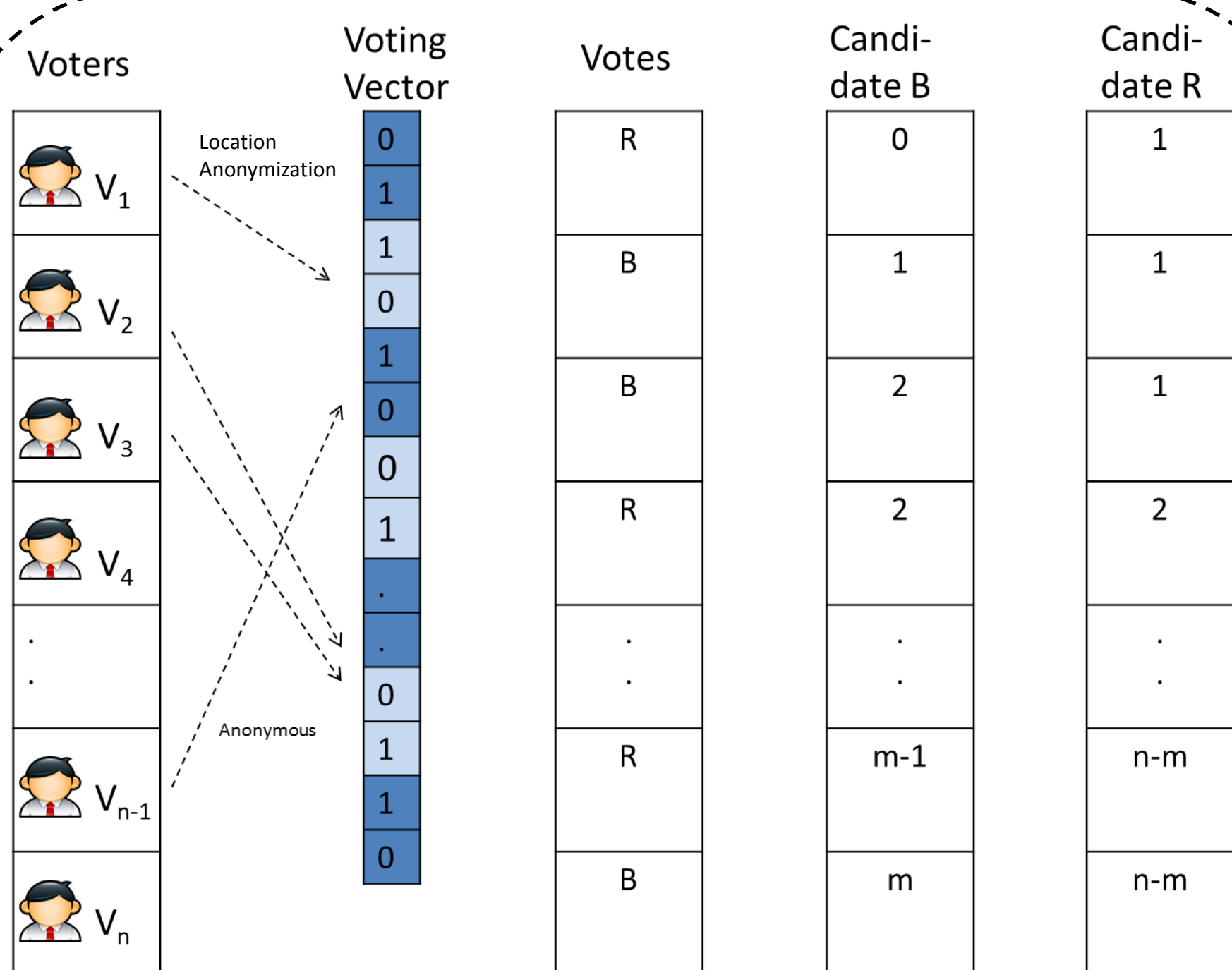


Mutual Restraining Voting Involving Multiple Conflicting Parties

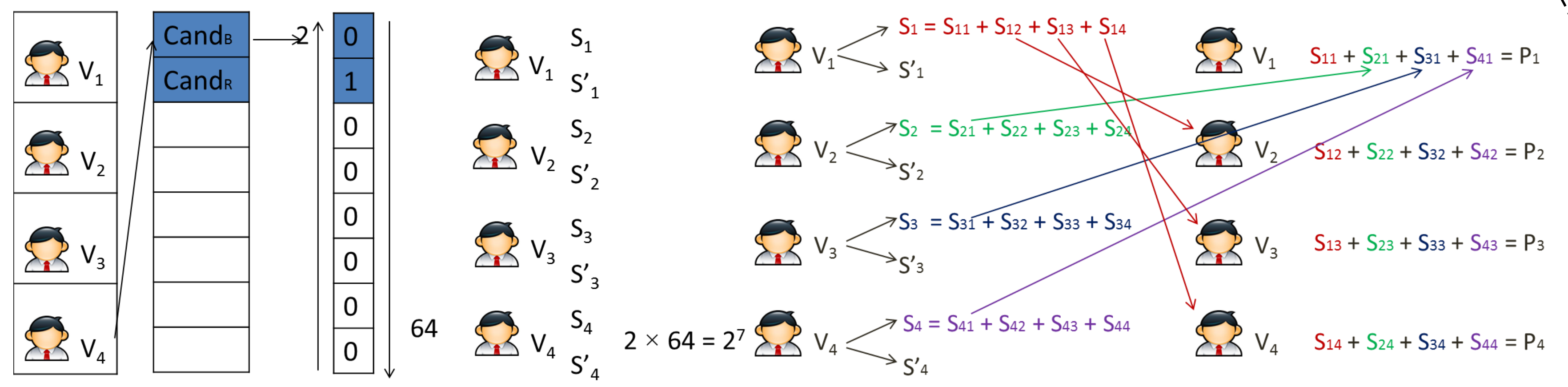
A. Problem Statement

- 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



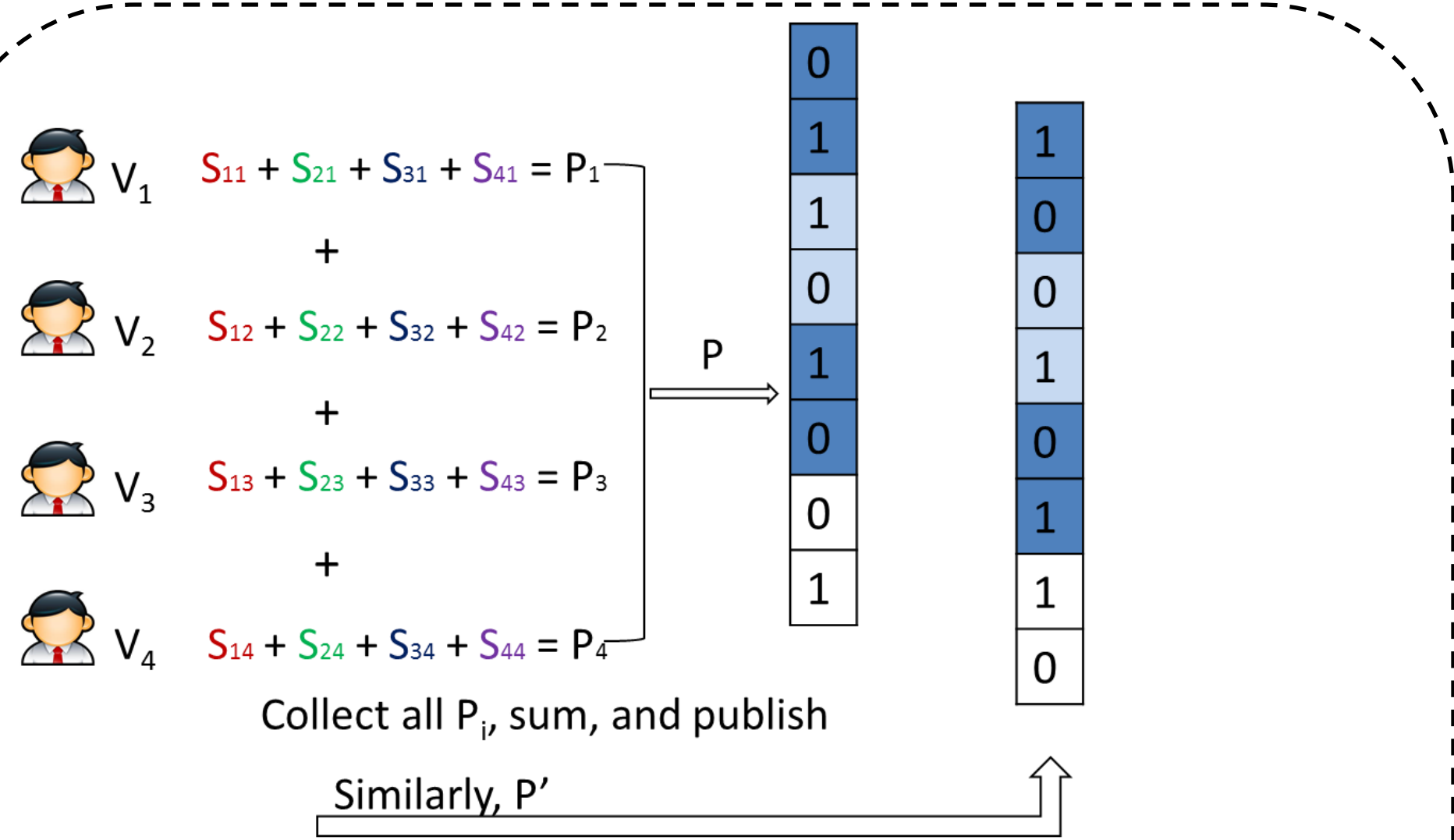
TP1: Visual bulletin board: universally verifiable tallied voting vector and (incremental) tallies.



$S_4 \times S'_4 = 2 \times 2^6 = 2^7$
 For any voter, $S_i \times S'_i = 2^{N-1}$ where $N (=4 \times 2=8 \text{ here})$ is the length of the voting vector. Enforce one and just one vote.

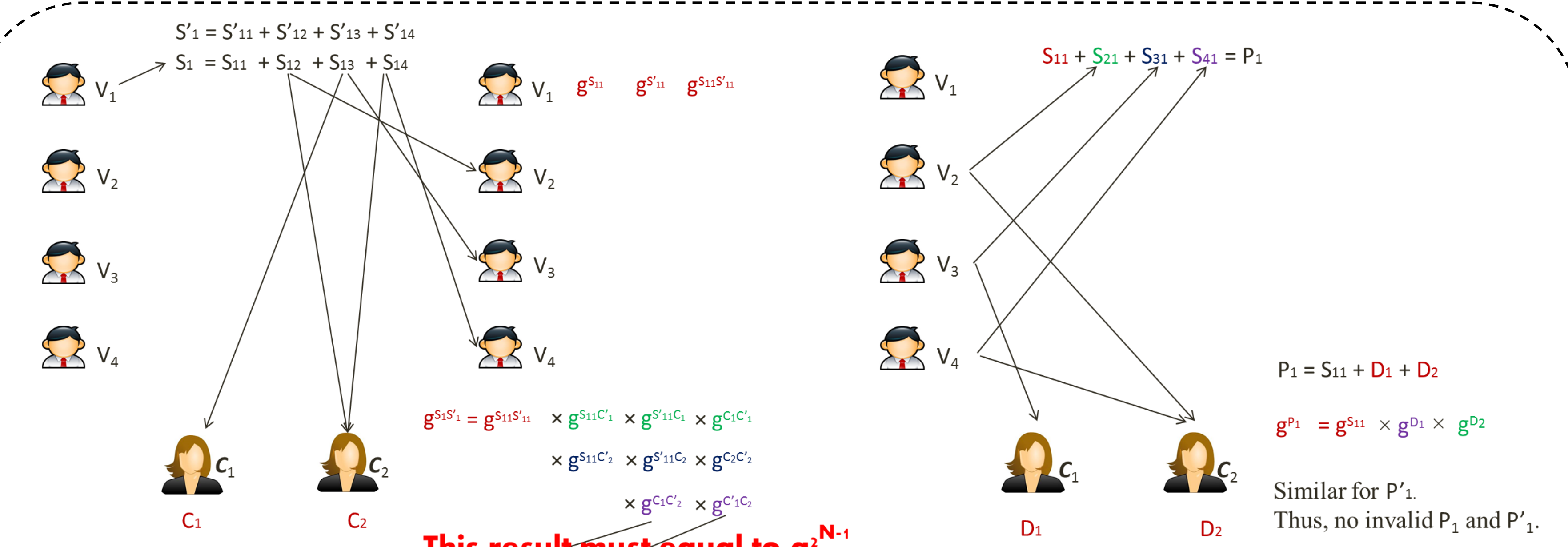
1. Split S_i into and distribute shares
2. Sum up received shares (and its own) and publish the result Similarly, for S'_i .

TP2: forward and backward mutual lock voting by simplified (N,N) secret sharing.



P is an reverse of P' , they mutually verify and enforce each other. Since all P_i are published, any voter can tally votes by simply summing them.

Votes collection.



This result must equal to $g^{2^{N-1}}$.
 $g^{C_1 C_2}$ and $g^{C_1 C_3}$ are computed by STPM

TP3: in-process verification and enforcement, using Secure Two Party Multiplication (STPM).

C. A Voting Example and Web Based Dynamic Bulletin Board

Voter	Secret Location	Vote	Shares		Secret ballot
			Self-computed	Server generated	
V ₁	2	B (32)	12 (=32-5-15)	<u>5</u> , 8,7 (sum=15)	45 (=12+1+15+17)
V ₂	3	R (4)	13 (=4-1-(-10))	<u>1</u> , -3,-7 (sum=-10)	28 (=5+13+7+3)
V ₃	4	B (2)	-10 (=2-15-(-3))	15, <u>7</u> , -10 (sum=-3)	30 (=8+(-3)+(-10)+35)
V ₄	1	R (64)	9 (=64-17-38)	17, <u>3</u> , 35 (sum=38)	-1 (=7+(-7)+(-10)+9)

A voting example involving 4 voters and 2 candidates (R and B): Notes: shares with underline are generated by Server 1, e.g., 5 of V₁ and 7 of V₃, and shares in red are generated by Server 2, e.g., 8 of V₁ and 15 of V₃.

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.

Incremental aggregation			Incremental tallying			
Voter	Secret Ballot	Aggregation	V _A	Vote	R counts	B counts
V ₂	28	28	0	R	1	0
V ₁	45	73	1	B	1	1
V ₄	-1	72	0	R	2	1
V ₃	30	102	1	B	2	2
			0			

1. Incremental aggregation of the cast secret ballots
2. All partial aggregations 28, 73, and 72 has no information on votes
3. Last aggregation 102 (=32+4+2+64) exposes all votes and it is the final tallied voting vector V_A