FHElect: Un sistema de votación usando Fully Homomorphic Encryption

Fuentes Tievoli D'Elia

December 7, 2025

Abstract

Los procesos electorales son fundamentales para las democracias y la toma de decisiones en organizaciones privadas. Para garantizar su legitimidad, es esencial asegurar propiedades como el anonimato y la integridad. Este trabajo explora el uso de Fully Homomorphic Encryption (FHE) como solución a los desafíos de los sistemas de votación electrónicos. Se analiza como FHE permite el conteo verificable de votos sobre datos cifrados, preservando la privacidad del votante y asegurando la transparencia.

Contents

1 Introducción y Motivación

A lo largo de los años los sistemas de votación han evolucionado progresivamente en la búsqueda de mayor transparencia y robustez. Sin embargo a medida que los procesos electorales aumentan su escala y requieren condiciones de seguridad cada vez más rígidas, su ejecución se ha tornado costosa e ineficiente en términos de tiempo.

En la actualidad, predominan dos paradigmas:

Por un lado, definimos como voto tradicional al voto que se realiza fisicamente mediante la introducción del mismo en un sobre para colocarlo en una urna.

Por otro lado el concepto de voto electrónico abarca cualquier implementación digital diseñada para gestionar este proceso. A lo largo de este informe, se presentarán distitnas alternativas de voto electrónico.

1.1 Voto Tradicional

El paradigma del voto tradicional es el estándar predominante en las democracias modernas y en muchas votaciones donde el anonimato es fundamental. Esto se debe a la confianza histórica del sistema, y la sencillez con la que el elector se asegura de que su voto es en efecto anonimo.

Sin embargo este sistema trae consigo varias desventajas:

- **Ineficiente temporalmente**: El recuento manual es un proceso lento que retrasa la oficialización de resultados.
- **Costoso**: La logística necesaria para garantizar unas elecciones seguras y transparentes puede generar un costo muy elevado. Esto sucede especialmente en elecciones nacionales. Se estima que el costo de las elecciones nacionales en Argentina en 2025 fue de $ 230.000 millones de pesos[cite: 1].
- **Centralizado**: El sistema es vulnerable a errores humanos y fraudes, ya que el conteo depende de la autoridad electoral.

1.2 Voto Electrónico

La motivación para implementar el voto electrónico nace de la necesidad de crear un sistema más ágil que elimine el recuento manual de votos y el uso masivo de boletas físicas. De esta manera los procesos electorales podrian resultar mucho más económicos gracias al desplome de los costos logísticos y permitiendo a su vez la obtención de resultados de manera instantánea.

Implementar sistemas de esta naturaleza puede implicar algunos inconvenientes:

- **Confianza**: A diferencia del sistema tradicional, en este caso los votantes no tienen la percepcion natural de que su voto va a ser contabilizado. En lugar de depositarlo en una urna deben confiar en que el sistema digital con el que interactuan efectivamente va a realizar las operaciones esperadas
- **Centralización**: Si estos sistemas se implementan de manera centralizada persiste el riesgo de que la autoridad electoral sea corrupta y manipule los resultados
- **Ataques**: Como el sistema de votaciones es software pueden aparecer vulnerabilidades de seguridad informaticas que pongan en riesgo el proceso.

Las implementaciones de voto electrónico *descentralizado* si bien resuelven el problema de la centralización, traen otras complicaciones que se van a discutir luego.

2 Propiedades de un Sistema de Votación

2.1 Privacidad

2.2 Integridad

2.3 Verificabilidad Individual y Universal

2.4 Resistencia a la Coerción

3 Análisis Crítico de los Enfoques Actuales

3.1 Limitaciones del Voto Tradicional

3.2 El Problema del Voto Electrónico Centralizado

3.3 Blockchain "Naive": Transparencia vs. Privacidad

4 Planteamiento del Problema Criptográfico

References

[1] *Going from bad to worse: from internet voting to blockchain voting.* MIT DigitalCurrency Initiative.

[2] Zama AI. *FHEVM Whitepaper.*

[3] La Nación. *El costo de la elección será de por lo menos de 230 mil millones.* 18/10/2025.