigatório, o eleitor deve, em várias situações, provar que está em situação regular perante a Justiça Eleitoral, ou seja, que tem participado das eleições. Nesse contexto, é adequado acrescentar um sétimo requisito:

1) Cada eleitor deve receber um comprovante de ter participado (votado) na eleição.

2.4 Soluções Iniciais

De forma a atender os sete requisitos apresentados anteriormente, algumas soluções simples com criptografia podem ser usadas e, combinadas, podem formar um robusto protocolo criptográfico.

1) Somente pessoas autorizadas podem votar. Essa restrição pode ser resolvida com assinatura do voto. Essa assinatura não é necessariamente do eleitor, mas de alguma autoridade confiável que valide e identifique a cédula de forma a garantir a sua contabilização.
2) Ninguém pode votar mais de uma vez. Cada eleitor deve possuir um identificador único, de forma que a recepção de votos detecte a existência de multiplicidade do identificador do eleitor e proceda a ação adequada.
3) O voto é secreto. Esse requisito obriga que não exista vínculo algum entre o voto e o eleitor. Essa solução é preferencial, mas difícil de ser obtida. Uma forma alternativa é fazer com que essa vinculação seja possível apenas sob certas circunstâncias, unindo informações distribuídas e com o envolvimento de autoridades confiáveis.
4) Ninguém pode duplicar o voto de alguém. Cada voto deve ser identificado de maneira única, de forma que a apuração possa detectar a existência de multiplicidade de votos e proceder a ação adequada.
5) Ninguém pode alterar o voto de alguém. Esse requisito é atendido se o voto contiver um resumo assinado. Nessa situação, qualquer alteração no conteúdo do

voto provoca a inconformidade com o resumo assinado, e o voto pode ser invalidado.

6) Cada eleitor deve poder verificar se o seu voto foi computado. Nesse requisito, alguma informação especial, de conhecimento do eleitor, mas que não o identifique, deve ser afixada junto ao voto. Essa informação pode ser usada pelo eleitor para reconhecimento posterior do voto, caso ele seja divulgado em listas de totalização. O ideal nessa situação é a geração de alguma seqüência numérica aleatória que fique de posse com o eleitor.

7) O eleitor deve receber um comprovante de ter participado (votado) na eleição. Essa solução exige novamente a utilização de assinatura. Um certificado emitido por uma autoridade confiável pode satisfazer esse requisito. A autoridade pode incluir informações que identifiquem o contexto da eleição. Pode, adicionalmente, incluir o próprio voto do eleitor, devidamente cifrado a ele, de forma a ser mais um instrumento de verificação do mesmo.

Essa inclusão, no entanto, pode ser perigosa em situações pouco democráticas: o eleitor pode ser forçado a decifrar o voto. Uma solução é fornecer mais um nível de cifragem, a uma terceira parte, também confiável. Isso impossibilita o eleitor de abrir seu voto contra a sua vontade, mas ainda permite uma verificação posterior, contando com o envolvimento dessa terceira parte.

3 SISTEMAS EXISTENTES

Neste capítulo são apresentados alguns sistemas de votação. Alguns são bastante simples, de tal forma que a análise sobre suas deficiências em relação aos requisitos exigidos de uma eleição segura é rápida e evidente. Alguns outros são mais elaborados e atendem parcial ou totalmente aos requisitos.

3.1 Tipos de Protocolos

Um protocolo é dito **arbitrado** quando uma terceira parte, desinteressada e confiável, faz parte do protocolo a fim de completá-lo: o árbitro. Ele é desinteressado em relação ao objetivo final do protocolo, e confiável porque os demais participantes devem aceitar a sua palavra como sendo verdadeira.

Um protocolo é dito **adjudicado** se pode ser dividido em duas partes, ou dois subprotocolos. Em um subprotocolo, o funcionamento é completo sem a figura de um árbitro. Entretanto, em certas circunstâncias, como uma disputa, pode ocorrer a execução do segundo subprotocolo, este sim com a terceira parte, desinteressada e confiável. Na parte não arbitrada do protocolo, devem ser colhidas evidências e provas que permitam ou facilitem a decisão do árbitro.

Finalmente, um protocolo é dito **auto-sustentável** se ele nunca requer a presença de um árbitro. O próprio protocolo é construído a eliminar disputas e dúvidas, garantido justiça e imparcialidade. Se uma das partes envolvidas tenta trapacear, a(s) outra(s) parte(s) pode(m) detectar a tentativa e bloquear o processo, ou travar o protocolo.

3.2 Conceitos

As autoridades confiáveis, participantes dos protocolos aqui apresentados, são denominadas **centrais eleitorais**. Uma central eleitoral pode receber um nome mais específico de acordo com o papel desempenhado ou com a fase do processo na qual está inserida. Essas centrais não possuem o papel de árbitro; por tal razão, estes protocolos são auto-sustentáveis.

Os protocolos apresentados no presente capítulo têm a finalidade de implementar eleições computacionalmente seguras. Eles se valem, além dos conceitos de cifragem, assinatura, algoritmo e protocolo, abordados na introdução, das características e requisitos de uma eleição segura, explanados no capítulo anterior. Para maior clareza do texto, os requisitos são reapresentados abaixo.

Uma eleição computacionalmente segura deve oferecer os seguintes requisitos (SCHNEIER, 1996):

1) Somente eleitores cadastrados podem votar.
2) Ninguém pode votar duas vezes.
3) O voto é secreto.

4) Ninguém pode duplicar o voto de alguém.
5) Ninguém pode alterar o voto de alguém.
6) Cada eleitor deve poder verificar se o seu voto foi contado.
7) O eleitor deve poder provar ter participado da eleição.

3.3 Protocolo sem Central

Este protocolo é implementado sem o uso de uma central eleitoral. O sistema faz com que cada voto passe por cada eleitor, duas vezes. Por esse motivo, é chamado de sistema de voto distribuído. Se existem *n* eleitores, então existem *n* mensagens (votos) circulando na rede. Cada mensagem é transferida *2×n* vezes. Deve existir uma ordem circular preestabelecida entre os eleitores.

O protocolo funciona da seguinte maneira:

1) Cada eleitor escolhe seu voto V e faz o seguinte:
   a) Anexa um número aleatório R_1 ao seu voto.
   b) Para cada eleitor cadastrado *j*, o voto *V* é cifrado para (com a chave pública de) *j:* $E_j(V,R)$. Isso deve ser feito ao contrário da ordem preestabelecida.
   c) Para cada eleitor cadastrado *j* ele anexa um novo número aleatório *R* e cifra para o referido eleitor. Isso deve ser feito ao contrário da ordem preestabelecida.

Supondo quatro eleitores, *A*, *B*, *C* e *D*, nesta respectiva ordem, um voto ao final do passo um terá a seguinte aparência:

$$E_A(R_5, E_B(R_4, E_C(R_3, E_D(R_4, E_A(E_B(E_C(E_D(V,R_1)))))))$$

2) Cada eleitor envia seu voto ao primeiro (pela ordem preestabelecida).
3) Seguindo a ordem da lista, cada eleitor, a partir do primeiro, faz o seguinte:
   a) Decifra todas as mensagens.
   b) Retira todos os números aleatórios de sua etapa.
   c) Passa os votos para o próximo da lista.

Isso significa que, quando o último da lista, no caso *D*, receber os votos, eles terão a seguinte aparência:

$$E_D(R_4, E_A(E_B(E_C(E_D(V,R_1)))))$$

O último eleitor também faz a mesma coisa. No caso, *D* remete a *A* o seguinte pacote:

$$E_A(E_B(E_C(E_D(V,R_1))))$$

O primeiro da lista (*A*) recebe os votos com essa forma e os decifra. Ela assina os votos e os envia ao próximo. Isso significa que *B* recebe um pacote contendo:

$$S_A(E_B(E_C(E_D(V,R_1))))$$

4) Seguindo a ordem da lista, cada eleitor, a partir do segundo, faz o seguinte:
   a) Verifica a assinatura.
   b) Retira a assinatura.
   c) Decifra a mensagem com sua própria chave privada.
   d) Verifica se o seu voto está incluído (pelo seu número aleatório).

e) Assina.
f) Envia para o próximo na lista.

O que o último obtém são votos com números aleatórios. Ele deve então assinar todos dos votos e enviar aos demais eleitores.

5) Cada eleitor, por sua vez, verifica a assinatura, contabiliza se seu voto está no meio. Os votos são, então, computados.

O método funciona porque a cada rodada, todos conseguem verificar se o seu voto está presente, através dos números aleatórios gerados. No final, o voto também pode ser verificado através do primeiro número aleatório.

Entretanto, há alguns problemas intrínsecos: a responsabilidade pela correção do processo recai sobre todos os votantes. Todos os votantes também devem também estar aptos a proceder esse complicado mecanismo. O protocolo exige um processamento computacional enorme, além do que centraliza muito poder no último eleitor da lista, que sabe do resultado antes dos demais. Além disso, também é possível que um eleitor copie um voto de outro eleitor.

3.4 Protocolos de Uma Central

Os seguintes protocolos são analisados em relação aos requisitos anteriores, e suas definições são bem simples. Por esse motivo, não é usada uma notação mais formal, pois podem ser compreendidos facilmente pela descrição textual.

Certos conceitos utilizados, entretanto, quando combinados, formam protocolos mais robustos, como aqueles analisados na próxima seção.

3.4.1 Voto Cifrado à Central de Eleição

Existe uma Central de Eleição (CE), com chave pública disponível aos eleitores. Esse protocolo consiste nos seguintes passos:

1) Cada eleitor cifra seu voto com a chave pública da CE.
2) Cada eleitor envia seu voto à CE.
3) A CE decifra os votos, realiza a contagem e publica os resultados.

O protocolo é extremamente simples e falho. O único requisito respeitado é o 3 - cada voto é secreto.

3.4.2 Voto Assinado e Cifrado à Central de Eleição

Existe também uma Central de Eleição (CE). Adicionalmente, a CE tem cadastrados todos os eleitores, e tem conhecimento sobre suas chaves públicas. Os eleitores, por sua vez, também dispõem da chave pública da CE. O protocolo consta de:

1) Cada eleitor assina seu voto com sua chave secreta.
2) O voto assinado é cifrado com a chave pública da CE.
3) Cada eleitor envia seu voto à CE.
4) A CE decifra cada voto.
5) A CE verifica a assinatura de cada voto.
6) A CE conta os votos válidos e publica o resultado.

Esse protocolo implementa com facilidade os requisitos 1, 2, 4 e 5, mas deixa de cumprir o 3 - os votos não são mais secretos. Os requisitos 6 e 7 também não são cumpridos.

3.4.3 Voto com Assinatura Cega

Antes de verificar o funcionamento deste protocolo, é preciso especificar o que é uma *assinatura cega*. O termo significa que alguém pode assinar um documento sem saber exatamente do que se trata. A matemática empregada é derivada basicamente do RSA. O funcionamento é exemplificado a seguir.

A pessoa *B* tem uma chave pública *e*, e uma chave privada *d*, e um módulo público *n*, um dos componentes do par de chaves. A pessoa *A* quer que *B* assine uma mensagem *m* cegamente.

1) *A* escolhe um valor aleatório, *k*, chamado fator de cegamento ou de ocultação. Ela então cega a mensagem calculando
   $t=m\times k^e \bmod n$
2) *B* assina a mensagem cega *t*:
   $t^d= (m\times k^e)^d \bmod n$
3) *A* retira o fator de cegamento
   $s=t^d/k \bmod n$
4) O resultado é a mensagem original *m* assinada por *B*:
   $s=m^d \bmod n$

O protocolo então, é realizado com uma Central Eleitoral (CE), e funciona da seguinte maneira:

1) Cada eleitor gera 10 ou mais conjuntos de mensagens, cada conjunto contendo um voto válido para cada possibilidade. Cada mensagem também contém um número aleatório, grande o suficiente para evitar duplicidades.
2) Cada eleitor cega todos os seus conjuntos, e os envia para a CE.
3) A CE verifica se o eleitor ainda não votou. Ela seleciona 9 conjuntos (todos menos 1) e pede ao eleitor os fatores de cegamento. Abrindo as mensagens, a CE verifica se os conjuntos estão bem formados. A seguir, a CE assina os votos do conjunto ainda cego.
4) O eleitor recebe o seu conjunto assinado e retira o fator de cegamento. A seguir, ele escolhe qual voto deseja usar, e elimina os demais.
5) O eleitor cifra seu voto e envia para a CE.
6) A CE decifra o voto, confere sua assinatura, registra o número aleatório (e verifica duplicações) e faz a computação dos votos.
7) A CE publica os resultados, listando cada voto com o respectivo número aleatório.

Através desse sistema, o eleitor pode conferir o seu voto na publicação final dos resultados. Os votos não são duplicados, pois a CE pode controlar os votos que já tenha recebido. Entretanto, não há garantias de que a CE não consiga forjar votos. Ela mesma pode assinar votos cegos para si e depois computá-los. Ela também pode permitir que eleitores inaptos votem.

3.5 Protocolos de Duas Centrais

Os seguintes protocolos utilizam duas centrais eleitorais. Elas desempenham funções semelhantes, mas os protocolos são significativamente diferentes em sua operação e nos requisitos atendidos.

3.5.1 Voto sem Assinatura

Esse protocolo foi proposto por Nurmi, Salomaa e Santean (CRANOR, 1997). As duas centrais são a Central de Validação (CV) e a Central de Conferência (CV). Na

verdade, as tarefas de validação dos eleitores cadastrados, de contagem e publicação dos resultados são compartilhadas entre ambas centrais. Seu funcionamento é o seguinte:

1) A CV distribui para cada eleitor um número secreto identificador R.
2) A CV envia para a CC a lista de todos os números R emitidos, sem correspondência com os eleitores.
3) Cada eleitor escolhe uma chave de cifragem simétrica K. Com essa chave, cifra tanto o seu voto V, quanto o número R: E [(V, R), K]
4) O eleitor envia o pacote cifrado acompanhado do respectivo número R, em claro, para a CC:{ E [(V, R), K], K }

Nesse ponto, a CC pode reconhecer que os votos são válidos pela conferência do número K, enviado em claro. Não pode, entretanto, estabelecer ligação com os votantes nem contabilizar o voto, pois está cifrado.

1) A CC publica uma lista de todos os pacotes cifrados.
2) Cada eleitor envia a CC a chave de decifragem K.
3) Quando o processo de votação acaba, a CC publica uma lista de todos os votos com os respectivos pacotes cifrados.

O protocolo permite que o eleitor confira seu voto. Além disso, votos válidos não podem ser desconsiderados. Entretanto, apresenta também alguns problemas. A comunicação entre o eleitor e a CC deve ser anônima e, mais grave, o eleitor precisa entrar em contato uma segunda vez, fornecendo a chave para decifragem do voto.

3.5.2 Voto com Assinatura

Neste sistema, existem duas centrais eleitorais, a de Cadastramento (CC) e a de Votação (CV). A CC tem todos os eleitores previamente cadastrados, tendo conhecimento, inclusive, sobre suas chaves públicas. De outra parte, a CV tem sua chave pública disponível aos eleitores. O protocolo segue os seguintes passos:

1) Cada eleitor envia uma mensagem assinada para a CC, solicitando um número de validação.
2) A CC verifica a assinatura do eleitor, e envia para ele um número aleatório de validação K, cifrado com a chave pública do mesmo. Ela mantém uma lista de todos os números K gerados, e também uma lista de todos os destinatários, para evitar que alguém tente votar duas vezes.
3) A CC envia a lista de números de validação K para a CV, devidamente assinada e cifrada.
4) Cada eleitor escolhe um número aleatório de identificação R. Ele cria uma mensagem com o seu voto, o número de identificação R e o número de validação K, cifrando essa mensagem com a chave pública da CV. Ele envia o texto cifrado à CV.
5) A CV decifra o texto recebido. Ela verifica o número K (de acordo com a lista recebida da CC), registra o número R e conta o voto.
6) A CV publica o resultado, listando cada voto com o número R gerado pelo respectivo eleitor.

Com esse protocolo, o eleitor consegue verificar se o seu voto foi computado através das listagens contendo os votos e os números R, que foram gerados pelos eleitores. Portanto o requisito 6 é satisfeito.

A CV não sabe de nenhuma ligação entre os números K gerados pela CC e os eleitores, porque a CC apenas manda uma listagem com os números. Dessa forma a CV não consegue identificar os eleitores. Quando a CV faz a publicação dos votos com a seqüências R, ela não publica os números K. Isso garante que a CC não pode reconhecer

o eleitor que gerou cada voto através da publicação dos resultados. Portanto, requisito 3 é satisfeito: o voto é secreto.

Somente eleitores previamente cadastrados podem votar, satisfazendo o requisito 1, já que somente aqueles que possuem assinatura reconhecida pela CC é que ganham os números K. De outra parte, como a CC mantém uma lista de números K fornecida aos eleitores, ela evita que eles possam votar duas vezes, satisfazendo, desta forma, o segundo requisito.

A CV não pode falsificar votos porque os votos são identificados, quando da publicação, pelos números R. Também não pode inventar votos, porque a CC sabe quantos eleitores estavam aptos a votar, e pode rastrear a falsificação. Entretanto, a CC pode autorizar eleitores inaptos a votar, ou ainda autorizar múltiplas vezes eleitores a votar. Esse risco é minimizado se a CC publicar lista de eleitores para conferência.

O requisito 3 é violado se, e somente se, as duas centrais cruzarem seus dados, que contém conjuntamente os números K, R e as identificações dos eleitores. Contudo, as centrais eleitorais são consideradas autoridades confiáveis e esse comportamento não é admissível.

O protocolo proposto neste trabalho é fundamentado nesses dois últimos protocolos. Como os apresentados a seguir, possui três centrais eleitorais, mas é realizado com menor complexidade.

3.6 Protocolos de Três Centrais

Os protocolos mais robustos são os de três centrais. Eles atendem a quase todos os requisitos de uma eleição segura. As centrais desempenham, comumente, papéis ligados a cada uma das três fases básicas de uma eleição tradicional: alistamento, votação e escrutínio.

3.6.1 Protocolo Sensus

O protocolo Sensus foi proposto por Cranor e Cytron (CRANOR, 1997). Possui três centrais, denominadas Central de Votação (CV), Central de Validação (CA) e Central de Contagem (CC). A atividade de alistamento é considerada coadjuvante e por isso, pode não ter uma central automatizada específica.

De início é feito o cadastro dos eleitores. Nesse cadastro constam seus nomes, chaves públicas e identificadores ID. Também há um campo booleano indicando se o eleitor já votou. O funcionamento segue os seguintes passos:

1) O eleitor vota em uma cédula na CV. Esse processo é totalmente feito às claras, o que exige confiança total do eleitor na CV. O resultado é o voto V.
2) A CV cifra o voto V com uma chave de cifragem S_e e calcula seu resumo, obtendo uma mensagem m.
3) A CV cria um número aleatório grande K, para servir de fator de cegamento.
4) A CV cria uma mensagem b, consistindo na cifragem cega (feita com o número K) do resumo m para a Central de Validação CA.
5) A CV assina a mensagem b com a chave privada I_d do eleitor, obtendo B.
6) A CV envia a CA um pacote cifrado contendo b, B e a ID do eleitor.
7) A CA recebe o pacote e o decifra.
8) A CA confere a assinatura de B a partir da ID e de b.
9) A CA marca o campo booleano como verdadeiro no registro ID no cadastro de eleitores.
10) A CA assina a mensagem b e a cifra para CV.

11) A CA envia o pacote acima para CV.
12) A CV decifra o pacote, obtendo b assinado pela CA.
13) A CV retira o fator de cegamento K, obtendo o resumo m assinado por CA.
14) A CV confere a assinatura da mensagem m.
15) A CV envia, cifrado para CC, um pacote contendo o voto original V cifrado com a chave S_e e o seu resumo m assinado pela CA.
16) A CC recebe o pacote e o decifra.
17) A CC confere e retira a assinatura do resumo e verifica se o resumo pertence ao voto.
18) A CC assina o voto cifrado e atualiza a lista de recibos.
19) A CC envia o recibo e o voto cifrado e assinado de volta à CV.
20) A CV confere a assinatura da CC e manda de volta para a CC o número do recibo em conjunto com a chave de decifragem S_d. O recibo é também enviado ao eleitor.
21) A CC decifra o voto com a chave de decifragem S_d, computa o voto e atualiza os resultados.

O protocolo Sensus garante, em uma primeira análise, quase todos os requisitos importantes de uma eleição segura. O eleitor, porém, não consegue conferir seu voto. Além disso, há, também, seu ponto fraco: a total confiança depositada na Central de Votação, a ponto de ela poder assinar uma mensagem pelo eleitor.

3.6.2 Protocolo Farnel

Este protocolo foi proposto em (DEVIGILI, 2001). Nele são previstas as centrais de Alistamento (CA), de Votação (CV) e de Escrutínio (CE). São necessárias ainda duas cestas, C1 e C2. O protocolo tem o funcionamento descrito a seguir.

Na fase de configuração e alistamento, as centrais depositam seus certificados em um diretório público. São geradas todas as possíveis combinações de votos, e cada uma dessas combinações é assinada pela AE, depois colocada também no diretório. É nesse momento que é realizado o cadastro dos eleitores junto à CA, sendo atribuído, a cada um, um número único identificador. Esses números são incluídos na lista de votantes.

Já na fase de votação, os passos podem ser descritos como:

1) Cada votante V se autentica perante a CV. Essa autenticação inclui informações e certificados que garantam a exatidão da eleição.
2) A CV produz uma cédula em branco e a envia para a CE.
3) A CE assina a cédula e a remete de volta à CV.
4) A CV envia a cédula em branco assinada ao eleitor V.
5) V verifica a assinatura e a retira, obtendo a cédula original em branco.
6) V assina a cédula em branco. V faz seu voto e o cifra para CE com fator de ocultação.
7) V envia para a CV um pacote assinado e cifrado contendo a cédula em branco (assinada), o voto (cego) e seu número identificador.
8) A CV decifra esse pacote e o repassa à CE.
9) A CE confere a assinatura do envelope e assina o voto cegado. Atualiza a lista de votos entregues.
10) A CE envia o voto cego assinado de volta para a CV.
11) A CV repassa o voto ao eleitor V.
12) O eleitor V retira o fator de ocultação e obtém seu voto assinado.
13) V deposita no cesto C1 seu voto, juntamente com identificador.

14) C1 recebe o voto assinado e confere, junto à CE, se o respectivo identificador ainda não teve voto computado.
15) C1 retira uma cédula aleatoriamente e a envia para o eleitor V.
16) O eleitor V deposita a cédula recebida em C2.

Na fase de encerramento e apuração, a CE retira os votos restantes que estiverem em C1 e os deposita em C2. Assim, todos os votos assinados ficam neste cesto. O resultado final da votação é obtido pela diferença entre os votos totais ao final e os votos gerados no início, com todas as combinações possíveis.

O protocolo satisfaz aos requisitos propostos. Entretanto, há de ser considerada a sua complexidade. Há necessidade de assinatura cega e geração de todas as combinações possíveis de votos. Além disso, o cesto C1 é constituído na verdade, de uma rede de mistura, a fim de guardar o anonimato dos votantes. Uma rede de mistura é um conjunto de servidores que repassam mensagem adiante entre si. Eles garantidamente repassam as mensagens, mas não devem informar de onde vieram nem guardar informações a esse respeito. Todos esses fatores somados exigem um considerável suporte computacional.

3.7 Considerações

Os protocolos apresentados anteriormente possuem algumas características interessantes, soluções reaproveitadas em outros. O que pode ser observado, de forma geral, é que quanto mais requisitos são atendidos, mais cresce a complexidade do protocolo. Por esse motivo, protocolos de uma única central eleitoral são insatisfatórios para a maioria dos casos de aplicações reais.

Os protocolos apresentados de duas e de três centrais, entretanto, se aproximam mais das soluções desejadas. Dois deles, porém, podem se tornar impraticáveis sob o ponto de vista da realidade. O que funciona baseado no voto distribuído é completamente inviável em situações onde exista um número significativo de eleitores. Além do mais, se um eleitor parar, todo o processo é travado.

Por outro lado, os protocolos baseados em assinatura cega requerem que o eleitor ou o sistema simule todas as possíveis combinações de votos. Isso pode ser fácil de implementar num plebiscito sobre monarquia ou república, mas não em uma votação real onde há algumas dezenas de candidatos para cada cargo.

O protocolo mais realista é o que utiliza duas centrais eleitorais com assinatura. Ele torna-se frágil se houver uma comunicação demasiada entre as centrais, havendo cruzamento de informações, podendo, então, haver violação sobre o sigilo do voto. Ainda assim, este protocolo guarda muitas semelhanças ao processo realmente utilizado em votações tradicionais e serve de base para a proposta do protocolo apresentado no capítulo a seguir.

3.8 Implementações

A seguir são descritas algumas implementações de sistemas seguros de votação eletrônica. Alguns são realizações de protocolos mencionados anteriormente; outros são sistemas comercias. Por fim, é abordada a urna eletrônica utilizada na eleição brasileira.

3.8.1 Versões Acadêmicas

O protocolo Sensus foi implementado (CRANOR, 1997) por uma equipe da Washington University. Os módulos foram desenvolvidos em C e Perl sobre plataformas Unix com suporte a CGI. Rodavam em servidores separados, para aumentar a confiabilidade do sistema. Também foi elaborado um módulo específico para o registro dos eleitores.

O protocolo Farnel ganhou implementações por equipes da UFSC (CUSTÓDIO, 2002). A primeira implementação consistia de aplicações rodando uma versão simplificada do protocolo. Essa simplificação consistia na redução das quantidades de autoridades de escrutínio e de servidores na rede de mistura.

A segunda implementação ganhou interface Web. Foi usado código Java e JavaScript, além de bibliotecas proprietárias da Microsoft. O sistema foi flexibilizado com a parametrização de vários itens, inclusive a do próprio protocolo a ser utilizado. Essas implementações fazem parte de um projeto denominado Ostracon, sobre votações seguras, desenvolvido naquela universidade.

3.8.2 Versões Comerciais

Existem poucos sistemas comerciais voltados a eleições seguras. Normalmente, detalhes técnicos são omitidos.

Dentre os sistemas existentes, pode-se citar o VoteHere e SafeVote. VoteHere afirma garantir a exatidão de uma eleição segura. São usados códigos de verificação, autoridades confiáveis e redes de embaralhamento. Maiores detalhes podem ser obtidos em www.votehere.com.

SafeVote, por sua vez, possui uma linha de produtos para diferentes magnitudes de eleições. Desde uma simples cabina eleitoral à uma eleição via internet, passando por redes locais. SafeVote não fornece maiores detalhes sobre seus sistemas. Mais informações podem ser obtidas em www.safevote.com

3.8.3 A Urna Eletrônica

A urna eleitoral brasileira consta de um terminal de eleitor e um microterminal para operação dos mesários. Ela é equipada com o sistema operacional VirtuOS, da empresa Microbase. O sistema recebeu várias extensões em relação ao produto de prateleira da empresa, a fim de aumentar sua segurança e garantir os requisitos, segundo relatório da Unicamp (BRUNAZZO FILHO, 2003).

Embora o TSE venha apresentando o código fonte do sistema aplicativo que controla a eleição, inclusive em sessões com compilação, há uma série de dúvidas a respeito da confiabilidade da urna como um todo, já que o sistema operacional é proprietário e de código fonte fechado.

Fraudes no processo de votação podem estar ocorrendo, como a vinculação entre o eleitor e seu voto, ou ainda a alteração de resultados. Há também acusações sobre fraudes como eleitores mortos que votam. Entretanto, esse tipo de problema decorre de falhas no processo de alistamento eleitoral, e não possui muita relação com a confiabilidade geral da urna.

4 PROTOCOLO GERYON

Um protocolo é um conjunto de regras, que devem ser seguidas em uma determinada seqüência, a fim de se obter determinado resultado. Um protocolo criptográfico é um protocolo que usa codificação (cifragem) e decodificação (decifragem) de informações em alguns ou em todos os seus passos. Os participantes de um protocolo podem ser amigos e confiar mutuamente, ou podem ser adversários e desconfiar (e tentar trapacear) mutuamente.

De qualquer maneira, a realização de um protocolo requer que todos os participantes envolvidos no protocolo conheçam-no, assim como todos os seus passos, para seguir em avanço. Cada parte envolvida no protocolo também deve aceitar segui-lo. O protocolo também não pode ser ambíguo, cada etapa deve ser bem definida, sem possibilidades de confusão.

A definição de um protocolo mais robusto (LICHTLER, 2000) para eleições é apresentada aqui. Esse protocolo trabalha com três centrais eleitorais, derivando daí o nome Geryon. A comunicação de dados entre as mesmas deve ser restrita ao especificado.

A Central de Cadastramento (CC) é a responsável, basicamente, por verificar e validar a população de eleitores, assim como emitir a cédula eleitoral. A Central de Votação (CV) é a responsável por receber os votos dos eleitores, emitir os certificados (comprovantes de votação) aos eleitores e enviar a informação a um terceiro elemento, a Central de Apuração (CA). Essa contabiliza os votos, dando fim ao processo.

O detalhamento desse protocolo é apresentado nas seções seguintes, assim como a análise de possíveis fraudes.

4.1 Contexto

Os requisitos básicos de uma eleição segura, já apresentados e explicados no capítulo anterior, são:

1) Somente eleitores autorizados podem votar.
2) Nenhum eleitor pode votar mais de uma vez.
3) O voto é secreto.
4) Nenhum voto pode ser duplicado.
5) Nenhum voto pode ser alterado.
6) Cada eleitor pode verificar se o seu voto foi computado.
7) Cada eleitor deve receber um comprovante de ter participado (votado) na eleição.

Os protocolos apresentados até aqui falhavam, ou por sua demasiada simplicidade e o conseqüente descumprimento de alguns dos requisitos, ou pela extrema complexidade, que os tornavam impraticáveis para um número grande de eleitores ou de candidatos, como é o caso do modelo de eleições atualmente em vigor no Brasil. O

presente protocolo busca resolver essa questão, satisfazendo requisitos não cumpridos pelos protocolos de duas centrais, mas sem a complexidade encontrada nos de três.

.

4.2 Definições

Sejam três as centrais eleitorais da Justiça, com as respectivas competências, avaliadas e fiscalizadas pela própria Justiça e comissões representativas das partes interessadas:

1) Central de Cadastramento (CC). Esta central tem por obrigação especificar, reconhecer e cadastrar a população de eleitores. Assim, com base em critérios especificados pela legislação eleitoral, esta central recolhe dados comuns dos eleitores, como nome, domicílio, número da carteira de identidade, além de dados «eletrônicos», formados basicamente pelo endereço de correio eletrônico do cidadão e a chave pública do mesmo, sendo esta de recolhimento imprescindível. Por ocasião de uma eleição, essa central é responsável, também, pelo fornecimento da cédula ao eleitor.
2) Central de Votação (CV). Esta central opera somente nas ocasiões em que há eleição, e sua principal atribuição é receber o voto do eleitor, validá-lo, e emitir um comprovante de votação para o eleitor. Os votos validados são repassados à terceira central.
3) Central de Apuração (CA). Tem por objetivo recolher os votos validados pela Central de Votação e computá-los. Essa central deve, também, publicar uma lista de votos, através da qual os eleitores podem conferir a contabilização de seu próprio sufrágio.

4.3 Funcionamento

O funcionamento deste protocolo é razoavelmente simples. Ele é fundamentado na comunicação restrita entre as Centrais, o que deve ser garantido através de fiscalização e meios legais.

A primeira fase do processo é o cadastramento dos eleitores. Cada eleitor deve se dirigir pessoalmente a uma unidade da Central de Cadastramento (CC). Nessa etapa, o reconhecimento do eleitor é feito de forma convencional, através dos documentos tradicionais de identificação, assinatura e apresentação pessoal. Do ponto de vista de garantias contra fraudes, esse processo é tão vulnerável quanto o que atualmente ocorre, já que é feito da mesma forma.

O detalhe adicional nessa etapa é que o eleitor deve, obrigatoriamente, entregar uma assinatura digital, que será o instrumento fundamental de todas as etapas posteriores. Opcionalmente, outros dados para comunicação eletrônica podem ser requisitados ao eleitor, de forma a facilitar e agilizar a mesma. As chaves públicas devem ser armazenadas e validadas pela CC, de forma a não haver duplicidades ou inconsistências dentro de uma mesma seção eleitoral. A CC deve fornecer ao eleitor a chave pública da Central de Votação, para uma posterior comunicação segura entre ambos.

Quando da ocorrência de eleições, acontece a próxima etapa, que é a de votação. Ela é iniciada quando o eleitor solicita a CC uma cédula. Esse pedido, já pode ser feito remotamente, através de correio eletrônico, por exemplo, bastando para isso que o eleitor assine o pedido.

A CC então envia a cédula ao eleitor. A cédula consta de um texto ASCII ou um formulário HTML, por exemplo, ou qualquer outro arquivo digital que permita ao

eleitor fazer a sua escolha. Além disso, a CC gera um número secreto, aleatório, que também é passado ao eleitor. Esse número é chamado Número de Validação (VAL), e é parte integrante da cédula. Por outro lado, uma lista de todos os números de validação deve ser remetida à Central de Apuração (CA).

A CC também envia, à Central de Votação (CV), uma lista contendo dados sobre os eleitores, como nome, identidade, *e-mail*, e chave pública.

A CA deve disponibilizar aos eleitores a sua chave pública. É interessante que essa disponibilização seja feita através da CV, evitando-se, assim, qualquer contato direto entre o eleitor e a CA. Então, de posse da chave pública da CA, e da cédula fornecida pela CC, o eleitor faz seu voto. Cada um gera um número aleatório, grande o suficiente para evitar duplicidades em uma seção eleitoral. Este número é chamado Número de Verificação (VER).

O voto consiste na cédula fornecida pela CC, alterada ou marcada conforme a legislação especificar. O eleitor cifra o voto (que contém também VAL) e a sua própria seqüência VER com a chave pública da CA. Este pacote é assinado pelo eleitor, e remetido à CV.

A CV, por sua vez, é responsável por receber os votos emitidos pelos eleitores. A cada voto recebido, a CV emite um comprovante de votação assinado ao respectivo eleitor. O comprovante consiste do próprio voto e de um anexo que identifique a eleição.

Nesse momento, a CV já possui o cadastro de todos os eleitores, com suas respectivas chaves públicas, o que permite retirar as assinaturas dos pacotes recebidos e enviá-los, então, à CA, que é a responsável pela última etapa do processo.

Esses pacotes, oriundos da CV, podem ser assinados pela mesma e cifrados à CA, a fim de garantir ainda mais a segurança no canal de comunicação entre as centrais. Recebendo esses pacotes, a CA verifica a assinatura da CV e a retira. O que ela obtém é um pacote, cifrado para sua própria verificação - já que o eleitor usou a própria chave pública da CA para cifrar os votos - que contém uma cédula marcada (o voto), uma seqüência VAL e uma seqüência VER.

Nessa etapa, a CA pode computar os votos. Ela contabiliza apenas os votos que estiverem de acordo com a legislação específica, e que tenham seqüências VAL constantes da lista recebida da CC. Para aumentar a segurança do sistema, todas as informações trocadas entre as centrais são cifradas à central de destino e assinadas pela de origem.

O passo final do processo é a publicação de uma listagem que contém os votos com as respectivas seqüências VER, o que permite ao eleitor verificar se o seu voto foi computado.

A figura 4.1 ilustra alguns dos passos mais importantes deste protocolo, com uma seqüência de passos ordenados por setas, considerando-se que o processo de cadastramento da população de eleitores já tenha sido realizado pela CC.

Para a compreensão do esquema representado na figura 1, deve-se observar a seguinte notação:

- O eleitor hipotético chama-se X. Seus dados pessoais relevantes ao processo são denotados por #X, sua chave privada é KD_X, sua chave pública é KE_X, seu número de validação é VAL_X e seu número de verificação é VER_X.
- $E(M, KE_X)$ significa cifrar (E) a mensagem M com a chave pública (KE) de X.
- $A(M, KD_X)$ significa assinar (A) a mensagem M com a chave privada (KD) de X.
- As centrais de Cadastramento, de Votação e de Apuração são indicadas, respectivamente, por CC, CV e CA.

Os passos ilustrados na figura 1 são:

1) A CC envia Cédula e VAL cifrados ao eleitor X: E[(Cédula, VAL_X), KE_X).
2) A CC envia dados de X, inclusive sua chave pública, devidamente assinados e cifrados à CV: A{E[(#X, KE_X),KE_{CV}],KD_{CC}}.
3) A CC envia VAL assinado e cifrado à CA: A[E(VAL_X,KE_{CA}),KD_{CC}). Este passo pode, também, ser feito ao final da prazo de votação, quando todas as seqüências VAL são enviadas juntas.
4) A CV envia a chave pública de CA, assinada e cifrada a X: E[E(KE_{CA},KE_X),KD_{CV}].
5) O eleitor X envia seu voto, seu VAL e sua seqüência gerada VER, assinados e cifrados à CA, para a CV: A{E[($Voto_X$, VAL_X, VER_X), KE_{CA}],KD_X}.
6) A CV verifica e retira a assinatura de X, e envia a ele um comprovante, que é seu próprio voto (e seqüências), ainda cifrado à CA, conjuntamente a um identificador da eleição, devidamente assinado: A($Comprovante_X$, KD_{CV}).
7) O pacote contendo voto, VAL e VER, recebido do eleitor X, e ainda cifrado à CA, é remetido a esta pela CV, devidamente assinado: A{E[($Voto_X$, VAL_X, VER_X), KE_{CA}],KD_{CV}}. Este passo pode ser feito a cada voto, ou ao final do período de votação, quando todos os pacotes são enviados juntos.
8) A CA computa os votos e publica listagens de votos com os respectivos números de verificação.

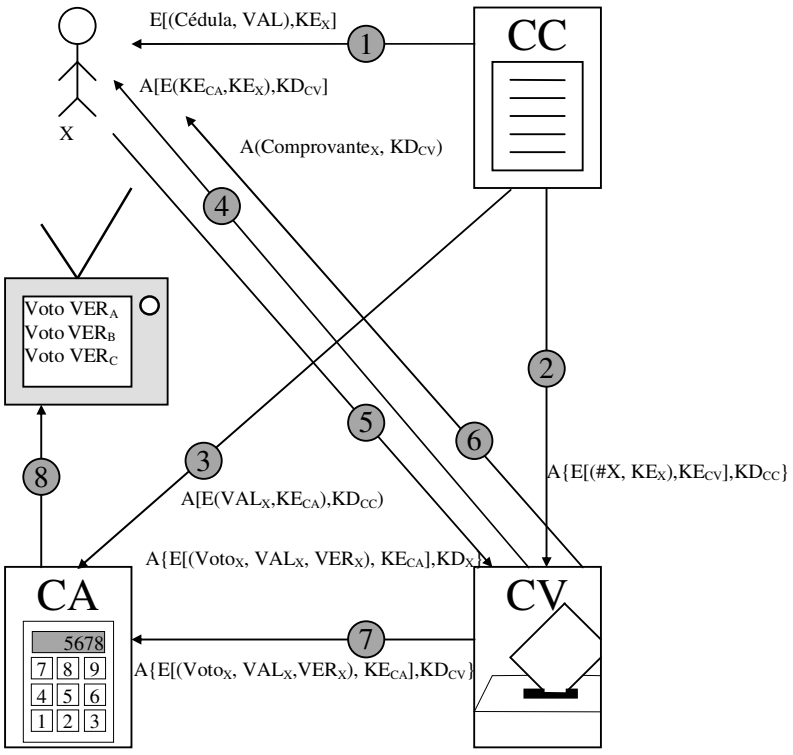


Figura 4.1: Principais etapas do protocolo

Dos passos listados anteriormente, são inferidas três fases de funcionamento do protocolo. A execução de uma fase depende do completo término da anterior. As fases são: cadastramento, votação e apuração.

A fase de cadastramento pode ser considerada uma preparação para o protocolo. Nela, os eleitores comparecem à CC e depositam ali suas chaves públicas. A fase de cadastro termina quando a CC envia para a CV a lista dos eleitores.

Começa então a fase de votação. Nessa fase os eleitores cadastrados fazem requisição de voto à CC, que lhes envia a cédula. Eles a preenchem, obtendo seus votos, que são enviados à CV. Essa, por sua vez, lhes emite o certificado de participação.

Terminada essa fase, a CC envia a listagem dos números válidos de cédulas para a CA, que também recebe a lista dos votos recebidos da CV. A CA pode, finalmente, proceder a apuração dos votos, que é objetivo dessa terceira fase.

Do ponto de vista do eleitor, o protocolo é de fácil funcionamento. Sua tarefa é receber a cédula da CC, marcá-la adequadamente e cifrá-la a CA. Depois disso, deve assiná-la e remetê-la a CV. Assim, a CV envia o comprovante de votação quando o voto for recebido e o eleitor pode conferir o seu voto quando da publicação pela CA.

4.4 Análise

A seguir são feitas algumas análises quanto a possibilidades de fraude e suas conseqüências no funcionamento do protocolo, a fim de evidenciar quais são seus requisitos essenciais. Os possíveis ataques, falhas e fraudes estão agrupados pelos atores do sistema.

Quando os eleitores votam, eles devem gerar números próprios, preferencialmente números aleatórios bem grandes, para posterior conferência do voto, publicado pela CA. Números idênticos dentro de uma mesma seção podem causar confusão e a sensação de engodo ao eleitor. Dessa forma, sugere-se que o algoritmo para geração da seqüência VER seja fornecido pela própria Justiça Eleitoral.

4.4.1 Do Eleitor

Os possíveis problemas causados pelo eleitor podem ser:

1) Um eleitor tentar votar por outro.
2) Um eleitor tentar votar mais de uma vez.
3) Um não eleitor tentar votar.
4) Um eleitor questionar a computação do seu voto.
5) Um eleitor ser forçado a mostrar seu voto.

As garantias oferecidas pelo protocolo são mostradas a seguir.

1. Se um eleitor mal intencionado, tentar votar por outro eleitor, não conseguirá, pois o voto enviado à CV deve ser assinado pelo eleitor. Além disso, o número de validação de cada eleitor lhe é cifrado. Essa dupla garantia satisfaz o primeiro item. Mesmo assim, se o falsário, por acaso, conseguir roubar a chave privada do eleitor antes do mesmo votar e então, votar em seu lugar, não há o que fazer, pois o requisito fundamental da chave privada pessoal e intransferível foi violada.

2. Se um eleitor tentar votar mais de uma vez, o sistema não aceitará, pois a CV tem a obrigação de validar apenas um voto por eleitor, e ela tem como fazer isso, já que dispõe de cadastro dos eleitores enviado pela CC, no qual consta, inclusive, a chave pública de cada eleitor cadastrado.

3. Se um não eleitor tentar votar, a probabilidade de sucesso da fraude é irrisória, pois ele não possui uma assinatura digital que conste na CV, nem de um número de validação fornecido pela CC. Assim, mesmo que conseguisse forjar uma assinatura e ser aceito pela CV, teria que ter seu voto computado pela CA, o que também é improvável.

Tabela 4.1: Garantias contra fraudes de eleitores

Um...	não pode...	porque...
eleitor	• votar por outro • votar várias vezes • questionar a computação do voto • ser obrigado a mostrar seu voto	• o voto é assinado pelo próprio. • apenas um voto é aceito. • é possível, via auditoria, verificar o voto, quebrando o sigilo. • está cifrado para a Central de Apuração..
não eleitor	• tentar votar	• não possui assinatura nem seqüência de validação.

4. Quando um eleitor questionar a computação do seu voto, seja ela como incorreta ou inexistente, ele está deliberadamente declinando do sigilo em torno do mesmo. Nesse caso, o seu voto assinado está armazenado na CV, que pode repassá-lo diretamente à CA para análise do caso. Além disso, a CC pode remeter à CA o número de validação correspondente ao eleitor, o que também serve para a verificação de fraude.

5. O comprovante de votação de um eleitor pode ser exigido por qualquer parte interessada, já que ele apenas é um atestado, assinado pela CV. No atestado está, de fato, o voto do eleitor, mas está devidamente cifrado para a CA. Assim, não existe a possibilidade de «voto de cabresto». Adicionalmente, com a publicação dos votos com as respectivas seqüências VER também não há risco de conferência por terceiros, já que a seqüência VER é pessoal e como foi dito, sugere-se que o algoritmo seja fornecido pela autoridade eleitoral competente, e que gere números suficientemente grandes, distintos e de baixa repetição. Caso o eleitor seja pressionado a mostrar a seqüência VER, ele pode arbitrar qualquer uma que conste na listagem publicada pela CA e que sirva aos interesses do solicitante, embora essa situação seja caso de polícia.

4.4.1 Das Centrais Eleitorais

Há basicamente, duas questões envolvendo as centrais eleitorais.

1) Uma central pode tentar falsificar ou inventar votos.
2) Uma central pode tentar inspecionar os votos.

A seguir, estão as garantias do protocolo a esses pontos.

1. A CC não tem meios de falsificar votos. Ela pode gerar eleitores falsos, mas esse tipo de fraude transcende às garantias de ciência da computação e da criptografia. Esse mesmo tipo de fraude pode ocorrer em votações tradicionais ou com a urna eletrônica, e não há solução simples para tal.

A CV não pode falsificar votos, uma vez que ela não possui a lista de seqüências VAL geradas pela CC, e este é um princípio fundamental. A CV não pode, em hipótese alguma, ter conhecimento das sementes empregadas pela CC para gerar os números de validação, ou outro detalhe qualquer que facilite a geração indevida de seqüências VAL. Assim, a seqüência VAL recebida da CC pelo eleitor deve ser tão bem guardada quanto a sua própria chave privada. Por outro lado, a divulgação desse número pelo eleitor poderia permitir à CA a inspeção do seu voto.

Pelo mesmo motivo, a CC não enviar uma listagem que contenha ligações entre VAL e alguma propriedade que identifique o eleitor, pois nesse caso a CA poderia também inspecionar o voto.

A CA não pode fraudar os votos, pois ela deve em primeiro lugar, receber somente aqueles que tenham sido assinados pela CV. Em segundo lugar, ela deve considerar apenas os votos que tenham números de validação constantes da lista emitida

pela CC. Nesse caso, portanto, a falsificação é garantidamente mais difícil. A tabela seguinte mostra como as Centrais estão impossibilitadas de fraudar (inventar ou alterar) votos.

Tabela 4.2: Garantias contra fraudes das centrais

A Central de ...	não pode fraudar voto porque ...
Cadastramento	• o voto deve estar assinado pelo eleitor.
Votação	• o voto está cifrado à CA e possui uma seqüência VAL desconhecida.
Apuração	• o voto deve estar assinado pela CV.

2. A CV deve sempre retirar as assinaturas dos votos recebidos e passá-los, então, à CA. É recomendado que a CA não tenha acesso a nenhum dado dos eleitores, nem às suas chaves públicas, o que aumenta a segurança do sistema caso algum voto recebido pela CV seja repassado à CA ainda assinado pelo eleitor.

A CA deve publicar somente os votos com os respectivos números de verificação. Jamais poderia publicar as seqüências VAL em conjunto, o que permitiria a membros da CC inspecionar os votos.

Dessa maneira, é garantido o segredo do voto, o eleitor pode conferir se seu voto foi computado e ainda recebe um comprovante de que votou. A tabela seguinte resume as garantias que o eleitor tem de que seu voto não seja violado (inspecionado).

Tabela 4.3: Garantias de voto secreto

A Central de ...	não pode inspecionar o voto porque ...
Cadastramento	• a listagem final publicada pela CA contém apenas o voto e o VER, não tendo mais o VAL;
Votação	• o voto está cifrado para a CA;
Apuração	• o voto não está mais assinado;
	• não possui o conhecimento das relações entre as seqüências VAL e os eleitores.

4.5 Auditoria

O sistema permite que seja feita gravação dos canais de comunicação entre as centrais, ou seja, os passos 2, 3 e 7 representados na figura 4.3.1.

Como as mensagens são adequadamente cifradas a cada central, não existe risco de obtenção indevida de informações sigilosas. Contudo, em caso de dúvidas sobre a lisura do processo, as informações de um canal podem ser decifradas mediante a quebra de segredo da chave privada da referida central.

A quebra de segredo da chave privada de uma central possibilita que seja verificado se as mensagens recebidas estão de acordo com o que especifica o protocolo, mas não permite nenhuma conclusão que fira as restrições da eleição.

Assim, partidos políticos interessados em verificar possíveis fraudes podem solicitar, a uma instância competente da justiça, a quebra de segredo de uma determinada central.

As três centrais podem ter, ainda, seus segredos abertos simultaneamente, desde que não haja cruzamento das informações armazenadas em cada uma delas. Caso isso ocorra, o anonimato (ou sigilo) do voto é perdido.

4.6 Considerações Finais

A grande questão é garantir um sistema operado por seres humanos em que não haja o vazamento ilícito dessas informações. O ideal é que o processo fosse o mais automatizado o possível, principalmente nas fases de retirar as assinaturas dos votos, enviar listas e votos entre as centrais e publicar os resultados para conferência.

Dessa maneira, enquanto todos os algoritmos sejam de domínio público, inclusive para fiscalização partidária, os números secretos de validação, de verificação, bem como as chaves privadas e as sementes utilizadas para a geração de números aleatórios devem ficar em sigilo absoluto. É evidente que no caso de uma auditoria, deve-se quebrar o segredo da chave privada de determinada central. Isso, contudo, não prejudica futuras utilizações do sistema, pois, nesse caso, é suficiente gerar novos pares de chaves.

5 PROTÓTIPO

No presente capítulo são abordados aspectos tecnológicos e de modelagem que devem ser considerados na implementação de um sistema de votação baseado no protocolo Geryon. Além disso, é apresentado o protótipo elaborado, juntamente com descrição da sua estrutura funcional.

5.1 Princípios Funcionais

O sistema de votação é divido em quatro módulos:

- módulo de cadastramento (MC);
- módulo de votação (MV);
- módulo de apuração (MA);
- módulo do eleitor (ME).

Para cada um desses módulos, são apresentados os requisitos e as funcionalidades a serem implementadas.

5.1.1 Módulo de Cadastramento

O módulo de cadastramento é a parte de software correspondente à CC. Durante a sua instalação, ele deve gerar o par de chaves da central. Além disso, deve recolher o número IP do servidor onde está sendo instalado.

Em execução, ele deve permitir as seguintes tarefas, bem como gerir os dados a elas inerentes:

1. Cadastrar eleitores.
2. Gerar, se necessário, pares de chaves aos eleitores. Exportar as chaves geradas.
3. Gerar o modelo de cédula a ser usado na votação.
4. Gravar, em arquivo de configuração, a sua chave pública, o seu número IP, o número IP da CV e outras informações necessárias ao módulo do eleitor (ME).
5. Gerar os números VAL e enviá-los aos MEs, quando requisitado.
   5.1. Gerar o número.
   5.2. Assinar o número.
   5.3. Cifrar o número para o respectivo eleitor.
   5.4. Enviar ao ME correspondente.
6. Enviar listagem de eleitores para CV:
   6.1. Gerar listagem de eleitores e respectivas chaves.
   6.2. Assinar listagem.
   6.3. Cifrar listagem para CV.
   6.4. Enviar listagem ao MV.
7. Enviar listagem VAL para CA.
   7.1. Gerar listagem de números VAL.

7.2. Assinar listagem.
7.3. Cifrar listagem para CA.
7.4. Enviar listagem ao MA.

8. Enviar cédulas para eleitores:
   8.1. Gerar cédula.
   8.2. Assina cédula.
   8.3. Cifra cédula ao eleitor.
   8.4. Envia cédula ao respectivo ME.

5.1.2 Módulo de Votação

O módulo de votação é a parte de software correspondente à CV. Em fase de instalação, deve gerar o par de chaves da respectiva central. Deve enviar seus dados (chave pública e número IP, por exemplo) para a CC.

Durante a execução normal, o módulo deve permitir as seguintes tarefas, assim como gerir os dados relativos a elas:

1. Receber a lista de eleitores oriunda da CC:
   1.1. Decifrar a mensagem.
   1.2. Verificar a assinatura da CC.
2. Receber os votos provenientes de cada eleitor.
3. Verificar a assinatura dos votos e enviar, para cada voto assinado e inédito de eleitor, um comprovante de votação:
   3.1. Decifrar a mensagem.
   3.2. Verificar a assinatura do eleitor.
   3.3. Verificar se o eleitor ainda não votou.
      3.3.1. Caso positivo:
         3.3.1.1. Formar comprovante (declaração mais o voto).
         3.3.1.2. Assinar o comprovante.
         3.3.1.3. Cifrar o comprovante ao eleitor.
         3.3.1.4. Enviar comprovante ao ME.
      3.3.2. Caso negativo:
         3.3.2.1. Gerar aviso de erro.
         3.3.2.2. Assinar aviso.
         3.3.2.3. Cifrar o aviso ao eleitor.
         3.3.2.4. Enviar aviso ao ME.
4. Enviar para a CA a lista dos votos aceitos:
   4.1. Gerar lista dos votos aceitos.
   4.2. Assinar a lista.
   4.3. Cifrar a lista à CA.
   4.4. Enviar a lista ao MA.

5.1.3 Módulo de Apuração

O módulo de apuração é a parte do sistema que cabe à CA. Durante sua instalação, ele deve gerar o par de chaves da sua central e repassar essa e outras informações importantes às demais centrais.

Em sua fase de operação normal, o módulo deve possibilitar as tarefas seguintes, além de administrar os dados a elas intrínsecos:

1. Receber a listagem de números VAL emitida pela CC:
   1.1. Decifrar a mensagem.
   1.2. Verificar a assinatura da listagem.

2. Receber a listagem de votos aceitos recebida da CV:
    2.1. Decifrar a mensagem.
    2.2. Verificar a assinatura da listagem.
    2.3. Decifrar os votos.
3. Para cada voto com seqüência VAL correta, fazer a contabilização.
4. .Gerar uma listagem contendo votos e números de verificação.

5.1.4 Módulo do Eleitor

O módulo do eleitor é um programa de instalação que ele deve receber, por correio eletrônico, ou por carga de arquivo, ou por cópia em meio flexível. Esse programa deve ser instalado na máquina do usuário e, durante esse processo, deve ser possível:

1. Obter de um arquivo de configuração, informações necessárias para a comunicação com as centrais, como os seus números IPs, suas chaves e outras.
2. Obter o par de chaves do usuário, assim como determinar o número de usuários que vão utilizar o sistema.

Estando em funcionamento, o módulo deve garantir a operação das seguintes atividades, da mesma forma que deve viabilizar o armazenamento dos dados a elas relacionados, para cada usuário:

1. Gerir senhas e pares de chaves.
2. Solicitar autorização para voto (número VAL).
3. Gerar número VER.
4. Solicitar cédula à CC.
5. Exibir cédula e permitir o voto.
6. Enviar o voto à CV:
    6.1. Gerar o voto.
    6.2. Anexar número VER.
    6.3. Anexar número VAL.
    6.4. Cifrar o voto à CA.
    6.5. Assinar o voto.
    6.6. Cifrar o voto à CV.
    6.7. Enviar o voto ao MV.

5.2 Possibilidades Tecnológicas

Em um primeiro momento, deve ser considerado que um sistema de votação baseado no protocolo Geryon é constituído basicamente de quatro módulos, com quatro interfaces e funcionalidades diferentes. A cada uma das três centrais eleitorais deve corresponder um módulo de software; à interação com o usuário deve corresponder um quarto módulo.

Nos parágrafos seguintes, são feitas considerações sobre possíveis formas de implementação de um sistema desse tipo. Qualquer que seja a implementação adotada, as três centrais eleitorais devem ser construídas em módulos de software independentes. De preferência, em servidores autônomos. Isso significa que a grande questão do modelo de implementação está na interface com o usuário.

5.2.1 Modelo com código carregável

Um tipo de solução pode ser obtido através do uso de navegadores (*browsers*). Nesse caso, o eleitor não precisaria de um módulo de software específico em seu computador, mas usaria algum tipo de serviço interpretado pelo navegador de internet do seu computador.

De um lado há tecnologias disponíveis como ASP, PHP e Perl, que têm em comum o fato de serem executadas no lado do servidor. Isto é, elas são embutidas no código HTML e são executadas pelo interpretador ou preprocessador existente no servidor. Esse tipo de linguagem não permite a manipulação de arquivos no lado do cliente, fazendo com que o tratamento de funções de cifragem e de decifragem fique a cargo do servidor. Isso implica que o servidor receberia as informações em claro, o que não é uma boa solução. Além disso, para a segurança do tráfego na rede, seria necessária a conexão através de um meio seguro usando, por exemplo, HTTPS.

De outro lado tem-se as linguagens interpretadas no lado do cliente, como Java Script e VB Script. Essas linguagens têm a facilidade de poderem manipular objetos no computador cliente, o que é uma facilidade para, por exemplo, gerenciar as chaves do eleitor. Entretanto, elas não têm suporte intrínseco à criptografia, fazendo com que a solução definitiva recaia na carga de páginas imensas de código que implemente cifragem e assinatura digital, ou novamente no envio das informações em claro para tratamento criptográfico no servidor, o que não é uma boa alternativa.

Uma terceira alternativa seria o uso de applets Java ou componentes ActiveX. Essas tecnologias envolvem a execução em máquinas virtuais e possuem bom suporte a criptografia. Entretanto, existem restrições quanto à compatibilidade entre várias plataformas e navegadores. Além disso, possuem algumas restrições de segurança que tornam o seu uso inviável. Um applet Java, por exemplo, não pode manipular arquivos nem se comunicar com mais de um servidor. Para várias circunstâncias de utilização, essas características podem tornar um sistema mais seguro, mas no caso específico desse sistema de votação, tornam-se limitadores decisivos.

5.2.2 Modelo com código instalado

Em um ambiente cliente-servidor, que use comunicação direta via internet, o eleitor recebe um programa para instalar e executar em seu próprio computador. Esse tipo de programa pode ser concebido como um executável auto-extrativo, de tal forma que o processo inteiro seja fácil ao usuário.

Nesse tipo de sistema, todas as funções criptográficas necessárias são compiladas junto do programa cliente, o que possibilita que as funções de cifragem e de assinatura digital sejam processadas no computador do eleitor, isentando o servidor de realizá-las. Além disso, a comunicação pode ser feita sem o uso de um protocolo de comunicação seguro, uma vez que o próprio computador cliente já é capaz de reconhecer e autenticar as mensagens.

Esse tipo de solução exige a elaboração de um protocolo de comunicação específico, assim como a prévia identificação dos servidores e das portas a serem usadas.

5.3 Arquitetura Utilizada

Para a implementação do protótipo de sistema de votação segura baseado no protocolo Geryon, foi escolhido o modelo de sistema com código instalado. Dessa forma, o computador do eleitor ganha um aplicativo, independente de linguagens

interpretadas ou de navegadores, que faz tanto a parte de processamento quanto a comunicação com os servidores.

A implementação em si foi desenvolvida usando-se certas plataformas específicas, assim como certos ambientes de desenvolvimento; essa escolha não deve ser interpretada como a solução ideal ou recomendada. É apenas uma das possibilidades encontradas e que pode ser recompilada para outras situações.

O sistema operacional para o qual (e no qual) os módulos foram compilados é o Microsoft Windows. Novamente vale a pena ressaltar que não se trata de nenhuma preferência ou recomendação.

A ferramenta de desenvolvimento utilizada foi o compilador Borland Delphi 6. Nesse caso a escolha recaiu não apenas pelo fato de existir uma certa experiência na programação nesse ambiente, como também porque essa suíte permite fácil integração com o sistema operacional Linux, através da suíte chamada Kylix.

Embora seja uma ferramenta bastante robusta, o Delphi na sua sexta versão ainda não incorporava facilidades para trabalhos envolvendo criptografia. Dessa forma, foi necessária a utilização de bibliotecas criptográficas adicionais.

Entre as várias bibliotecas disponíveis, optou-se pelo uso da PGP - SDK (*Pretty Good Privacy – Software Development Kit*) (PGP, 1999). O PGP é o sistema de cifragem mais amplamente usado no mundo (GARFINKEL, 1995) e talvez por isso, um dos mais confiáveis.

O pacote PGP – SDK contém uma série de bibliotecas de funções e tipos de dados em linguagem C. Essas funções são, em geral, de nível um tanto baixo, requerendo a manipulação exaustiva de ponteiros e estruturas complexas.

Como um facilitador, foi agregada ao desenvolvimento do protótipo, a utilização de componentes Delphi adicionados com funções criptográficas. Esses componentes, referenciados dentro do pacote PGP2Comp, são na verdade uma série de unidades Pascal que fazem a inclusão das inúmeras funções do PGP - SDK em funções de mais alto nível. Essas funções são dependentes de instalação do PGP, mesmo porque fazem uso do seu anel de chaves.

Essas funções são agrupadas nos componentes Delphi listados a seguir:

- Preferences: Configuração de preferências do usuário, como algoritmo padrão de cifragem simétrica, par de chaves padrão, etc.
- KeyServer: Funções para comunicação com servidores de chaves públicas.
- GetKeyProperties: Funções que retornam informações sobre determinadas chaves, como detalhes técnicos ou identidades.
- SetKeyProperties: Funções que configuram certas propriedades nas chaves, como senha de acesso, habilitação, etc.
- KeysGenerate: Métodos para geração de chaves, números primos, etc.
- KeyImport: Funções para importação de uma chave externa ao anel de chaves do PGP.
- KeyExport: Funções para exportação, em arquivo, de chaves existentes no anel.
- Encode: Funções para cifrar e assinar mensagens.
- Decode: Funções para decifrar e verificar assinaturas de mensagens.

A necessidade de se ter o PGP instalado para o funcionamento desses componentes pode parecer inconveniente. Entretanto, vale ressaltar que o PGP é um software com licença aberta para fins não comerciais. Além disso, é disponível para várias plataformas diferentes, como Macintosh, Linux e Windows. Além disso, é inegavelmente difundido.

Por esses motivos, não há desvantagens em exigir-se a instalação prévia do PGP. Vale ressaltar também, que se está apresentado um protótipo de funcionamento real de um protocolo de votação, e não um produto comercial.

Quanto aos componentes Delphi utilizados, fora os visuais, foram utilizados os componentes PGP descritos acima e também alguns para comunicação de rede. Usados para essa finalidade foram basicamente 4:

- ClientSocket: Funções para comunicação de um cliente através de sockets com um servidor.
- ServerSocket: Funções para configuração de um servidor para responder às mensagens dos clientes.
- IdIpWatch: Funções para recuperação sobre informações IP do computador local.
- IdSMTP: Funções para o envio de correio-e usando SMTP.
- IdMessage: Classes para a configuração de mensagem eletrônica.

5.4 Protótipo

A seguir é apresentado o protótipo como foi elaborado. Para um melhor entendimento, antes são feitas considerações sobre as fases do protocolo e o comportamento dos módulos durante cada uma.

5.4.1 Estados do Sistema

Os estados do sistema de votação são derivados das fases do próprio protocolo. Eles são em número de quatro e descritos a seguir.

1. **Cadastro**: Nesse estado, o Módulo de Cadastro aceita o alistamento de eleitores, e faz a geração e exportação ou a importação das chaves dos eleitores. Os outros módulos não conseguem trocar mensagens significativas, apenas requisições de verificação do estado atual e requisições de listagens, essas negadas.

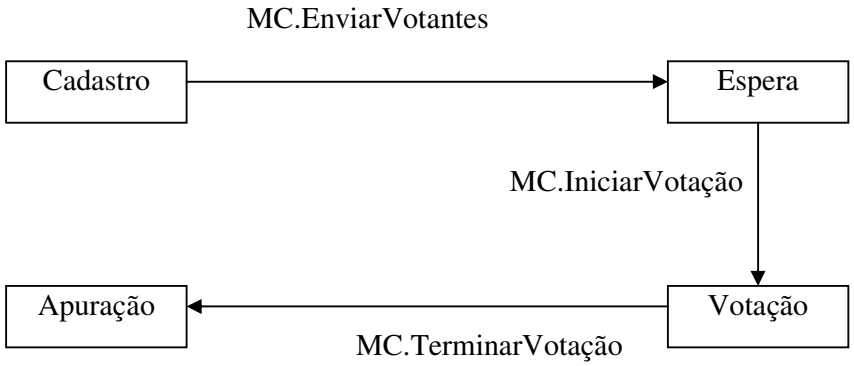


Figura 5.1: Diagrama de Transição de Estados

2. **Espera**: A espera não é uma fase do protocolo, mas é intervalo de tempo entre o fim da fase de Cadastro e o início da votação propriamente dita. Essa fase tem início com o envio da lista dos eleitores cadastrados da Central de Cadastro para a Central de Votação, que pode, por sua iniciativa, requisitar o reenvio da mesma.

3. **Votação**: Durante a votação, o Módulo de Cadastro espera requisições por parte dos módulos dos eleitores e lhes responde enviando cédulas com número de validação. Cada eleitor, por sua vez, utiliza seu módulo para receber a cédula, configurar o voto e o enviá-lo para a Central de Votação.
4. **Apuração.** Esta última fase tem início com o fim da votação. De início, o módulo da central de cadastro envia lista com os números de validação gerados para a Central de Apuração, que também recebe o conjunto de votos vindos da Central de Votação. Essas centrais têm ainda a possibilidade de solicitar e enviar essas mensagem de modo forçado, além do automático. Recebidas as duas listagens, a Central de Votação pode proceder a contagem dos votos.

A figura 5.1 ilustra o diagrama de transição de estados do sistema. A seguir, são apresentadas as interfaces do protótipo desenvolvido.

5.4.2 Interfaces

O Módulo da Central de Cadastro possui três guias. A primeira é para o cadastro de eleitores propriamente dito, e possui campos para a inserção do nome e do endereço de correio eletrônico do eleitor, que são as informações inerentes a uma chave pública PGP. Ela oferece além da geração de chave, a opção de importação de uma chave preexistente. A figura 5.2 ilustra essa guia.

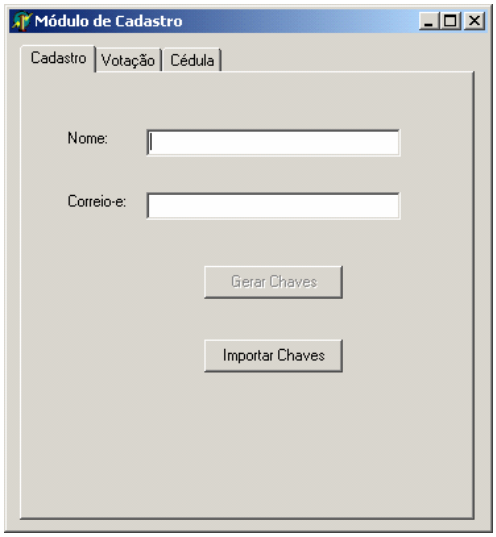


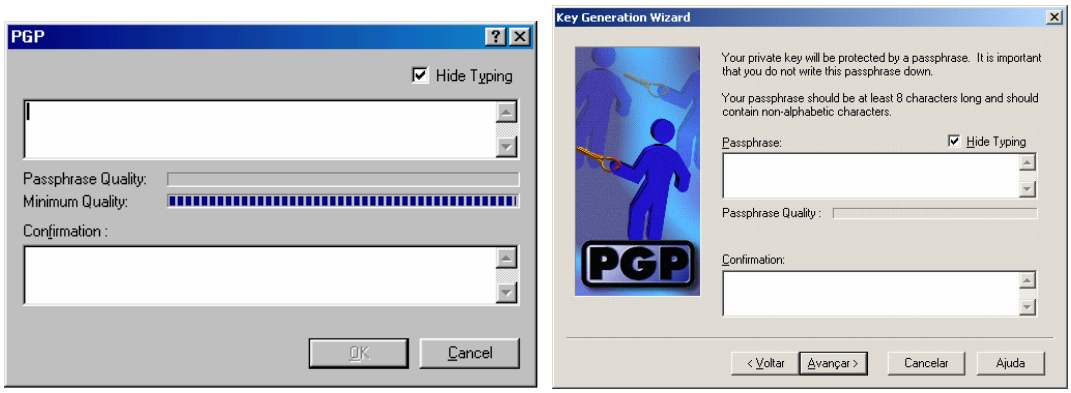
Figura 5.2: Cadastro de eleitor e chaves

Algumas das interfaces do sistema são providas pelo próprio PGP. Por exemplo, na geração de uma chave, excluindo-se a fase de inicialização de contexto do PGP, a criação propriamente dita é feita através da chamada de três métodos, conforme a figura 5.3. No caso das interfaces acionadas pelo próprio PGP, as mensagens são em inglês, o que torna fácil a tarefa de identificá-las.

```
PGPKeysGenerate1.UserName:= EdNome.Text;
PGPKeysGenerate1.EmailAddress:= EdCorreio_e.Text;
PGPKeysGenerate1.RSAKeyGenerate(false);
```

Figura 5.3: Código para geração de chaves

As duas primeiras linhas são configurações de parâmetro para a chave a ser gerada. A terceira linha é realmente a criação da chave. Mas esse método é também responsável pela exibição automática da caixa de diálogo apresentada na figura 5.4(a), para a entrada da frase de passagem (senha de acesso). Essa caixa é muito semelhante àquela utilizada pelo próprio PGP no *wizard* para a geração de chaves, ilustrada na figura 5.4(b).



(a) (b)

Figura 5.4: Interfaces providas pelo PGP.

Já na guia Votação, o objetivo é controlar as fases do processo. Por isso, as opções são básicas: botões que determinam o que deve ser feito. Cada um dos botões especifica o início de um novo estado, conforme pode ser observado na figura 5.1. Deve ser observado que o botão [Iniciar Votação] somente é habilitado se houver uma cédula configurada. A guia completa é apresentada na figura 5.5.

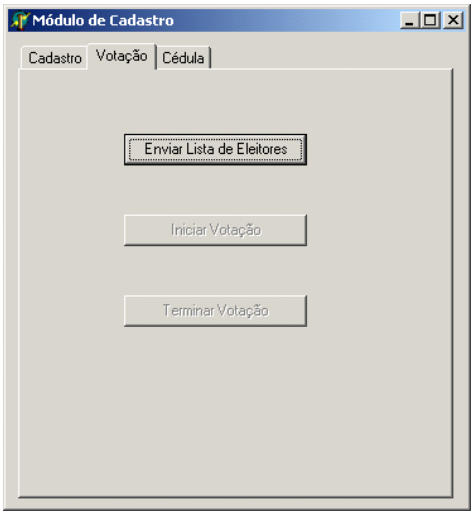


Figura 5.5: Controle da Votação

A guia Cédula contém os campos básicos para formatar uma cédula. Neles, podem ser especificados o título geral da eleição, uma informação adicional, o tipo da eleição e os itens de opção. O tipo da eleição determina se o eleitor poderá escolher apenas um dos itens de opção ou se poderá escolher vários. A diferença é configurada no módulo do eleitor, que utiliza botões de rádio (RadioButton) para o primeiro caso, ou caixas de checagem (CheckBox), para o segundo. A figura 5.6 apresenta essa interface.

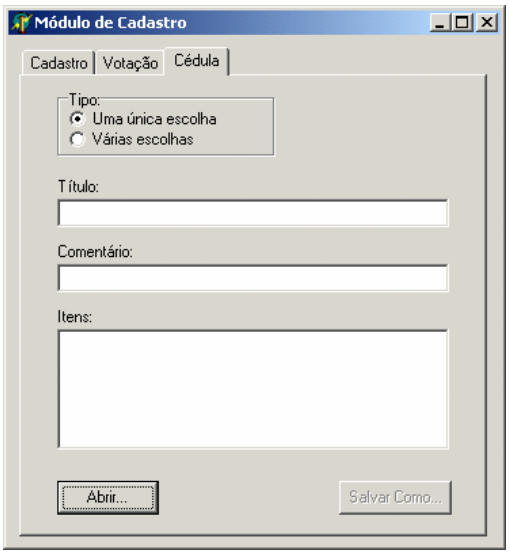


Figura 5.6: Composição da cédula

O módulo de votação possui tarefas muito automatizadas, sendo que grande parte delas são respostas do servidor aos pacotes *socket* recebidos. Esse módulo tem sua função principal na fase de votação, mas já antes disso se comunica com o módulo de cadastro para a obtenção da lista das chaves públicas dos eleitores. Na verdade, essa lista é enviada pela Central de Cadastramento; mesmo assim, há a possibilidade de fazer a requisição. Na fase de votação, recebe os pacotes enviados pelos eleitores e, como resposta, envia uma mensagem eletrônica usando os componentes IdSMTP e IdMessage. Dessa forma, não há muito o que a interface possa oferecer e sua configuração está ilustrada na figura 5.7.

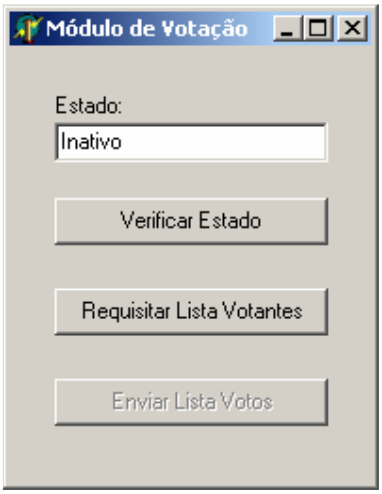


Figura 5.7: Módulo de votação

O módulo de apuração também possui uma interface simples, pelo mesmo motivo que o módulo da Central de Votação: a maioria das tarefas é automática. Dessa forma, o elemento mais significativo é o botão para efetivação da contagem de votos, denominado [Gerar Totalizações]. A representação dessa interface está mostrada na figura 5.8. Os dados são contabilizados de acordo com o tipo de eleição especificado e armazenados em arquivo texto, assinado pela própria central. Outro arquivo gerado é uma lista de votos, onde os votos são publicados em seqüência aos números de verificação gerados pelos eleitores. Esse também é um arquivo texto.

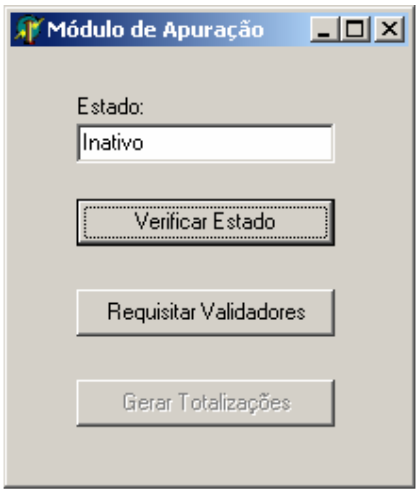


Figura 5.8: Módulo de apuração

O módulo do eleitor já apresenta algumas características a mais, pois necessita de maior interação. Há duas guias, uma de eleição, e outra de configurações. A guia de configurações possui caixas de texto para a entrada dos números IP dos servidores, e também das portas de comunicação. Possui também um botão para adicionar as chaves das centrais ao anel de chaves do PGP da máquina local.

A guia eleição permite ao eleitor fazer a carga da cédula, através do botão correspondente. Se a eleição não estiver na fase de votação, a solicitação é sem efeito. Caso contrário, uma cédula é carregada e é aberto um novo formulário, com os dados oriundos da central de cadastramento. A figura 5.9 ilustra a aparência inicial do módulo.

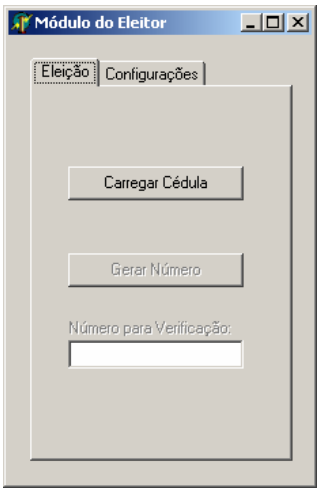


Figura 5.9: Módulo do eleitor

Tendo sucesso na carga, um novo formulário é criado, usando como parâmetros de disposição os dados recebidos da central de votação. Esses parâmetros influem em dois aspectos do formulário a ser montado: a quantidade de itens entre os quais o eleitor vai poder escolher (e, por conseqüência, no tamanho do formulário) e o tipo de escolha a ser feito, entre caixas de conferência e botões de rádio.

Para atender a esse requisito de flexibilidade do desenho do formulário, foi utilizada a criação dinâmica de componentes. Essa técnica consiste basicamente em se declarar uma variável de classe do objeto desejado e, a partir dela, serem alocados dinamicamente novos objetos, com o uso de métodos construtores como o `Create`.

Essa solução foi importante e adequada, pois permite flexibilidade da cédula e mantêm o controle das informações e das funções criptográficas do protocolo subordinado ao próprio aplicativo. Assim também é obtido um controle maior sobre as ações do usuário eleitor, sob vários aspectos. Do ponto de vista do preenchimento do voto, ele fica limitado às opções que lhe são fornecidas. Do ponto de vista de segurança, ele fica protegido pelo próprio sistema.

Na figura 5.10 está apresentada uma cédula montada no módulo da Central de Cadastramento.

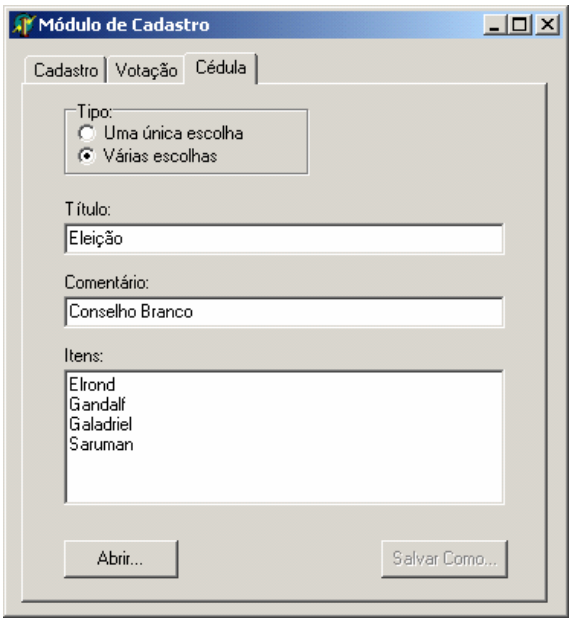


Figura 5.10: Cédula configurada

O conteúdo dos campos é formatado como um texto simples, de linhas seqüentes. Na primeira, vai o valor *Rad* ou *Che* conforme a escolha marcada no painel Tipo. O efeito dessa configuração é o formulário de cédula apresentado ao eleitor pelo seu módulo, como apresentado na figura 5.12.

Outra conseqüência importante da carga da cédula é a habilitação do botão que gera o número de verificação. Esse número é enviado em conjunto com o voto e pode ser usado pelo eleitor para conferir a contagem adequada do seu voto nas listas publicadas após o escrutínio. O número consiste na concatenação de uma série de cinco centenas aleatórias geradas pelo sistema. Essa mesma implementação foi usada para o número de validação. Nada impede que, de acordo com a necessidade, esse tamanho seja alterado, tanto no código fonte, quanto como um parâmetro a ser determinado em tempo de execução, incluído então na interface de algum dos módulos servidores.

O botão que permite a emissão do voto, rotulado [Votar], somente é habilitado após a criação do número de verificação. Mas isso pode ser definido de outra maneira, se for considerado que a emissão de tal número não é obrigatória, deixando assim de cumprir a verificabilidade.

Pelo protótipo, o módulo de Apuração faz a "publicação" dos resultados em arquivos texto. Esses arquivos podem ser usados posteriormente para publicação na internet, através de uma interface HTML ou equivalente.

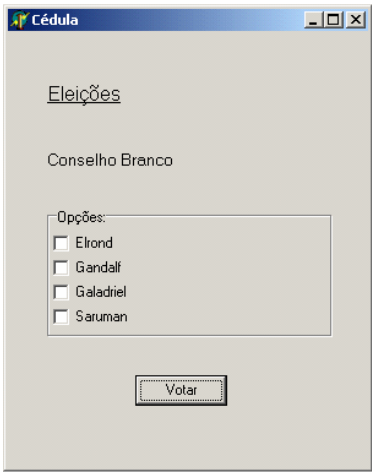


Figura 5.11: Cédula carregada

Como visto, o protótipo apresenta interfaces simples. Uma maior complexidade seria necessária na medida em que certos itens forem parametrizados, como por exemplo, o já citado tamanho dos números aleatórios; ou uma cédula com opções compostas de escolha; ou ainda contadores indicativos do processamento sendo executado.

6 CONCLUSÃO

Cada vez mais a representação de uma vontade através do voto se faz presente no mundo atual. Ela pode ser percebida nos governos de países republicanos e democráticos, no qual cidadãos votam para eleger seus representantes. Pode ser percebida em nível mais alto ainda, porém talvez menos justo, quando no Conselho de Segurança das Nações Unidas algumas poucas nações decidem sobre o futuro de outrem. Faz-se presente em escopo menor e restrito, como nas escolas, onde alunos e professores escolhem os diretores.

A participação do voto está presente mesmo em situações de pouca relevância. Pessoas são indagadas sobre sua opinião pessoal sobre assuntos como um jogo de futebol ou algum programa de televisão; e os resultados daí provenientes são apresentados como determinassem alguma coisa. Entretanto, pesquisas de opinião podem ter também seu valor: podem ser usadas para determinar a estratégia de mercado de alguma empresa ou produto; podem até ter efeito sobre políticas públicas.

Em todas as situações descritas acima, da mais ampla à mais restrita, da mais importante à mais supérflua, está presente o mesmo princípio, o mesmo mecanismo: a expressão de uma opinião através do voto. Votações podem ser eleições, plebiscitos, referendos, censos, pesquisas de opinião. Pouco importa: em todos esses casos a mesma necessidade de confiança nos resultados se faz presente. Afinal, se não fosse para um resultado ser confiável, então nem precisaria haver o processo.

A grande demanda do mundo atual é justamente essa. Como proceder para que votações produzam resultados confiáveis. A utilização de meios completamente manuais, onde o ser humano está presente em todas as macroetapas do processo ainda é muito utilizada, exatamente na mesma medida em que é vulnerável a fraudes. Afinal, se pessoas participam da elaboração, da execução e da apuração da votação, então há pontos fracos e corruptíveis em toda sua extensão.

A automatização parece ser uma tendência. Se em poucas situações uma automatização completa pode ser viável, busca-se pelo menos, a sua aplicação no momento mais crítico, que é quando os votos estão sendo gerados, depositados e, posteriormente, contados. Isso reduziria sensivelmente os pontos frágeis do processo.

Entretanto, não existe solução mágica em termos de tecnologia. Assim como no método tradicional, em que se confia nas pessoas que exercem autoridade sobre o processo de votação, no método informatizado é necessário se ter alguma confiança na tecnologia empregada.

Destarte, servidores confiáveis são necessários para a elaboração de uma rede que produza resultados precisos e mantenha a privacidade dos eleitores. Não há sistema determinístico que produza resultados completamente aleatórios. Pode haver um sistema determinístico que embaralhe dados sem possibilidade de rastreamento?

Em qualquer circunstância, alguma confiança é necessária em alguma autoridade. Todavia, se essa autoridade puder ser inspecionada ou auditada, as

expectativas de confiança aumentam significativamente. Mas isso somente é possível se houver transparência. No caso de um sistema de votação automatizado, a metodologia, a tecnologia e, enfim, o protocolo usados deve ser de domínio público.

Dos protocolos apresentados neste trabalho, é fácil verificar que a complexidade é diretamente proporcional à quantidade de requisitos atendidos. E dos sistemas comerciais apresentados, faltam informações detalhadas.

O objetivo que permeou a realização do presente trabalho foi fornecer uma ferramenta adicional na área de votações seguras. Ela possui algumas características importantes.

Quanto ao protocolo utilizado, percebe-se que ele atende aos requisitos propostos de uma eleição segura, mas de uma forma mais simples que os demais. Mais do que isso, a computação exigida também é inferior aos demais casos estudados. Assim sendo, pode ser considerado um protocolo simples, porém robusto, pois é fundamentado nas técnicas atuais e seguras que a criptografia oferece.

Adicionalmente, o protocolo permite a elaboração de um sistema de software relativamente simples. Não são empregados algoritmos complexos, ou ainda funções criptográficas não triviais, como a assinatura cega. Ao contrário, ele pôde ser transformado em protótipo com o uso de ferramentas de programação comuns e com o uso do sistema de chaves públicas mais largamente difundido.

Esse protótipo pode ser utilizado como fonte para a confecção de sistemas mais elaborados, que permitam maior nível de personalização. Entre os aprimoramentos que podem ser feitos, encontra-se a configuração de uma cédula mais complexa, com mais opções, talvez descrita em uma linguagem de marcação. A possibilidade do uso de um banco de dados, para permitir o relacionamento de vários eleitores com várias eleições também é uma questão a ser pensada. Assim, informações mais completas sobre as eleições e sobre os eleitores poderiam ser guardadas.

Enfim, idéias boas e soluções plausíveis existem. Entretanto, há ainda questões importantes a serem resolvidas nas fases de cadastramento e de autenticação, por exemplo.

No cadastramento, a forma fundamental usada é ainda o registro pessoal, de corpo presente. Mas na autenticação, como é possível garantir que o eleitor é realmente quem diz ser? Os métodos disponíveis levam em consideração algo que a pessoa saiba como uma senha, e/ou algo que a pessoa tenha, como um cartão, ou ainda algo que a pessoa seja, a chamada biometria. As fragilidades dos dois primeiros consistem em que uma senha pode ser repassada a outrem, e um cartão pode ser roubado. Deve ser levado em consideração, porém, que a perfeição está longe de ser obtida, pois nem a autenticação biométrica é totalmente confiável.

REFERÊNCIAS

AMERICAN BAR ASSOCIATION (ABA). **Digital Signature Guidelines Tutorial.** Disponível em: <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>. Acesso em: fev. 2004.

BRASIL. Tribunal Superior Eleitoral (TSE). **Código Eleitoral Anotado.** Disponível em: <http://www1.tse.gov.br/servicos_online/legislacao/codigo_eleitoral_anotado/>. Acesso em: mar. 2004.

BRUNAZO FILHO, A. Avaliação da Segurança da Urna Eletrônica Brasileira**.** In: SIMPÓSIO DE SEGURANÇA DE INFORMÁTICA, SSI, 2000. **Anais**... São José dos Campos: Instituto Tecnológico da Aeronáutica, 2000.

BRUNAZO FILHO, A. et al. **Burla Eletrônica**. Rio de Janeiro: Fundação Alberto Pasqualini, 2003.

CANTÙ, Marco. **Dominando o Delphi 3.** São Paulo: Makron Books, 1997.

CRANOR, L. F.; CYTRON, R. K. Sensus: A Security-Conscious Polling System for the Internet**.** In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, HICSS, 1997. **Proceedings**... Wailea: University of Hawaii, 1997.

CUSTÓDIO, R. F.; PEREIRA, F. C. Ostracon: Um Sistema de Votação Digital Segura pela Internet**.** In: WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS, WSEG, 2., 2002, Búzios. **Anais**... Rio de Janeiro: NCE/UFRJ, 2002.

DEVEGILI, A. J. **Farnel:** Uma Proposta de Protocolo Criptográfico para Votação Digital**.** 2001. Dissertação (Mestrado). Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina (UFSC). Florianópolis: UFSC, 2001.

GARFINKEL, S. **PGP**: Pretty Good Privacy**.** Sebastopol: O´Reilly & Associates, 1995.

HOUAISS, A.; VILLAR, M. de S. **Dicionário Houaiss da Língua Portuguesa.** Rio de Janeiro: Objetiva, 2001.

IBM. **Introduction to Cryptology.** Disponível em: <http://www.ibm.com/deveoperworks/s-crypto-a4.pdf>. Acesso em: dez. 2002.

LICHTLER, R. L.; WEBER, R. F. Proposta de Protocolo Criptográfico para Votações Digitais**.** In: WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS, WSEG, 2., 2002, Búzios. **Anais**... [Rio de Janeiro: NCE/UFRJ], 2002.

MERTZ, D. **Introduction to Cryptology.** Disponível em: <http://gnosis.cx/publish/programming/cryptology1.pdf>. Acesso em: mar. 2004.

PGP Software Developer's Kit – Reference Guide. Version 1.7 Int. Disponível em: <ftp://ftp.pgpi.org/pub/pgp/sdk/PGPsdkReferenceGuide.pdf>. Acesso em: mar. 2004.

RIERA, A. **An Introduction to Electronic Voting Schemes.** Barcelona: Prepublicacions i Informes de Recerca del Departament d'Informàtica (PIRDI) de la Universitat Autônoma de Barcelona (UAB), 1998.

RIERA, A. Practical Approach to Anonymity in Large Scale Electronic Voting Schemes**.** In: SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEMS, NDSS, 1999. **Proceedings**… San Diego CA: Internet Society (ISOC), 1999.

SCHNEIER, B. **Secrets and Lies:** Digital Security in a Networked World**.** New York: John Wiley & Sons, 2000.

SCHNEIER, B. **Applied Cryptography**, 2nd ed**.** New York: John Wiley & Sons, 1996.

SIMMONS, G. J. **Contemporary Cryptology:** The Science of Information Integrity**.** New York: IEEE Press, 1992.

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

TANENBAUM, A. S. **Redes de Computadores.** 5. ed. Rio de Janeiro: Campus, 1997.