A. Problem Statement

• A gap between casting secret ballots and tallying & verifying individual votes.
• Due to disconnection between the vote-casting process and the vote-tallying process or opaque transition (e.g., due to encryption) from vote-casting to vote-tallying.
• A groundbreaking e-voting protocol that fills this gap and provides a fully transparent election.

B. Proposed protocol

1. Split S, into distribute shares
2. Sum up received shares (and its own) and publish the result
3. Similarly, for $S'$.

C. A Voting Example and Web Based Dynamic Bulletin Board

What we get?

• Seamless, viewable, verifiable, and privacy-preserving transition from vote-casting to vote-tallying
• Individual voters can verify their own votes and are technically and visually assured that their votes are indeed counted in the final tally
• Public can verify the accuracy of the count, political parties will be able to catch fraudulent votes
• Secrecy of any voter’s vote is remained
• Transparent e-voting protocol: enable open and fair elections with full voter assurance, even for the voters of minor or weak political parties.

Dr. Xukai Zou (xkzou@cs.iupui.edu), Yan Sui, Huian Li, Wei Peng, and Dr. Feng Li