FHElect: Un sistema de votación usando Fully Homomorphic Encryption

Fuentes Tievoli D'Elia

December 8, 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

En esta sección se describen algunas propiedades fundamentales que debe cumplir un sistema de votación:

1. **Privacidad**: No se debe poder vincular un voto con la identidad de quien lo emite.
2. **Integridad**: El resultado final de una elección debe ser la suma exacta de los votos válidos. Nadie puede modificar un voto una vez emitido.
3. **Verificabilidad Individual**: Cada votante puede comprobar que su voto fue incluido en el conteo final.
4. **Verificabilidad Universal**: Cualquiera puede verificar que la suma de los votos emitidos corresponde al resultado final.
5. **Resistencia a terceros**: Ningún votante puede probar a un tercero el contenido de su voto.

3 Análisis de los Enfoques Actuales

A continuación se presenta un análisis de los sistemas de votación actuales respecto a las propiedades enunciadas en la sección anterior.

3.1 Limitaciones del Voto Tradicional

Este sistema satisface las propiedades de *privacidad* y la *resistencia a terceros*, dado que el acto físico en el cuarto oscuro impide vincular un voto con su emisor o probarlo ante un tercero.

Las propiedades de *integridad*, *verificabilidad individual* y *verificabilidad universal* no se garantizan necesariamente.

Las tres dependen tanto del error humano que pueda ser cometido durante el conteo, como la honestidad de la entidad a cargo de la votación. Si esta entidad central es corrupta, ninguna de estas propiedades se cumple.

3.2 El Problema del Voto Electrónico Centralizado

El voto electronico centralizado, si bien mejora la eficiencia temporal y reduce costos, presenta desafios respecto a las propiedades definidas.

La propiedad de *privacidad* no se satisface. Quien ejecuta el sistema podría vincular a quien emite el voto con su contenido ya que, en una versión simple, es la misma entidad la que recibe los votos y autentica a los votantes para, por ejemplo evitar votos duplicados.

Las propiedades de *integridad*, *verificabilidad individual* y *verificabilidad universal* no se garantizan ya que si quien controla la aplicación es corrupto, puede modificar los votos o el conteo final.

La propiedad de *resistencia a terceros* tampoco se cumple, ya que un votante podría mostrarle a un tercero como vota desde su dispositivo. Se cumple si el voto digital se emite desde un cuarto oscuro al igual que en el voto tradicional,

3.3 Blockchain "Naive"

Una primera aproximación para resolver los problemas del voto electrónico sería utilizar una implementación naive usando blockchain. En este esquema, se desplegaría un smart contract que registre cada voto.

En este modelo las propiedades de *integridad*, *verificabilidad individual* y *verificabilidad universal* se cumplen por las propiedades de la blockchain, donde el contenido

es inmutable y público.

Sin embargo, la *privacidad* y la *resistencia a terceros* no se cumplen. Dado que los votos son públicos en la blockchain, cualquiera podría vincular un voto con su emisor.

4 FHE

Como se planteó en la sección anterior, realizar las operaciones necesarias con los datos asociados a los votos sin revelar su contenido es necesario. La solución a estep problema es la criptografía homomórfica.

El cifrado homomórfico permite realizar operaciones sobre datos cifrados sin necesidad de descifrarlos previamente. El resultado de estas operaciones, cuando se descifra, coincide con el resultado que se obtendría si las operaciones se hubieran realizado sobre los datos originales.

Si tenemos una función de encriptación H y dos valores x e y, un esquema homomórfico aditivo cumple que:

$$H(x) + H(y) = H(x + y)$$

Con esta propiedad es posible sumar los votos sin necesidad de descifrarlos previamente, preservando la privacidad de los votantes.

Existen distintos niveles de homomorfismo. Los esquemas Parcialmente Homomórficos (PHE) permiten realizar solo un tipo de operación (sumas o multiplicaciones, pero no ambas).

Fully Homomorphic Encryption (FHE) permite realizar tanto sumas como productos sobre datos cifrados.

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.