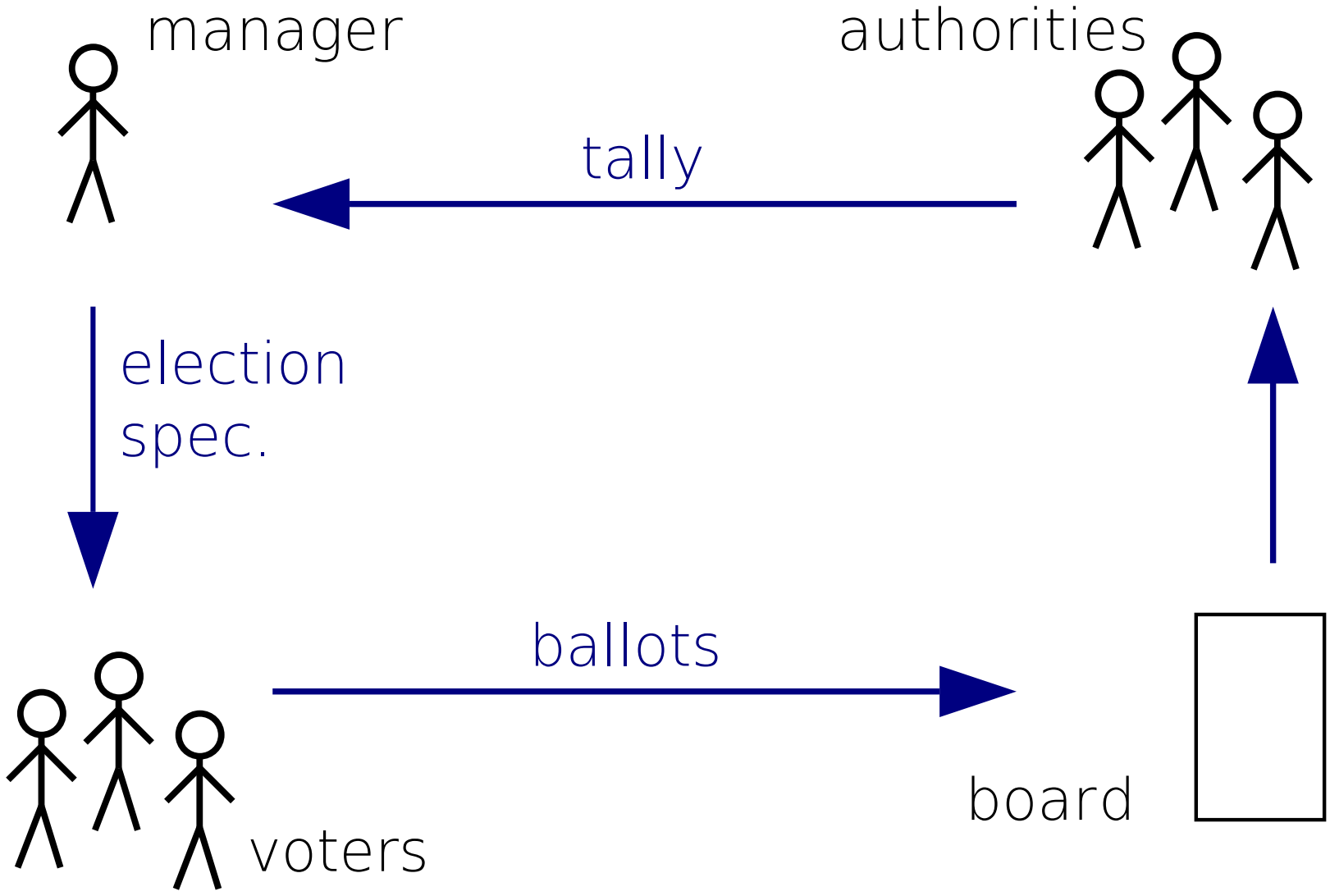
From Voting to Surveys

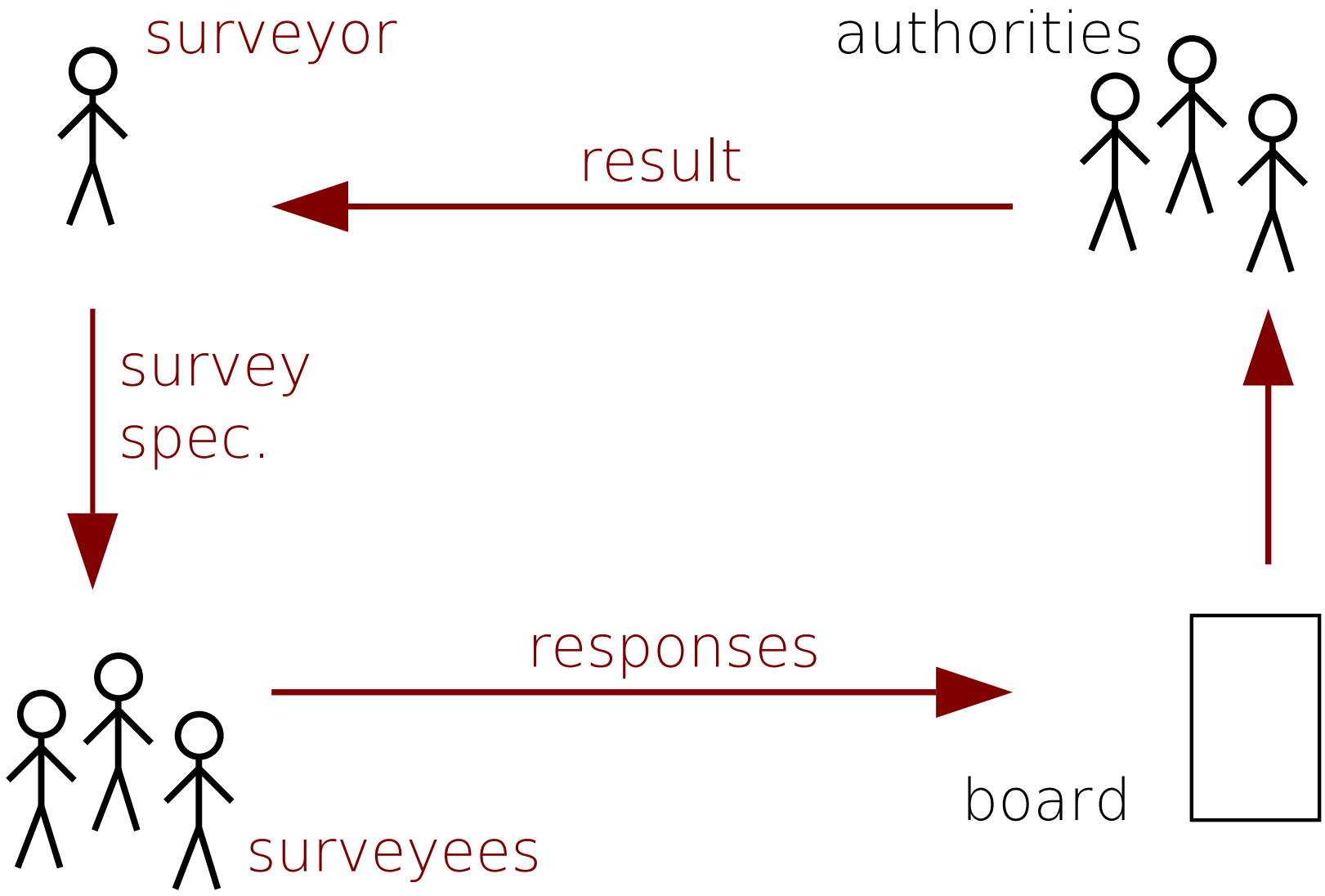
David Bernhard, Markulf Kohlweiss,
Cedric Fournet, George Danezis

Microsoft Research, Cambridge

Voting


manager
authorities
tally
election
spec.
ballots
voters
board

~~Voting~~ Surveys



Voting

votes

Surveys

name

age

gender

personal info
(medical etc.)

Voting

result (function)

hom. / linear

Surveys

statistics

disclosure control

Voting	Surveys
public results	?
verifiability	?
every vote counts!	statistics, samples, margin of error

Surveys

~~homomorphic~~

~~mix-nets~~

nonlinear stat's

record privacy

Surveys

~~homomorphic~~

~~mix-nets~~

nonlinear stat's

record privacy

Our solution: SPDZ

SPDZ

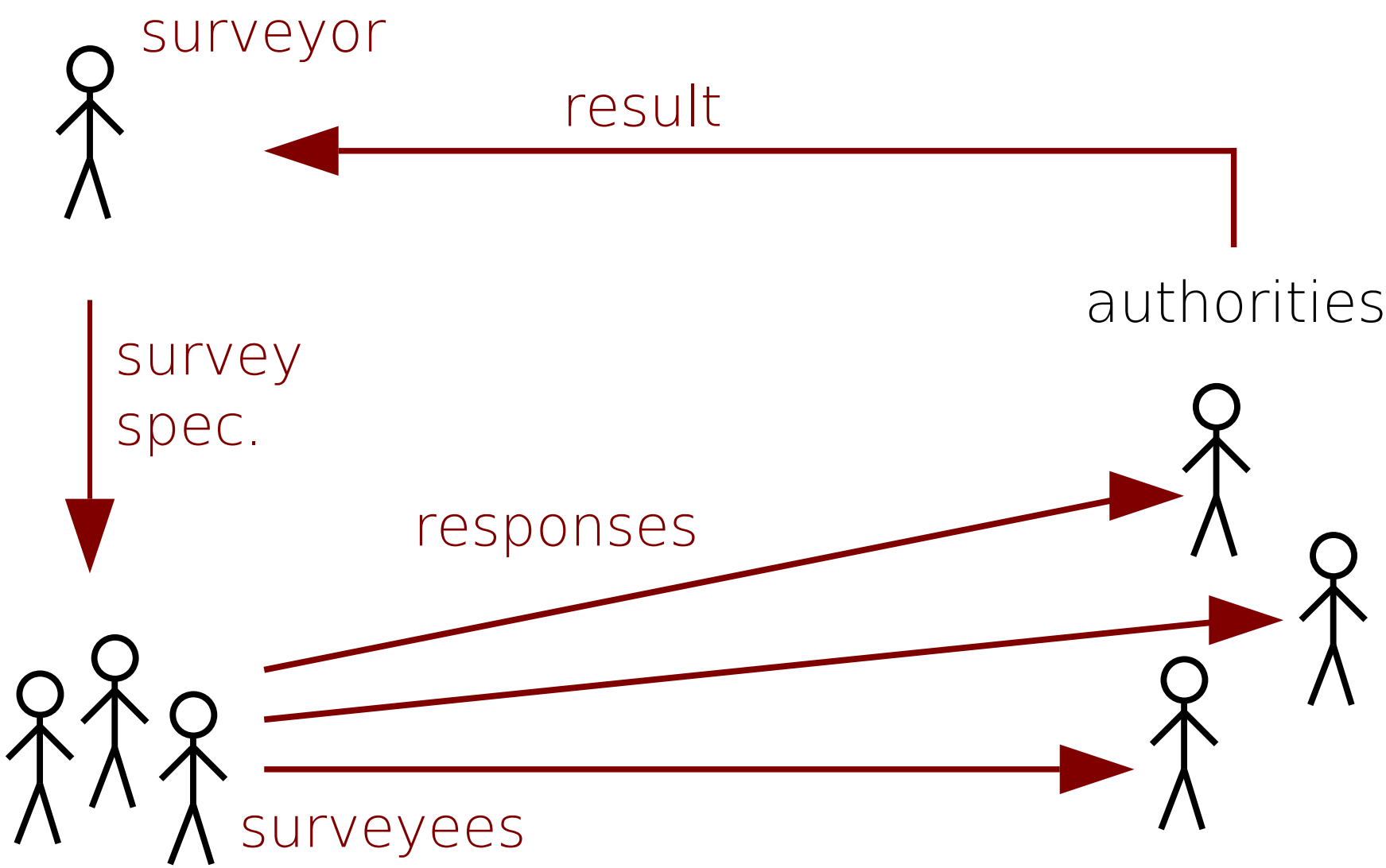
See also: [BNV13]

verifiability: n - 1

our surveys:

- no bulletin board
- no public verifiability

surveys


surveyor
result
authorities
survey
spec.
responses
surveyees

surveys

preprocessing, then very lightweight

mod-p arithmetic on 32/64-bit ints,
no modexp

privacy and verifiability:
up to n-1 dishonest authorities

Voting	Surveys
public verifiability	record privacy
mix-net, homomorphic	MPC
simple result functions	statistics, tables

More applications

political election

doodle poll

boardroom vote

national census

market research survey

lecture feedback

...