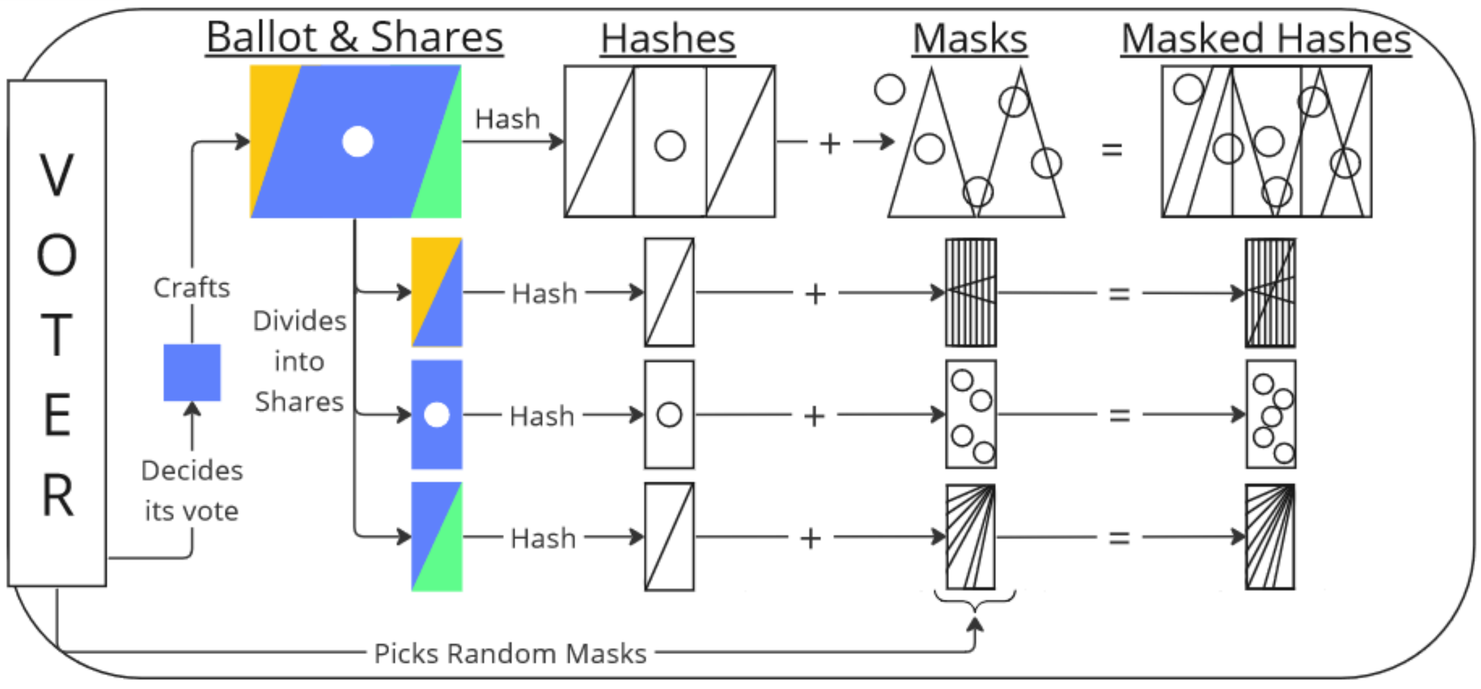
ALFA Group, Valencian Research Institute for Artificial Inteligence, Polytechnic University of Valencia (UPV)

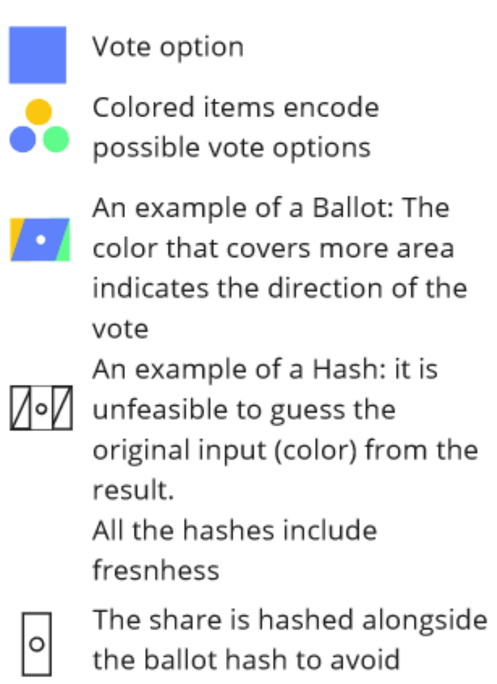
SUVS-r: Secure Unencrypted Voting Scheme with revocation

Jose Luis Martin-Navarro, Antonio M. Larriba, Damián López

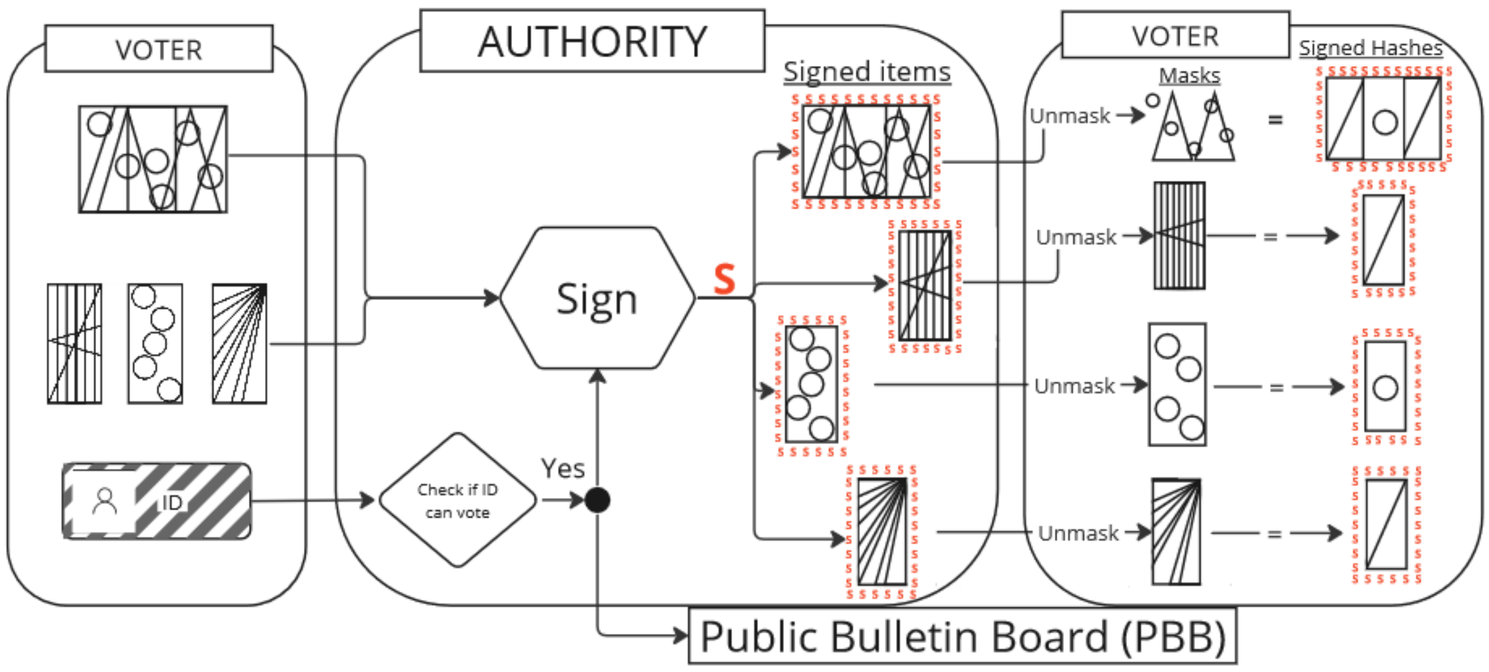
We developed a voting protocol that ensures the **anonimity** of the voter and the **transparency** and **correctness** of the results even with **non-trusted authorities**.
The protocol highlights are: **Universal verifiability**, where any entity can verify the elections results; **Vote Immutability**, with votes that cannot be altered (achieved by the Public Bolletin Board); **Revocation**, which allows a voter changing its vote; and **Cast-as-Intended**, where votes are recorded accurately (Step Y).
The security and privacy of the elections is ensured by combining *Blind signatures* and a novel ballot construction, that divides the ballot into shares, distributing the trust into all the parties involved.

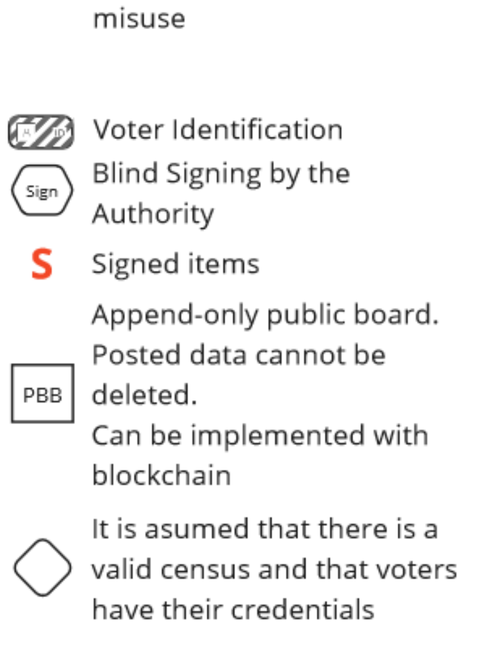
Step 1: Prepare Ballot



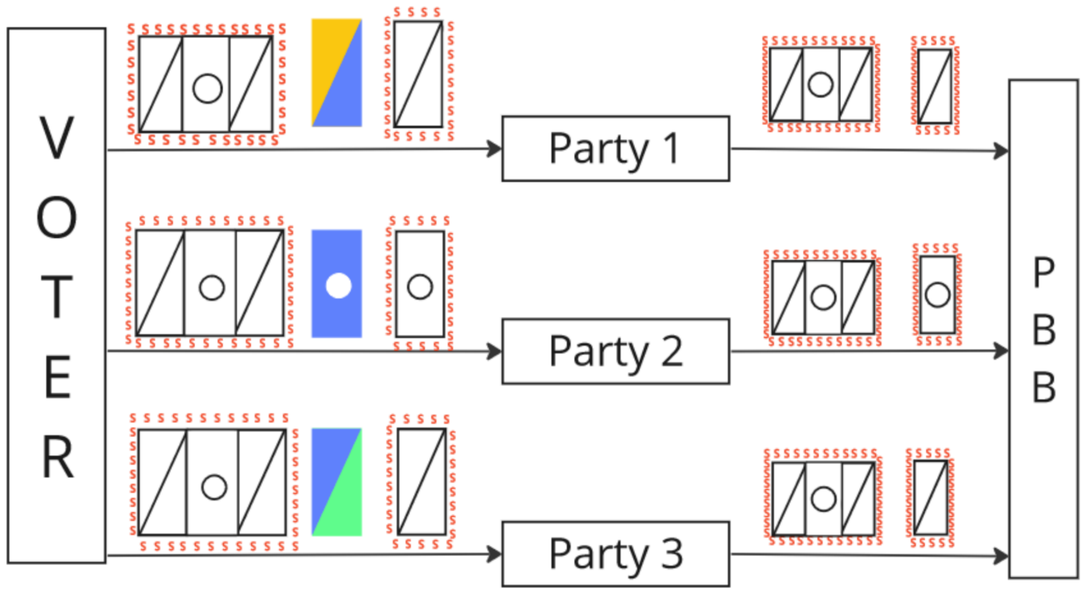


Step 2: Certify Ballot





Step 3: Cast Ballot

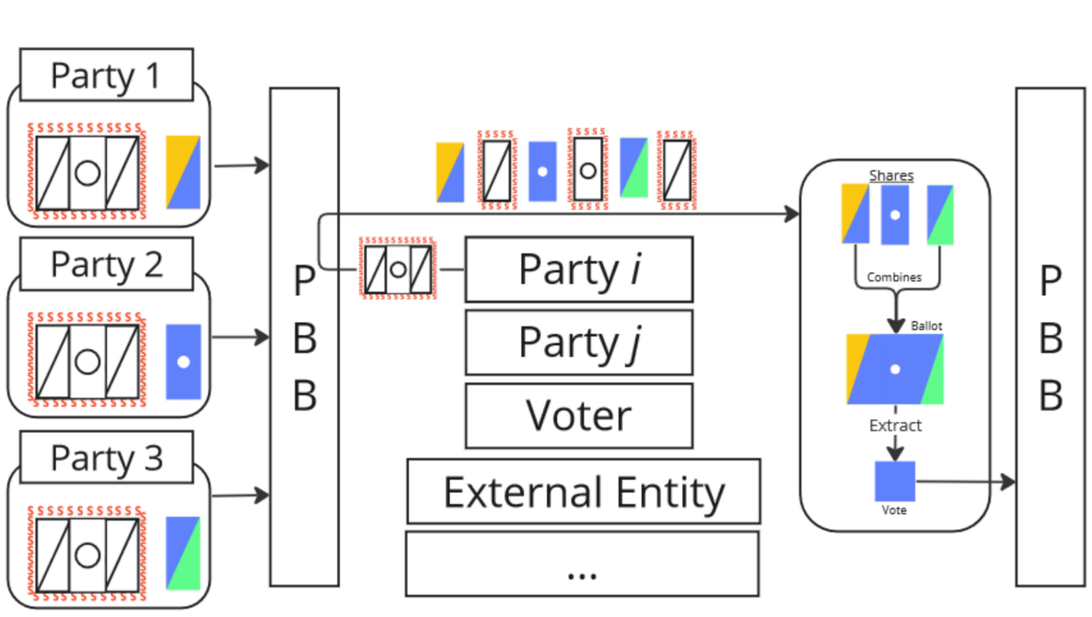


Both revocations, Step X and Step Y, can be performed multiple times before the Tally (Step 4) starts.

The revoken signed hashes are shared by the Authority with the rest of the entities.

Step 4: Tally

(With every received signed hash)



Note: Colors and Shapes are random examples for showcasing the protocol's workflow.

By INCIBE's Chair, funded by the EU-NextGenerationEU through the Spanish government's Plan de Recuperación, Transformación y Resiliencia. **Contact**: jomarna6@upv.es

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
VRAIN Valencian Research Institute for Artificial Intelligence