Esquema de Votação Seguro e Transparente através de Encriptação Homormófica

Pedro Vinícius Macêdo de Araújo
Antônio de Abreu Batista Júnior
Mario A. Gazziro

Universidade Federal do Maranhão

2 de Setembro de 2019

Conteúdo

Conteúdo

A democracia Representativa

somente funciona se todos os cidadãos elegíveis podem participar das eleições e estarem confiantes de que:

(A) a sua escolha foi expressa corretamente; e

(B) ela foi inclusa e contabilizada no resultado final.

Ameaças a integridade de eleições

Figura: Eleições para o Senado Federal.

Esquema de votação transparente e seguro

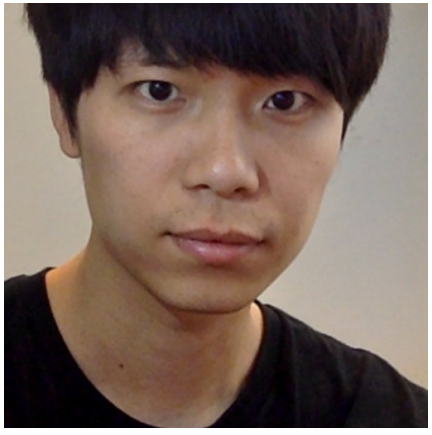
- Somente eleitores válidos podem votar;
- Cada eleitor só pode votar uma vez;
- Sigilo total do voto;
- O eleitor pode, após o voto, verificar se ele é realmente válido;
- O eleitor pode se convencer que seu voto realmente foi apurado;
- Ninguém deve conseguir alterar ou remover os votos na urna ou incluir votos ilegítimos;
- Todos os votos devem permanecer secretos até o fim da votação;
- A contagem dos votos deve ser pública;
- Deve ser possível auditar a contagem.

Trabalhos correlatos

Jeroen Graaf

Título: *Long-Term Threats to Ballot Privacy.* [Graaf, 2017].

Trabalhos correlatos



Xuechao Yang

IEEE Access

Título:*A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption* [Yang et al., 2018].

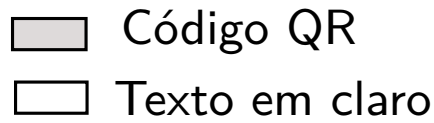
Desenvolveram um esquema de votação pela internet inspirado no chamado voto por aprovação.

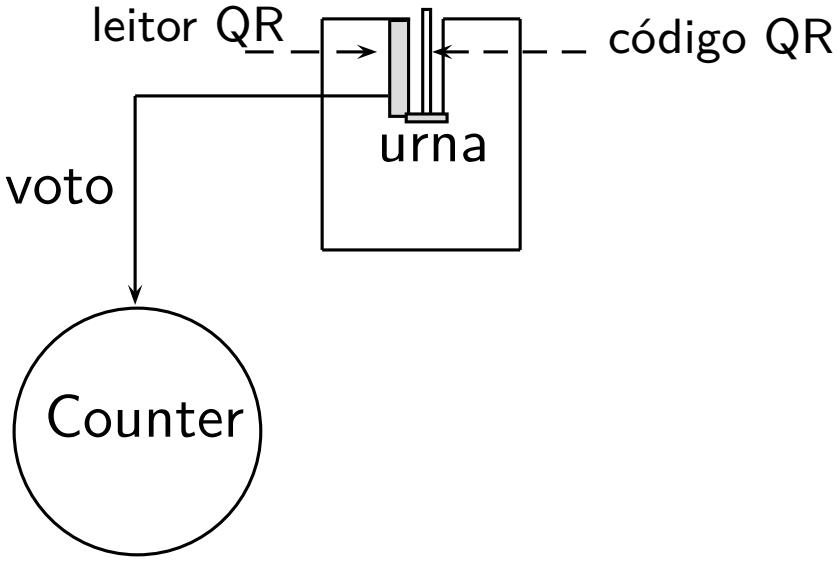
Blocos de construção

Blocos de construção	Função
ElGamal Exponencial	Processar votos sem revelar seus conteúdos
Comprometimento de Bit incondicional	Obter o sigilo do voto
Compartilhamento de segredo	Aumentar a segurança
Prova de conhecimento parcial	Validar votos

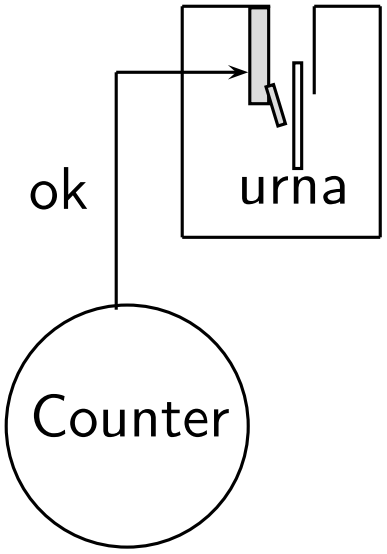
Conteúdo

Funcionamento





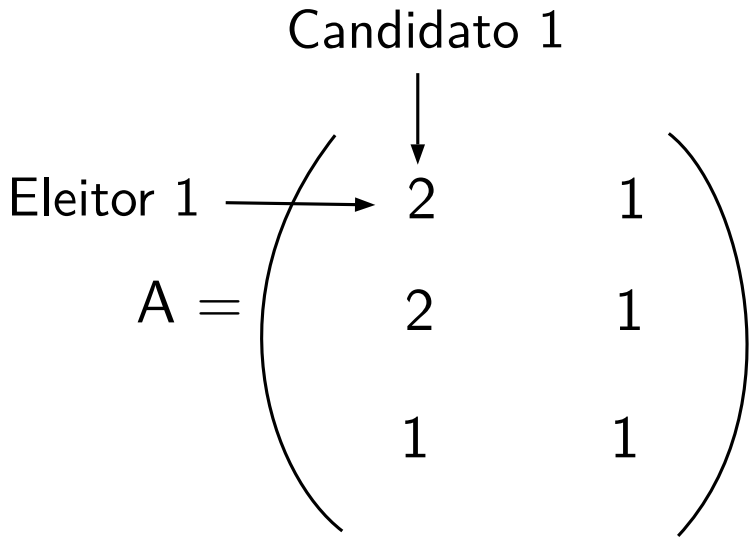
a) Urna envia voto



b) Counter contabiliza voto

Representação do voto

$$A = (a_{ij})_{I \times N} \text{ tal que } a_{ij} = \begin{cases} 2 & \text{se o eleitor } i \text{ votou em } j \\ 1 & \text{caso contrário} \end{cases}$$



O voto de um eleitor i é válido se :

$$\sum_{j=1}^{N} a_{ij} = \begin{cases} N+1 & \text{se o eleitor } i \text{ votou em algum candidato } j \\ N & \text{se o eleitor } i \text{ votou branco ou nulo} \end{cases}$$

Elgamal exponencial

	A	B
eleitor 1	1	1
eleitor 2	2	1

Chave	
privada	pública
a	g^a

$$C_1 = (g^{k_1}, \cancel{M} g^{a k_1}) \quad g^1$$

$$C_2 = (g^{k_2}, \cancel{M} g^{a k_2}) \quad g^2$$

g^{total}

$$C_1 \times C_2 = (g^{k_1+k_2}, g^{1+2} \cancel{g^{a(k_1+k_2)}})$$

$$g \in F_p$$

$$0 < a < p-2$$

$$(g^{k_1+k_2})^{-a} = g^{\cancel{-a}(k_1+k_2)}$$

Esquema de comprometimento de bit incondicional

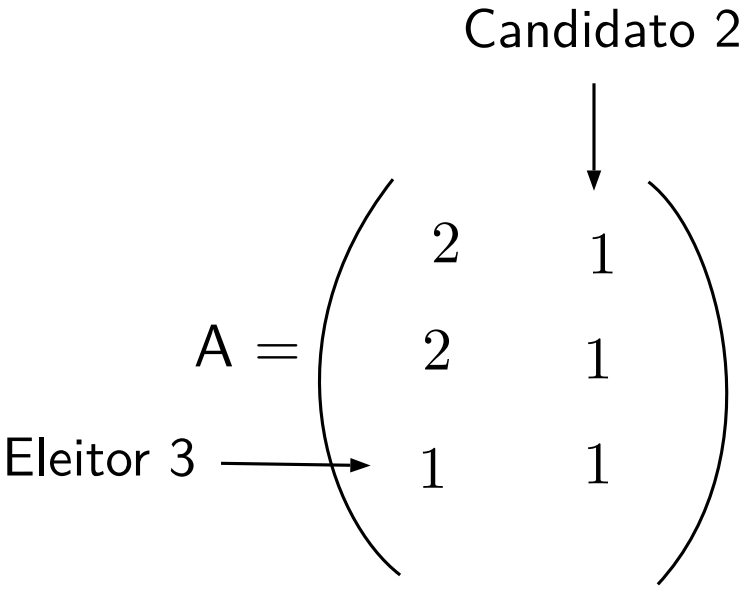
$$u(t, s) = g^{s} \beta^{t} \bmod p$$

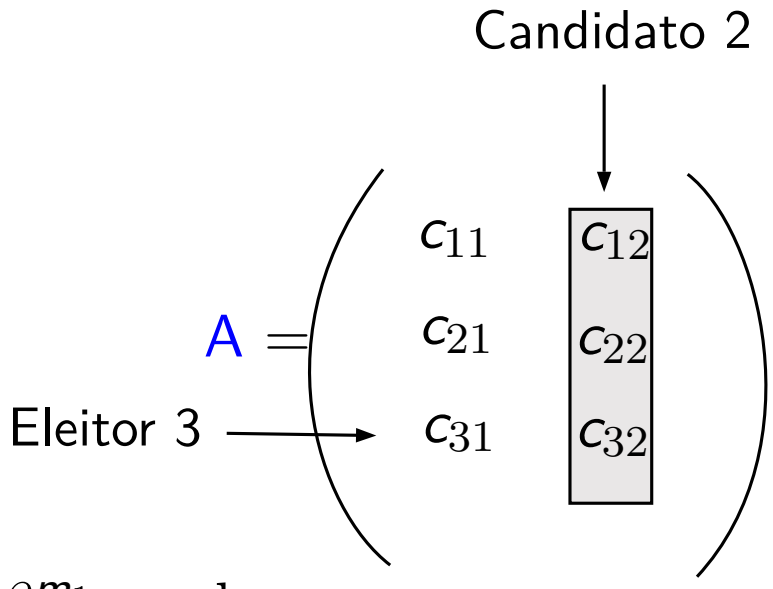
	A	B	C
Voto do eleitor 1	$g^{s_1} \beta^1$	$g^{s_2} \beta^2$	$g^{s_3} \beta^1$

s_1, s_2 e s_3 são números aleatórios.

$$g^{s_1} \beta^1 = g^{s_2} \beta^2$$

Verificação do total de votos de um candidato





$$c_{12} = g^{s_1}\beta^{m_1} \mod p$$

$$c_{22} = g^{s_2}\beta^{m_1} \mod p$$

$$c_{23} = g^{s_3}\beta^{m_1} \mod p$$

$$c_{12} \times c_{22} \times c_{23} = g^{\overbrace{s_1 + s_2 + s_3}^{s}}\beta^{\overbrace{m_1 + m_1 + m_1}^{m}} \mod p$$

Qtd de votos do Candidato 2 = m - Qtd de eleitores

Conteúdo

Experimento 1

O objetivo é validar o desempenho dos algoritmos de:

Geração do voto, Processamento do voto, Obtenção do resultado da eleição e Verificação do total de votos de um candidato.

Critério de avaliação:

Tempo médio de processamento.

Configuração do experimento 1

- Cada algoritmo foi executado 5 vezes
- Os tempos de execução são medidos em segundos
- Calculamos a média e o desvio padrão
- Computador com 2.5 GHz e 8 GB de memória RAM.

Resultados

Tamanho da chave	Algoritmo 1		Algoritmo 3	
	Qtd de candidatos		Qtd de candidatos	
	100	1000	100	1000
512	0.82 (0.02)	7.87 (0.21)	0.75 (0.01)	7.36 (0.35)
1024	4.77 (0.03)	47.44 (0.48)	4.38 (0.18)	43.38 (1.56)

Algoritmo	Descrição
1	Geração do voto
3	Processamento do voto

Resultados

Tamanho da chave	Algoritmo 4		Algoritmo 5	
	Qtd de eleitores		Qtd de eleitores	
	100	1000	100	1000
512	0.09 (0.01)	0.91 (0.03)	0.01 (0.01)	0.68 (0.29)
1024	0.52 (0.01)	5.04 (0.04)	0.33 (0.01)	2.63 (0.03)

Algoritmo	Descrição
4	Obtenção do resultado da eleição.
5	Verificação do total de votos de um candidato.

Conclusão:

Os algoritmos têm tempos de execução razoáveis.

Conteúdo

Considerações Finais

1. Provou-se que o esquema reúne diversas propriedades de um esquema de votação considerado seguro e transparente;
2. Os resultados experimentais indicam a viabilidade de verificação do resultado da eleição por qualquer uma das partes externas;
3. O sistema verifica a integridade de qualquer voto, sem comprometer o seu sigilo.
4. O eleitor pode verificar que o seu voto é considerado na contagem sem comprometer o seu sigilo;

Trabalhos futuros

1. Como garantir a inviolabilidade do software da urna;
2. Analisar a complexidade do processo sob a perspectiva do eleitor;
3. Testes de escalabilidade do esquema e o seu impacto na transparência e na segurança de uma eleição não foram avaliados;

Agradecimentos

Agradeço UFMA que apoiou o desenvolvimento dessa pesquisa.

Referências I


Graaf, J. A. M. V. d. (2017).
Long-term threats to ballot privacy.
IEEE Security Privacy, 15(3):40–47.


Yang, X., Yi, X., Nepal, S., Kelarev, A., and Han, F. (2018).
A secure verifiable ranked choice online voting system based on homomorphic encryption.
IEEE Access, 6:20506–20519.

Esquema de Votação Seguro e Transparente através de Encriptação Homormófica

Pedro Vinícius Macêdo de Araújo
Antônio de Abreu Batista Júnior
Mario A. Gazziro

Universidade Federal do Maranhão

2 de Setembro de 2019