CERIAS

The Center for Education and Research in Information Assurance and Security

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.

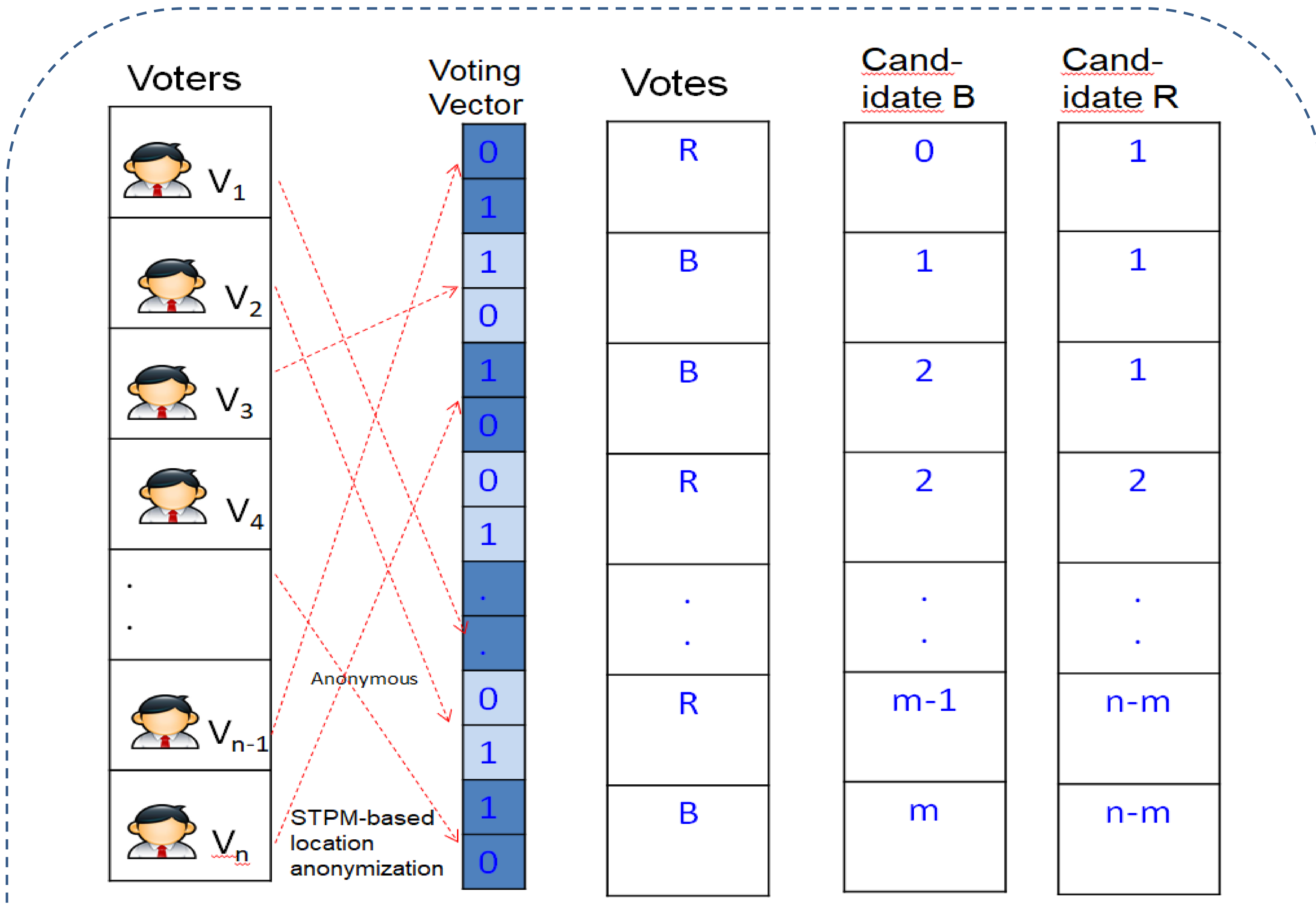
B. Principles:

One assumption: two or more interest-conflicting parties which won't share information and act as tallying authorities: C_1 and C_2

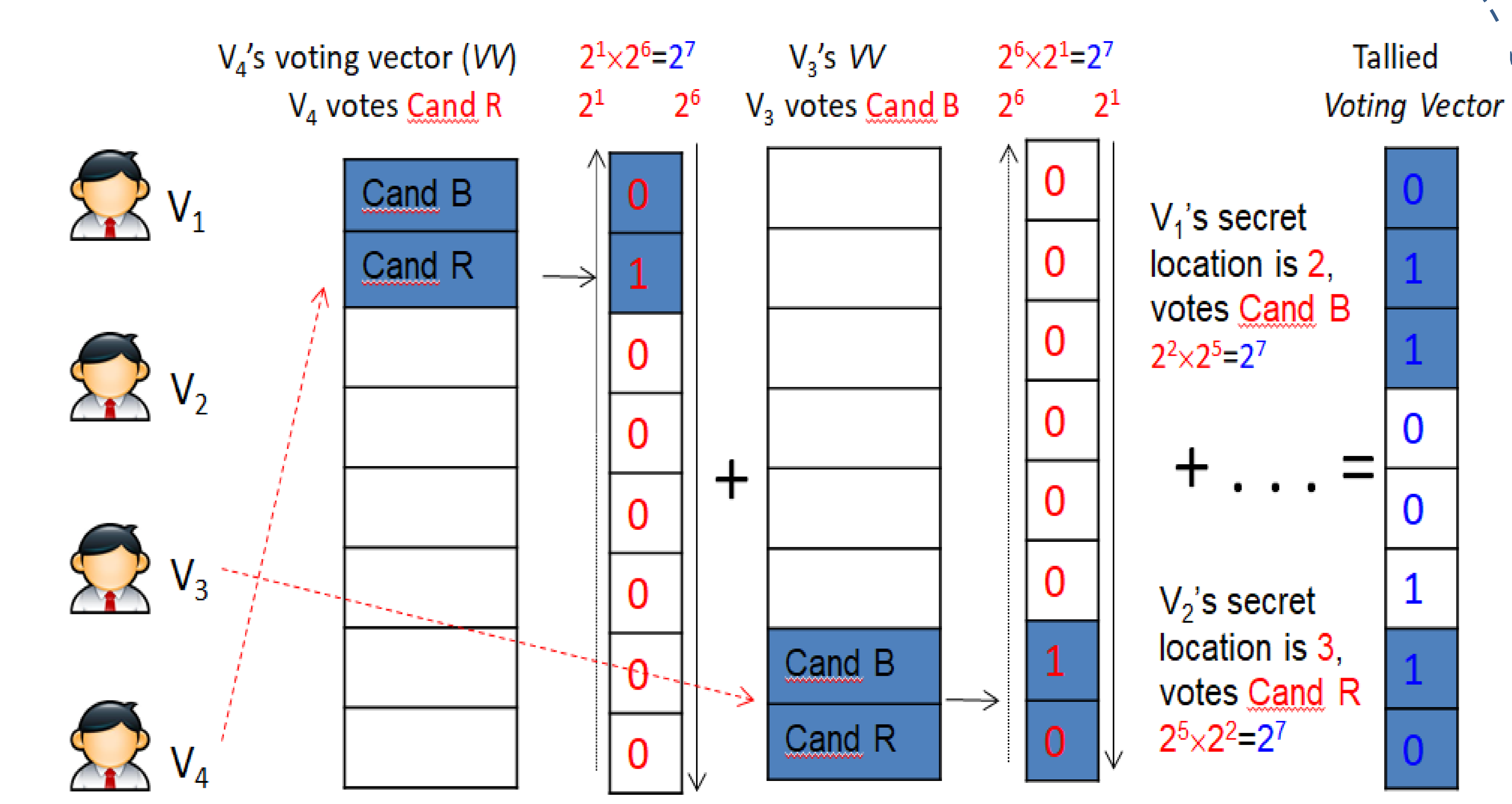
Two basic cryptographic primitives: (1) (n,n) secret sharing, and (2) secure two-party multiplication (STPM). Plus, Pedersen Commitment.

Three technical designs (TD): (1) verifiable tallied voting vector & tallies, (2) mutual-lock voting, and (3) in-process verification and enforcement.

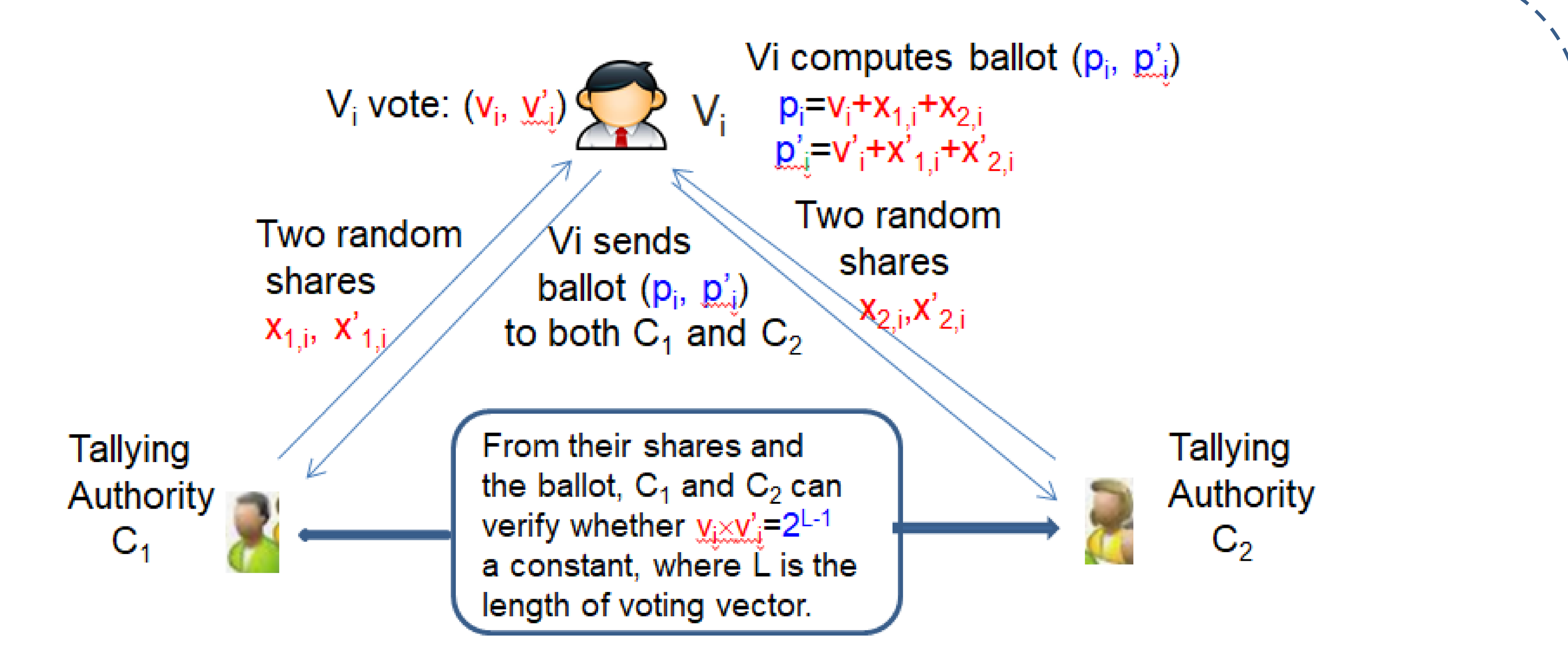
C. Protocol: texts/symbols in blue are all public and viewable by anyone and the ones in red are secret.



TD1: Fully transparent, visual, and verifiable tallied voting vector and tallies. Every voter has her own unique secret location (the index in voting vector and can see and verify the vote at her location is indeed what she voted.



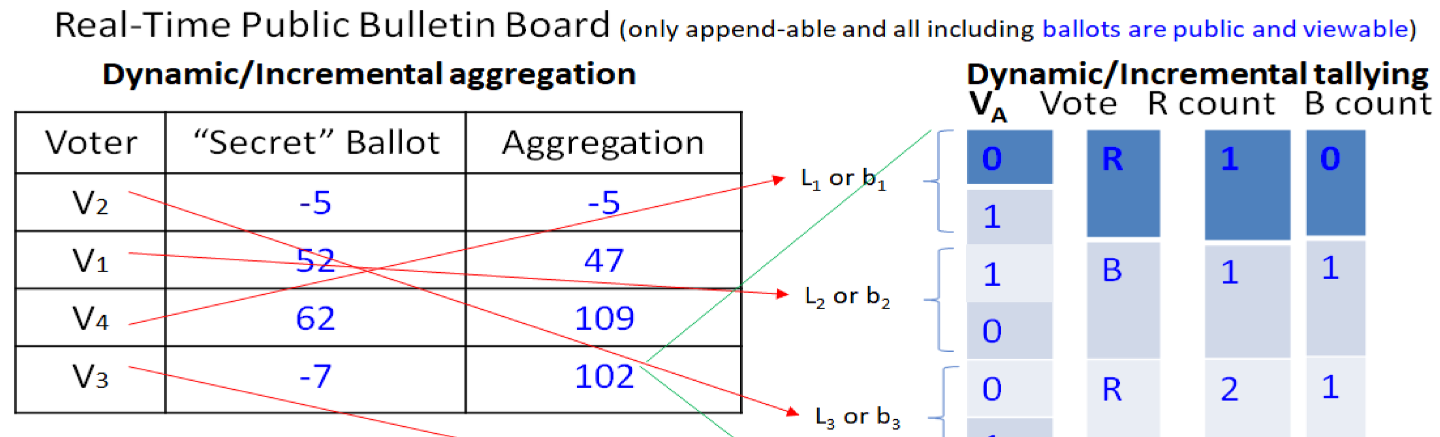
TD2: mutual lock voting – voter's private voting vector can be converted to two numbers whose product is a constant



TD3: in-process check and enforcement: C_1 and C_2 jointly check the validity of the ballot & enforce V_i to vote for one and only one candidate, using STPM without sharing their secret shares directly.

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

Real-Time Public Bulletin Board (only append-able and all including ballots are public and viewable)



Voter	"Secret" Ballot	Aggregation
V2	-5	-5
V1	52	47
V4	62	109
V3	-7	102

1. Aggregation of "secret" ballots by anyone when ballots are being cast in real time.
2. Partial sums -5, 47 and 109 have no information about (any) votes.
3. The last aggregation 102 (=32+4+2+64) exposes all votes.
4. Voters can verify their votes visually.

A voting example involving 4 voters and 2 candidates: R & B (numbers in red are kept secret)
Red numbers with black underline are computed by voters, with blue double line generated by collector C1, and with green wavy line by collector C2

Voter V_i	Secret location L_i	Secret vote v_i	Secret random shares of C1 and C2 For V1: 5: received from C1; 15: from C2; $x_{1,i}$ $x_{2,i}$	"Secret" ballot – published, so they are in fact public For V1: 5: received from C1; 15: from C2; 52: computed as 32+5+15 by voter herself
V_1	2	B (32)	5, 15	52 (=32+5+15)
V_2	3	R (4)	1, -10	-5 (=4+1+(-10))
V_3	4	B (2)	-20, 11	-7 (=2+(-20)+11))
V_4	1	R (64)	14, -16	62 (=64+14+(-16))

E: Election phases:

1. Voter registration. (as usual, suppose n voters).
   a. C_1 and C_2, using a novel STPM-based Location Anonymization Scheme, generate a private sequence of $(r_{1,1},\ldots r_{1,n})$ and $(r_{2,1},\ldots r_{2,n})$ respectively, such that $l_i=r_{1,i}+r_{2,i}$ is a unique location in 1 to n.
2. Voting / ballot casting: a. When a voter log in system to vote, she receives $r_{1,i}$ and $r_{2,i}$ from C_1 and C_2, gets her unique location $l_i=r_{1,i}+r_2$ and computes her vote v_i and v'_i. b. TD2 and TD3 are applied.
   c. Commitment: using Pedersen commitment, V_i commits her vote and C_1 and C_2 commit their shares.
3. Tally and verification by anyone. a. All ballots p_i'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.

PURDUE UNIVERSITY

Nathan Swearingen (nswearin@iupui.edu), Xukai Zou (xzou@iupui.edu)
Ninghui Li (ninghui@purdue.edu) and Feng Li (fengli@iupui.edu)

CERIAS