Encrypting your vote in JavaScript

Ben Adida

August 8th, 2011
EVT/WOTE 2011 Rump Session
more than 42,000 votes cast
v3.1 Release

- a number of UI tweaks (not enough)
  - especially on administration

- JavaScript-only version in testing
  - randomness generation needs more review

- mixnet integration?
  - requires a good bit more work on administration

- private elections
  - trade-off some verifiability for privacy

- external voter-list management
  - Facebook groups.
JavaScript Performance

- 2 years ago:
  - 1 modexp = 750ms-2s

- Today:
  - 1 modexp = 75-100ms
  - one candidate per second (or better).

- One more trick: Worker threads
go vote!

http://heliosvoting.org