Towards Secure Internet e-Voting

Yvo Desmedt[1,2] Stelios Erotokritou[1] Rebecca Wright[3]

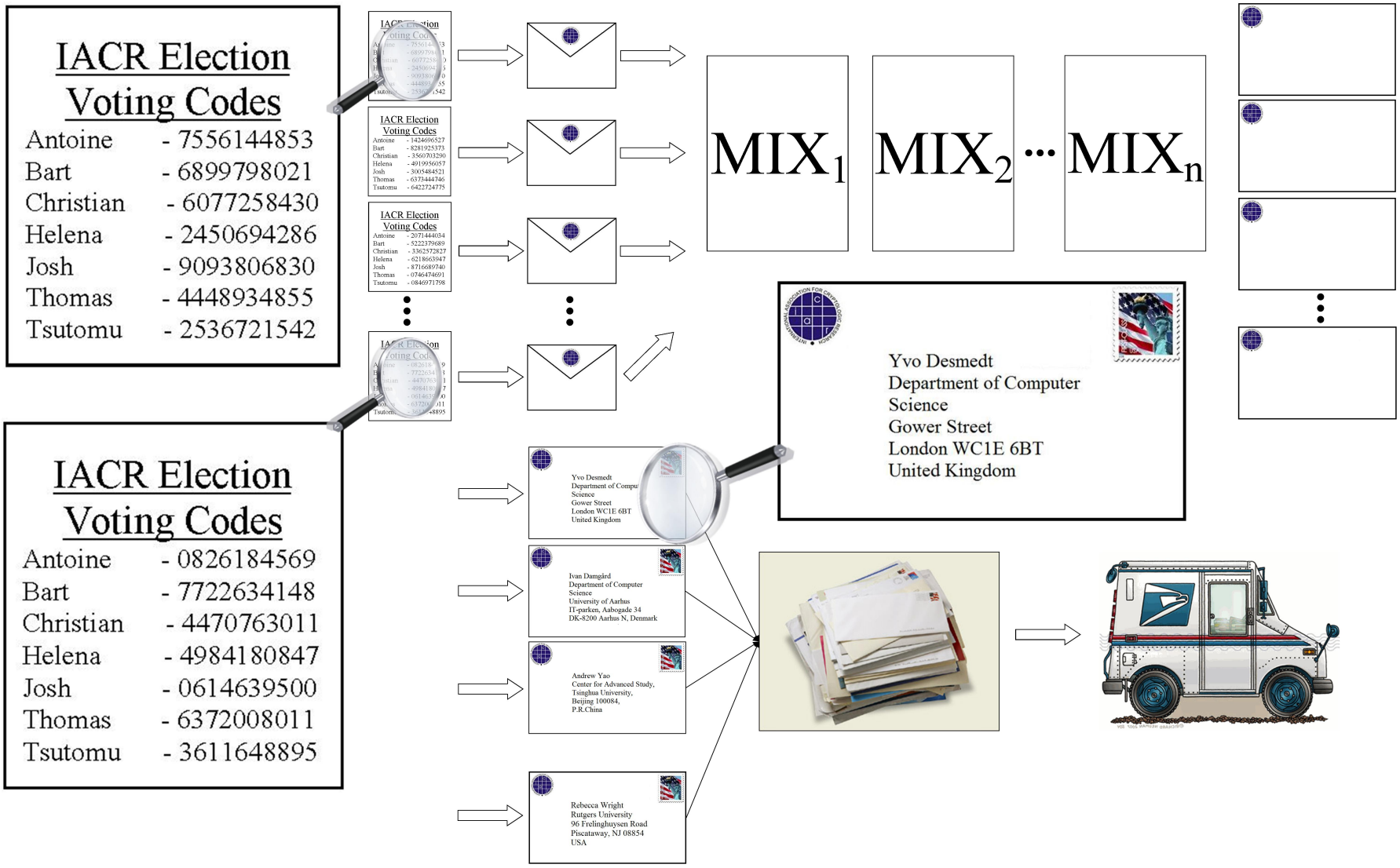
[1] Department of Computer Science
University College London, UK

[2] Research Center for Information Security (RCIS)
AIST, Japan

[3] Computer Science Department and DIMACS
Rutgers University

August 17, 2010

1. CODE VOTING



IACR Election Voting Codes

Antoine	- 8173472492
Bart	- 9287374672
Christian	- 0198291639
Helena	- 2373919017
Josh	- 2638939283
Thomas	- 1923872622
Tsutomu	- 8294729027

AIST

UCL

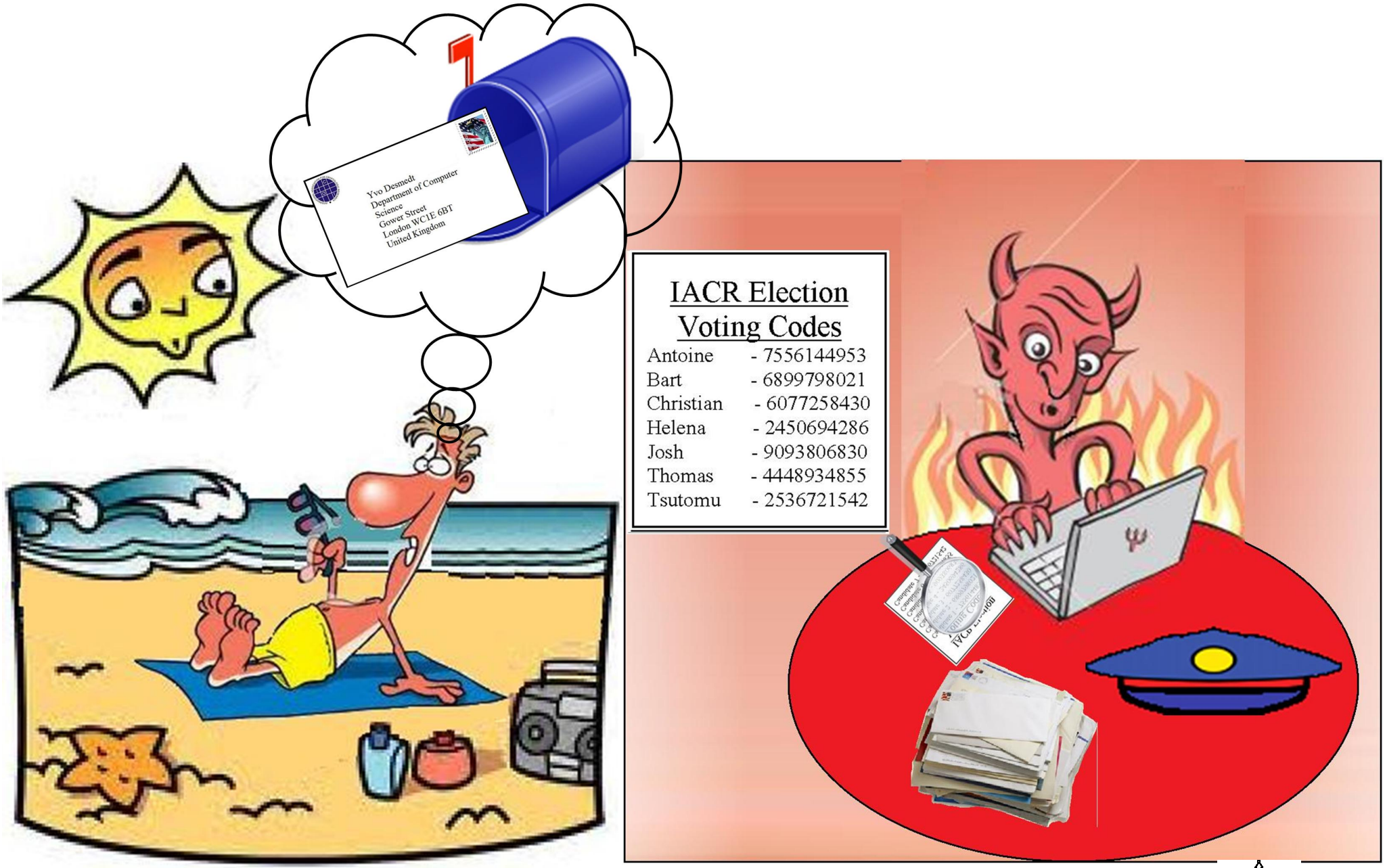
2. ADVANTAGES/DISADVANTAGES

Advantages of Code Voting: secure even if voter's machine hacked.

Disadvantages:

- requires IACR to send random numbers by postal mail, and
- no collusion between postal system (or sender of envelopes) and the party receiving the vote.

Ballot stuffing with Code Voting



3. VOTING USING OUR SOLUTION

IACR Election Voting Codes
Antoine - 2613
Bart - 9384
Christian - 8173
Helena - 6734
Tsutomu - 4832

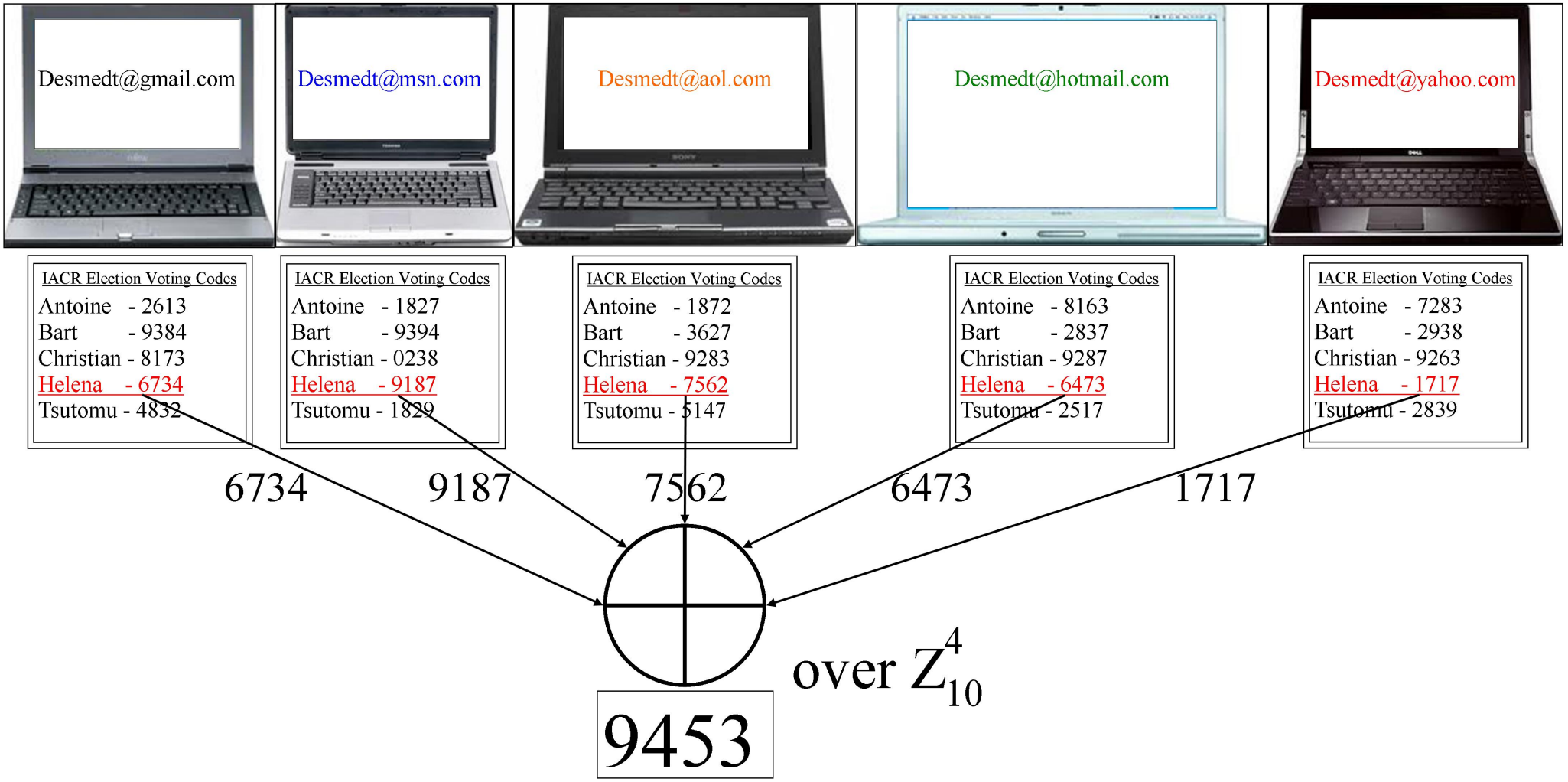
IACR Election Voting Codes
Antoine - 1827
Bart - 9394
Christian - 0238
Helena - 9187
Tsutomu - 1829

IACR Election Voting Codes
Antoine - 1872
Bart - 3627
Christian - 9283
Helena - 7562
Tsutomu - 5147

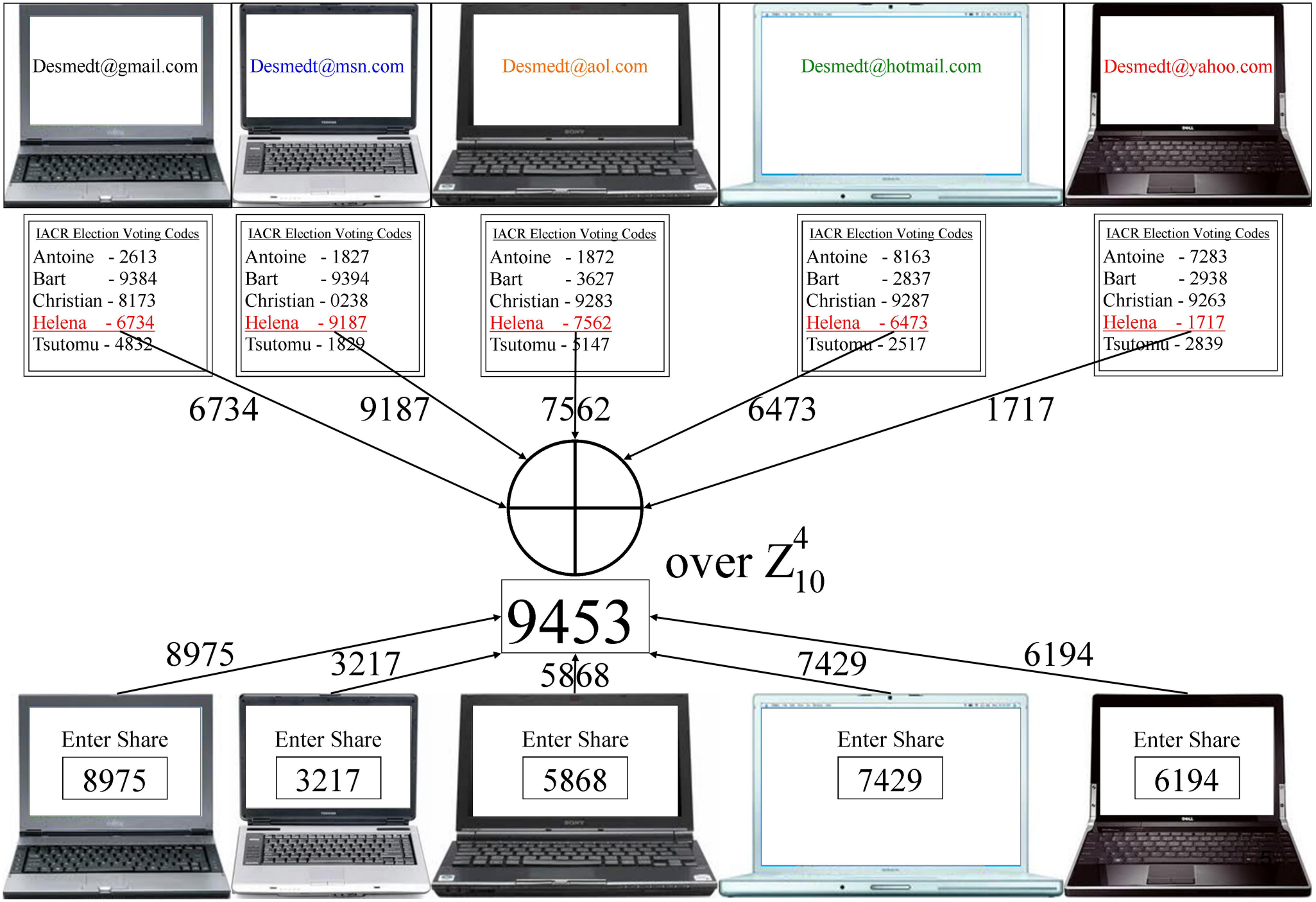
IACR Election Voting Codes
Antoine - 8163
Bart - 2837
Christian - 9287
Helena - 6473
Tsutomu - 2517

IACR Election Voting Codes
Antoine - 7283
Bart - 2938
Christian - 9263
Helena - 1717
Tsutomu - 2839

3. VOTING USING OUR SOLUTION



3. VOTING USING OUR SOLUTION



So main requirement for the voter:

So main requirement for the voter:

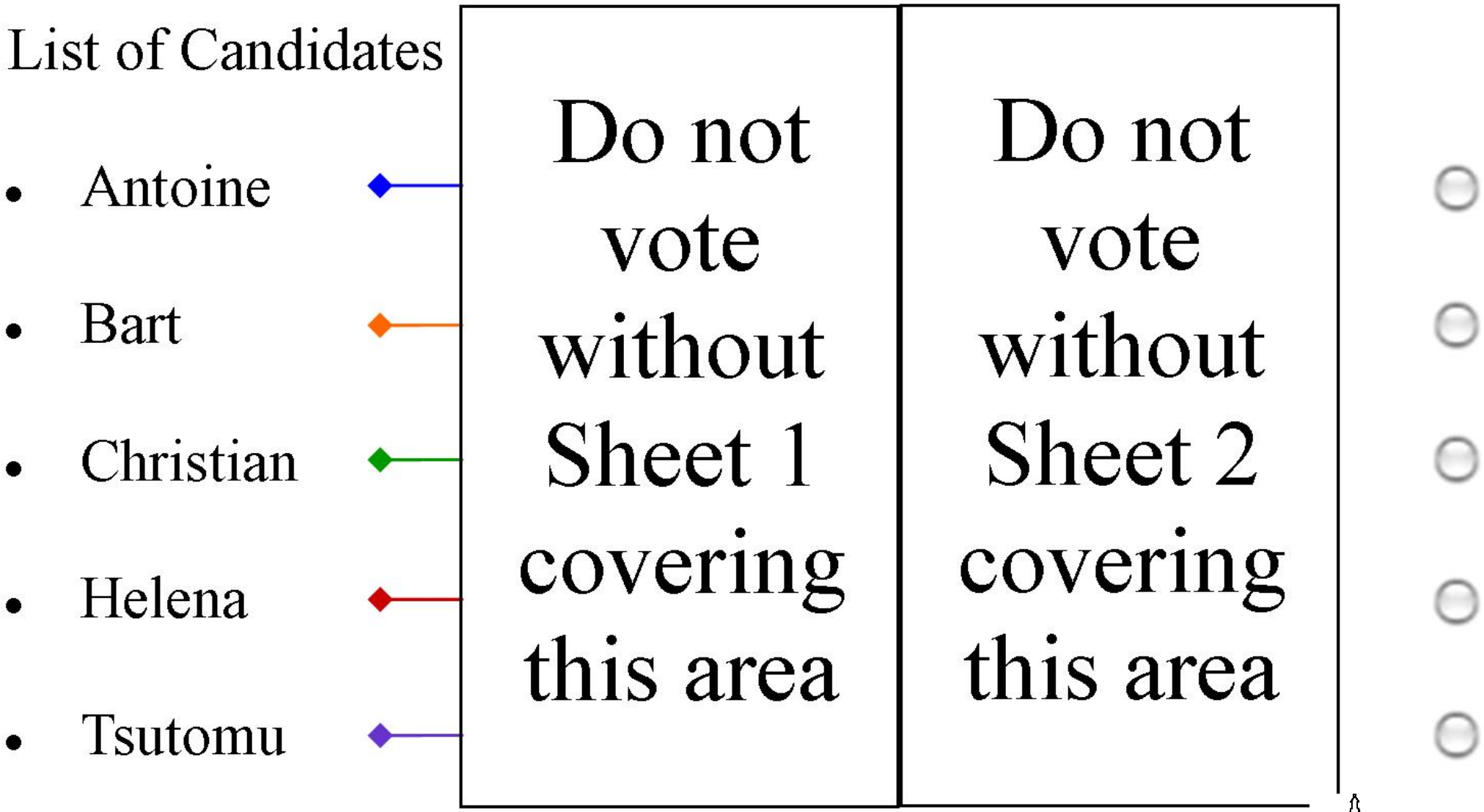
is to be able to add numbers mod 10.

So main requirement for the voter:

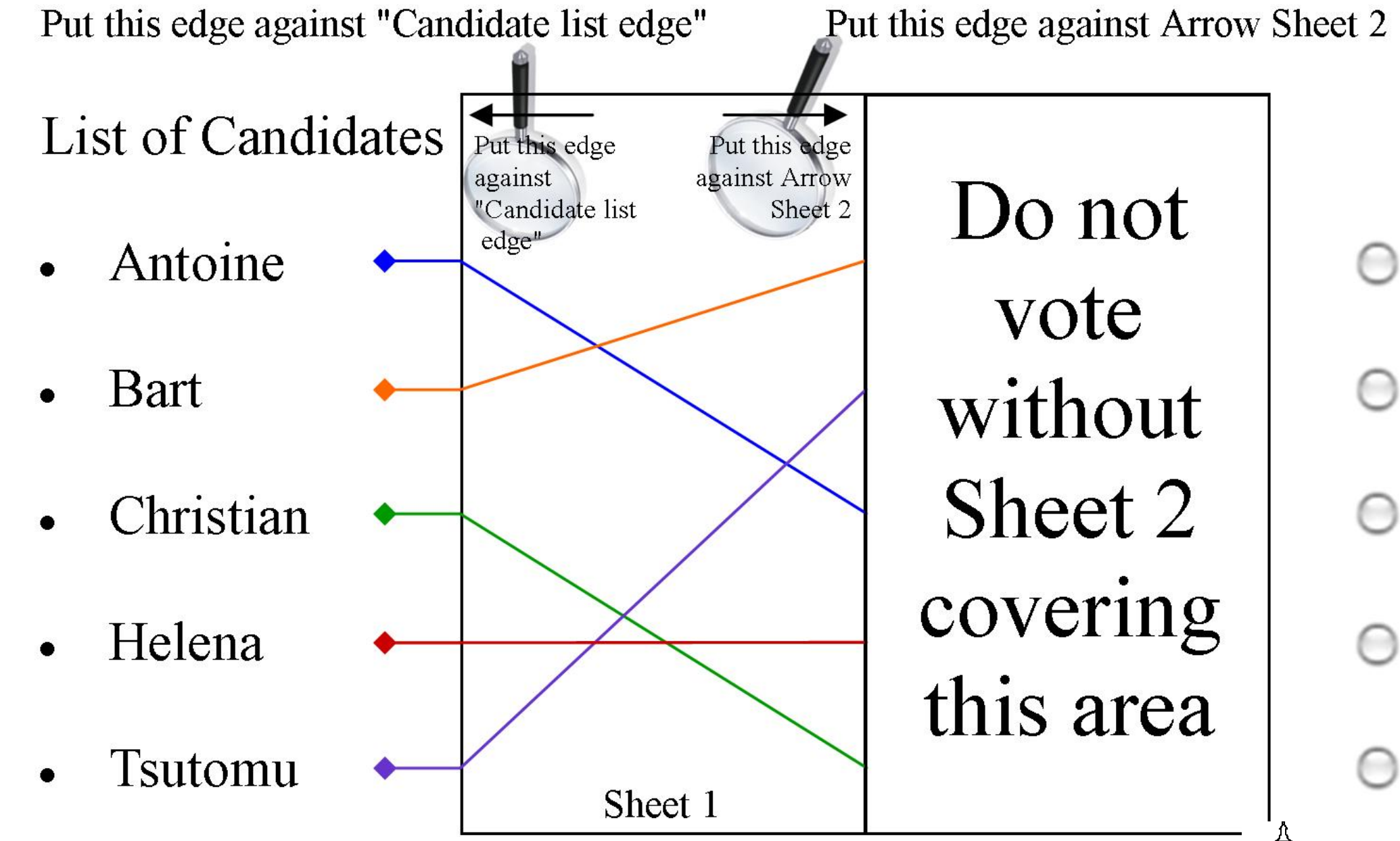
is to be able to add numbers mod 10.

Cryptographers should be able to do this (otherwise they should not vote!).

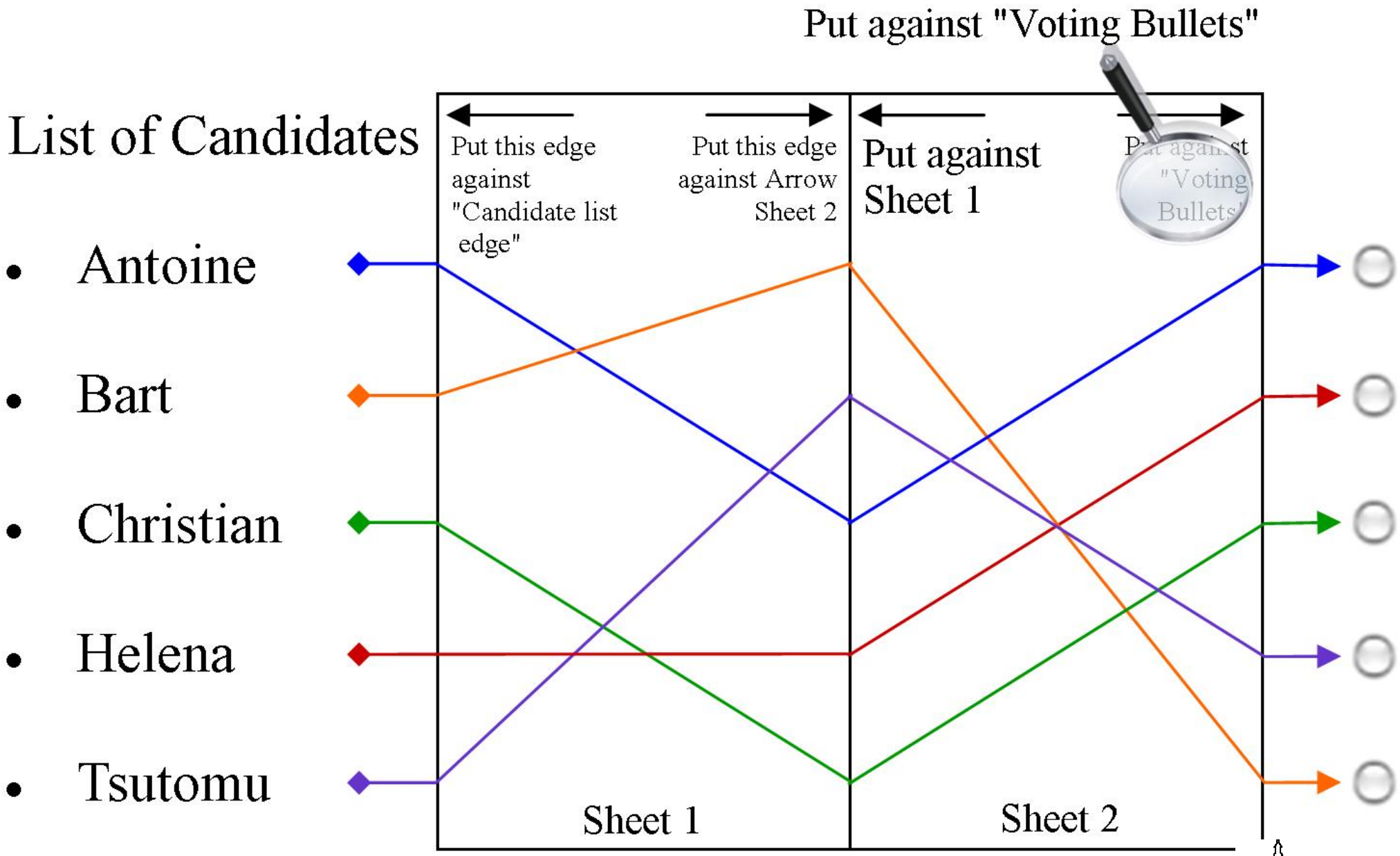
4. AVOIDING MOD 10



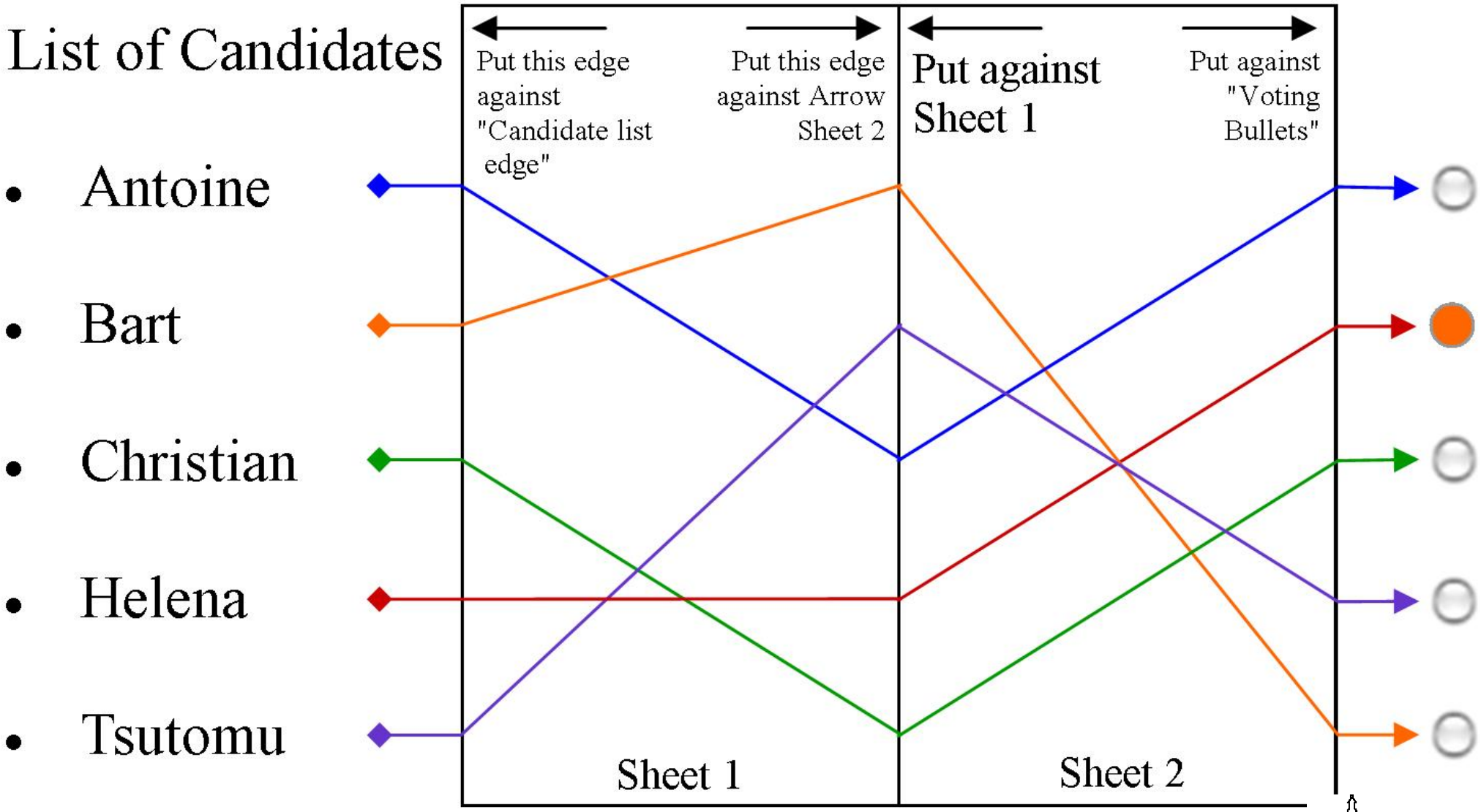
4. AVOIDING MOD 10



4. AVOIDING MOD 10



4. AVOIDING MOD 10



5. CORRECTNESS AND DETAILS

Using different secret sharing schemes and PSMT protocols, we can achieve 100% correctness against a t-limited adversary.

New primitives to achieve all this:

- (P)SMT with a Human, and
- Private Anonymous Communication.