Protocolo Criptográfico para Votações Digitais

Ricardo Luís Lichtler, Raul Fernando Weber
Instituto de Informática, UFRGS
Av. Bento Gonçalves, 9500 - Bloco IV
91501-970 Porto Alegre, RS
[lichtler|weber]@inf.ufrgs.br

Resumo: *O presente trabalho apresenta uma proposta de protocolo criptográfico aplicado como ferramenta na implementação de eleições seguras. O protocolo é baseado em criptografia assimétrica que possibilite cifragem e assinatura eletrônicas de mensagens. Com o uso deste protocolo é possível realizar eleições através de uma rede de computadores garantindo integridade dos votos durante todo o processo e assegurando ao mesmo tempo o anonimato do eleitor.*

Palavras-chave: *eleições; protocolos; criptografia; segurança.*

Abstract: *This paper presents a cryptographic protocol proposal, to be used as a tool in the implementation of secure elections. This protocol is based on asymmetric cryptography, which offers electronic enciphering and signature of messages. Using this protocol it is possible to conduct an election process using a computer network and ensure the integrity of the whole process while maintaining the voter's anonymity.*

Keywords: *elections; protocols; cryptography; security.*

1. Introdução

O uso de sistemas informatizados em ambientes de votações ou de eleições é uma necessidade para acelerar o processo como um todo, principalmente a fase de escrutínio. A garantia de confiança no sistema computacional empregado é baseada, sobretudo, em sua transparência, ou seja, os algoritmos e protocolos devem ser preferencialmente conhecidos pelas partes interessadas.

Essa transparência necessária, entretanto, nem sempre é oferecida. O sistema atual de urnas eletrônicas utilizadas nas eleições brasileiras é um exemplo [BRU00]. Não havendo total transparência em torno do sistema computacional, é normal que surjam dúvidas e polêmicas quanto à sua confiabilidade. Fraudes eleitorais acontecem em vários lugares do mundo [SCH00]. As dúvidas mais comuns e óbvias em relação ao uso das urnas eletrônicas são se as urnas de fato computam o voto de cada eleitor de maneira adequada e se elas não permitem identificação posterior do voto do eleitor.

O presente artigo discute uma maneira transparente de uso de sistemas computacionais através da utilização de um protocolo criptográfico. São descritos, anteriormente, os princípios gerais de uma eleição, que devem ser contemplados por eleições feitas através de sistemas computacionais.

2. Princípios gerais sobre eleições

O termo *eleições* que aqui se aplica não se refere somente ao tipo usual de eleições. Por *eleição* deve ser entendida qualquer votação, plebiscito, etc. 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 seja de alguma forma computado.

Uma eleição segura apresenta vários pontos fundamentais [SCH96]. Alguns deles são:

R1. Somente pessoas autorizadas podem votar.
R2. Ninguém pode votar mais de uma vez.
R3. O voto é secreto.
R4. Ninguém pode replicar o voto de ninguém.
R5. Ninguém pode alterar o voto de ninguém.
R6. Cada eleitor deve poder verificar se o seu voto foi computado.

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.

O sistema de eleições no Brasil é regido pela Legislação Eleitoral [TRI02]. 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 importante 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.

3. Proposta de um protocolo

A definição de um protocolo criptográfico robusto [SIM92] para eleições é apresentada aqui. Esse protocolo trabalha com três centrais eleitorais, descritas a seguir.

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.

3.1. Contexto

O protocolo aqui apresentado é proposto para garantir os seis requisitos básicos de uma eleição (R1 a R6), assim como um sétimo, extraído do modelo brasileiro:

R7. Cada eleitor que votou deve receber um comprovante de que tenha votado.

Alguns protocolos apresentados na literatura [SCH96] falham, ou por sua demasiada simplicidade e o conseqüente descumprimento de alguns dos requisitos, ou pela extrema complexidade, que os tornam impraticáveis para um número grande de eleitores ou de candidatos.

3.2. 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.

3.3. 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 pode ser 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, posto que é realizado 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 dispor aos eleitores a sua chave pública. É interessante que essa distribuição 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 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: $E[(\text{Cédula}, VAL_X), KE_X)$.
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.

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.

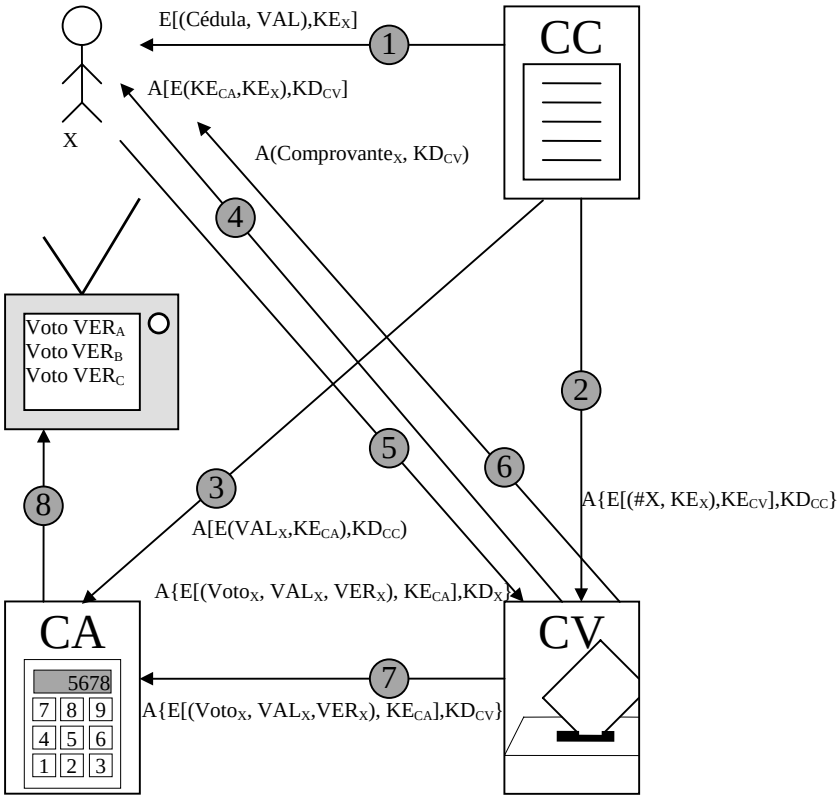

Figura 1. Esquema de Funcionamento do Protocolo Criptográfico

3.4. 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.

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 descritas a seguir.

1. Se um eleitor mal intencionado tentar votar por qualquer outro eleitor, não conseguirá, pois o voto enviado à CV deve ser assinado pelo eleitor. Além disso, o número de validação de um eleitor é cifrado para ele próprio. Essa dupla garantia satisfaz o primeiro item. Mesmo assim, se por acaso o falsário conseguir roubar a chave privada de eleitor de fato 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.

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 do 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 ele ainda 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 alguém 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 uma violação dos direitos e das garantias individuais do cidadão.

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 pode 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 1 mostra como as Centrais estão impossibilitadas de fraudar (inventar ou alterar) votos.

Tabela 1 - Garantias contra fraudes

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 2 resume as garantias que o eleitor tem de que seu voto não seja violado (inspecionado).

Tabela 2 - 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.

3.5. 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 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. Conclusão

O presente trabalho não pretende fornecer a solução derradeira em protocolos criptográficos para votações digitais, mas sim mostrar um sistema eficiente e robusto que pode ser aplicado, com garantia de funcionamento. O método é tão (ou mais) seguro quanto os tradicionalmente empregados, e é simples quando comparado com outros protocolos sugeridos na literatura [SCH96].

Aplicando-se métodos criptográficos seguros, o protocolo fornece todos os requisitos que uma eleição computacionalmente segura deve obedecer, sendo bem adequado ao modelo brasileiro de eleição, no qual foi inspirado.

Não é intenção deste trabalho sugerir a substituição da votação convencional - agora com a urna eletrônica. Na verdade, a votação através de protocolos criptográficos, como por exemplo o descrito neste artigo, poderia ser uma facilidade adicional ao cenário de eleições. O uso desse sistema é claramente adequado à Internet. Assim, pessoas que estejam impossibilitadas de comparecer a uma seção eleitoral, ou ainda, que estejam longe da mesma, poderiam proceder o voto sem maiores transtornos ou justificativas.

5. Referências Bibliográficas

[BRU00] BRUNAZO Filho, Amilcar. Avaliação da Segurança da Urna Eletrônica. Disponível por HTTP (janeiro de 2002) em www.brunazo.eng.br/voto-e/arquivos/SSI2000.zip.

[SCH00] SCHNEIER, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, 2000.

[SCH96] SCHNEIER, Bruce. Applied Cryptography. 2nd. ed. New York: John Wiley & Sons, 1996.

[SIM92] SIMMONS, Gustavus J. Contemporary Cryptology: The Science of Information Integrity. New York: IEEE Press, 1992.

[TRI02] TRIBUNAL Superior Eleitoral. Legislação Eleitoral. Disponível por HTTP (janeiro de 2002) em www.tse.gov.br/servicos/legislacao/index.html.