Voting: You Can't Have Privacy without Individual Verifiability

- Reference:
    - https://hal.inria.fr/hal-01858034/document

- Problem Statement
    - Two main security goals of electronic voting
        - Vote Privacy
        - Verifiability
            - Individual Verifiability
                - a voter can check that her ballot is counted
            - Universal Verifiability
                - anyone can check that the result corresponds to the published ballots
            - Eligibility Verifiability
                - only legitimate voters may vote

- Contribution
    - Privacy implies individual verifiability
    - Systems without individual verifiability cannot achieve privacy