Fully Transparent, Verifiable, Assurable, and Deployable (Remote) Electronic Voting Enabling Open and Fair Elections

A. Problem and Solution:

Have you ever voted in some elections? Are you sure that your vote is counted after casting your ballot? Did you feel frustrated and even painful during the 2000 general election amid of life-threatening COVID-19 pandemic?

- A gap between casting secret ballots and tallying & verifying individual votes in existing voting platforms.
  - Due to disconnection between ballot-casting and vote-tallying & verification or opaque transition (e.g., due to encryption) from ballot-casting to vote-tallying.
  - Impossible (very difficult) for voters to verify their individual votes and whether their votes are indeed counted.

- A groundbreaking e-voting protocol that fills this gap & delivers fully transparent, verifiable, practical, remote voting & election.
  - Allows voters to see and verify their own plain votes and also anyone to verify all individual plain votes and conduct tallying.
  - Voters, as well as the public, are visually and technologically assured that all votes are indeed counted and the final tally is accurate.

B. Principles: One assumption: two or more interest-conflicting parties which won’t share information and act as tallying authorities: C1 and C2

- Two basic cryptographic primitives: (1) (n,n) secret sharing, and (2) secure two-party multiplication (STPM). Plus, Pedersen Commitment.
- Three technical designs (TD): (1) verifiable tallied voting vector & tallies, (2) mutual-lock voting, and (3) in-process verification and enforcement.

C. Protocol: texts/symbols in blue are all public and viewable by anyone and the ones in red are secret.

D. Public bulletin board: seamless transition from ballots to all individual plain votes:

E: Election phases:

1. Voter registration. (as usual, suppose n voters).
   - a. C1 and C2, using a novel STPM-based Location Anonymization scheme, generate a private sequence of r1,1,…,ri,n and r2,1,…,r2,n respectively, such that li=r1,i+r2,i is a unique location in 1 to n.
   - Voting / ballot casting:
     - a. When a voter log in system to vote, she receives r1,i and r2,i from C1 and C2, gets her unique location li=r1,i+r2,i and computes her vote vi and v'i. TD2 and TD3 are applied.
     - b. Commitment: using Pedersen commitment, Vi commits her vote and C1 and C2 commit their shares.
   - Tally and verification by anyone:
     - a. All ballots pi's and p'I 's are aggregated respectively and the final aggregation is the tallied voting vector (two of them, reversing each other exactly).
     - b. TD1 applies. Voters can verify their individual plain votes. Anyone can tally and verify.

F: Summary (what we/you get?):

- An elegant, simple, verifiable, and assurable e-voting protocol and a fully transparent, verifiable, seamless, solid and practical (remote) e-voting platform.
- Ballots and plain votes are all publically viewable and verifiable. Transition from ballots, to votes, to tally is open and seamless.
- Individual voters can verify their own votes and are technically and visually assured that their votes are indeed counted in the final tally.
- No partial result disclosure: enabling open and fair elections with full voter assurance, even for the voters of minor or weak political parties.