Electronic Voting: Scantegrity II

Anupam Datta
CMU

Voting

Verifiability

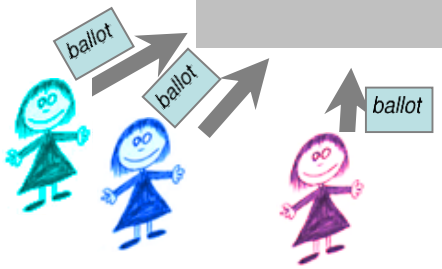
ballot

receipt

voting process

some additional data

Result



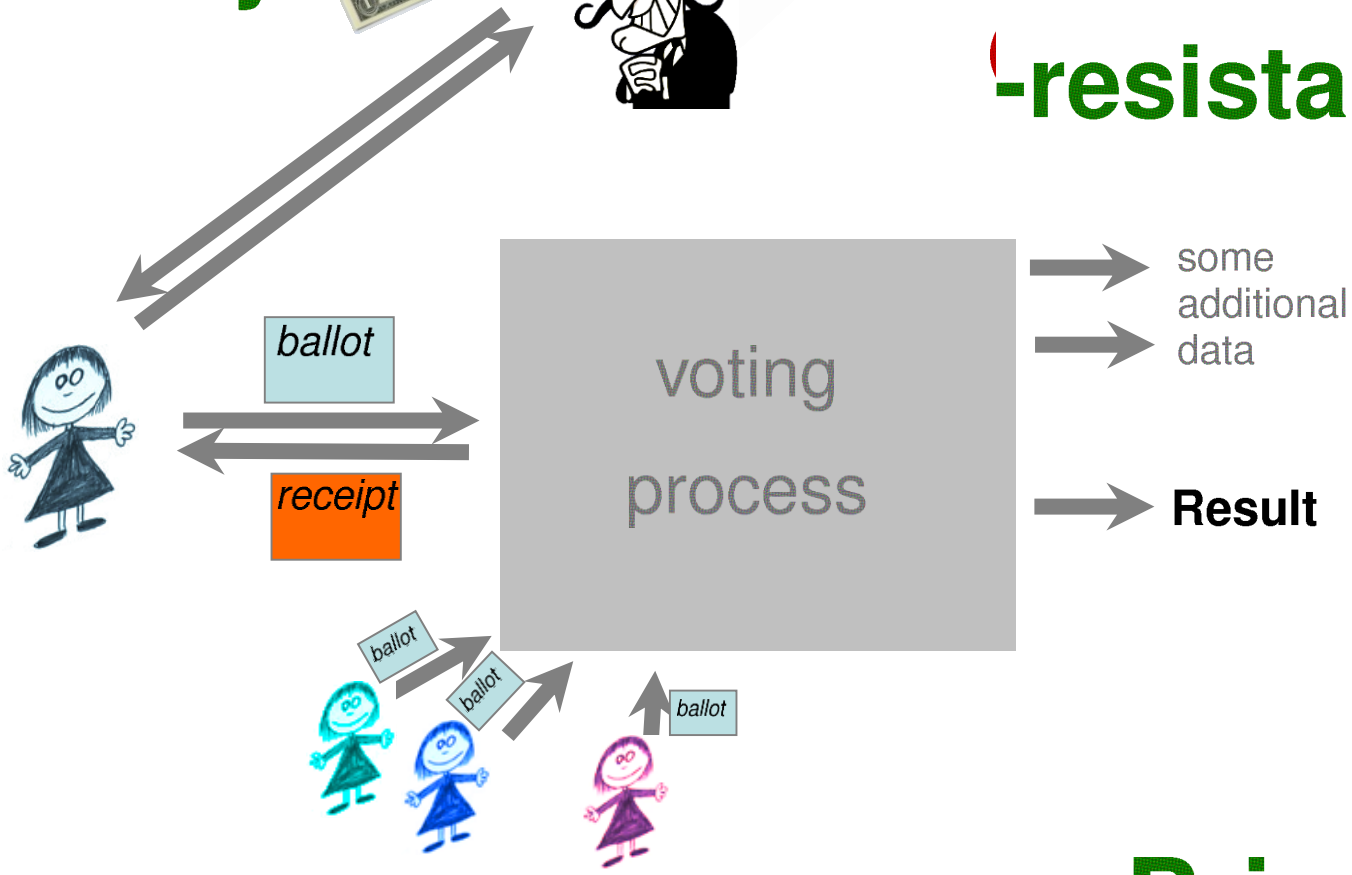
Privacy

Voting

Verifiability

v Coercion- !

-resistance

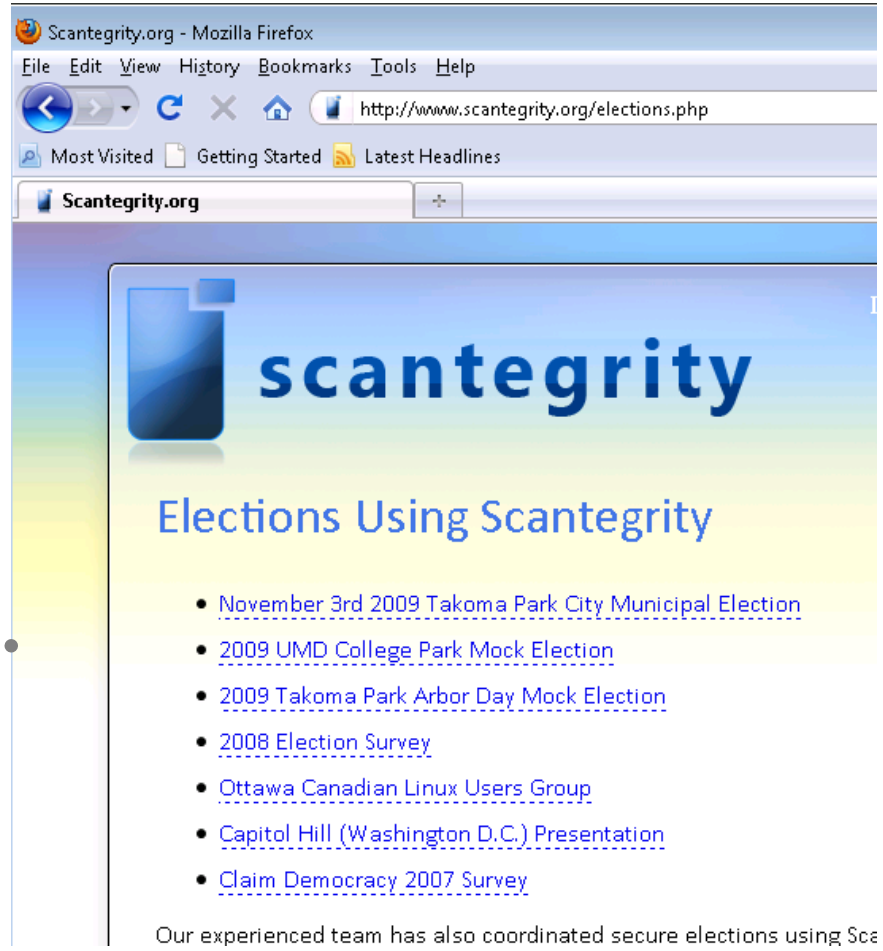


Privacy

Voting Protocols

Protocols achieving (various forms of) these properties:

- PunchScan
- ThreeBallot
- Bingo Voting
- Prêt-à-voter
- Civitas
- Scantegrity II



Outline of the Talk

- The Scantegrity II voting system
- Definition of Coercion-Resistance
- Coercion-Resistance of Scantegrity II

Goals

Security

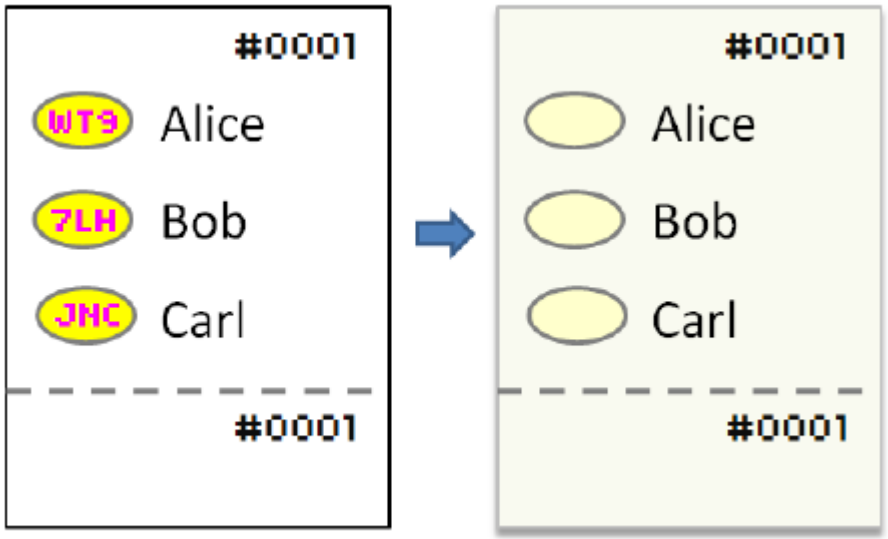
- End-to-end verifiability
- Coercion resistance
- Privacy
- Dispute resolution

Usability

- Compatibility with optical scan equipment
- Familiar ballot marking procedure

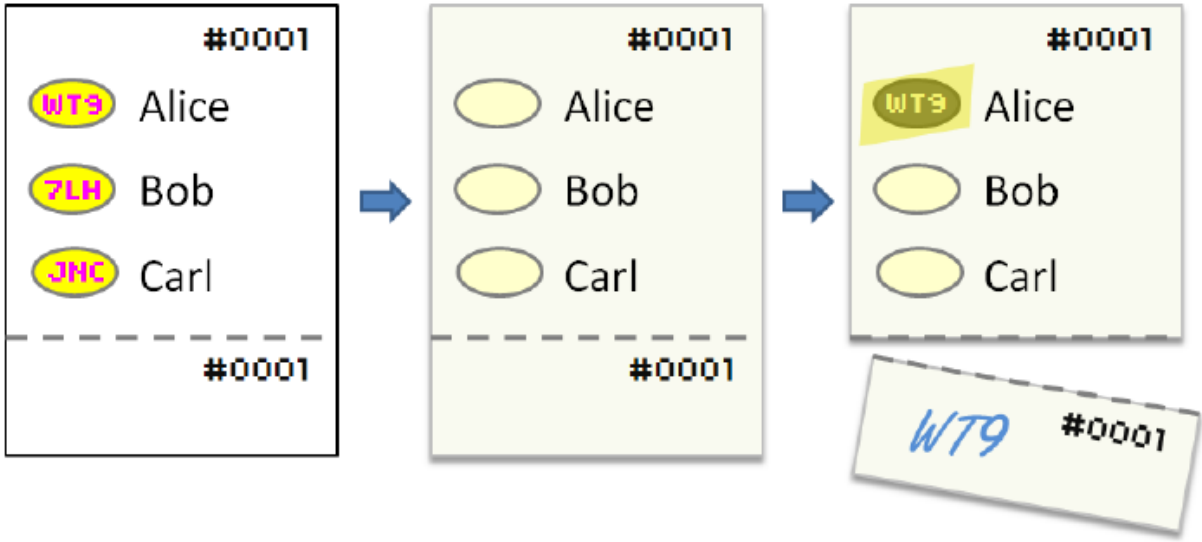
Ballot Creation

- Key step
  - Each ballot gets pseudorandom codes next to each candidate
  - **I**nvisible **I**nk: codes not initially visible to voter



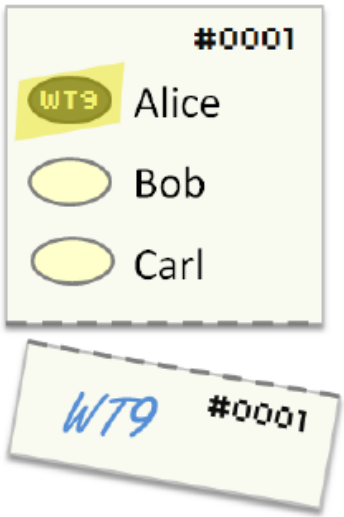
Voter Experience

1. Sign-in: to get decoder pen
2. Voting: by marking bubble with decoder pen
3. Create receipt: by manually transcribing revealed code and detaching receipt
   - Marked “Ballot Voted” by poll worker



Voter Experience (2)

4. Audit Ballot (optional): voter marks all bubbles and notes down all codes
   - Marked “Audit Ballot” by poll worker
   - Not included in result count
5. Post-Election Voter Verification
   - Check for ballot# that correct confirmation code is posted on election website
   - Challenge: How to enable verifiability while protecting coercion-resistance, privacy?



Scantegrity II - Initialization phase

officials

seed

workstation

PRNG

Q

1	$LL9$	$1A2$	$98F$
2	$WA4$	$X1P$	$BV6$
⋮	⋮	⋮	⋮

shuffled with random π_1

shuffled with random π_2

R

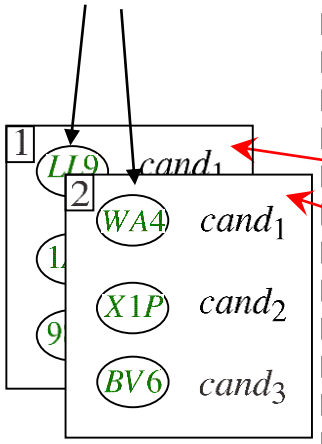
	Q-Pointer	S-Pointer

random correct pointers

Printer

Scanner

codes in invisible ink



P

	$cand_1$	$cand_2$	$cand_3$
1	$LL9$	$1A2$	$98F$
2	$WA4$	$X1P$	$BV6$
⋮	⋮	⋮	⋮

S

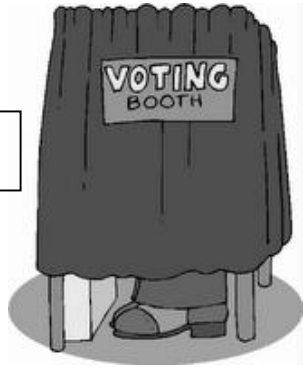
	$cand_1$	$cand_2$	$cand_3$
1			
2			
⋮			

public bulletin board

Commitments on Q, R-tables

Scantegrity II - Voting phase

notes id and code down

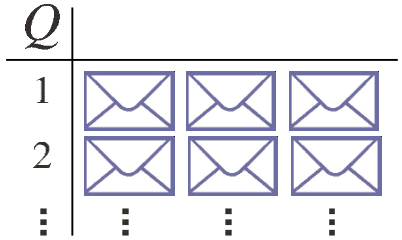


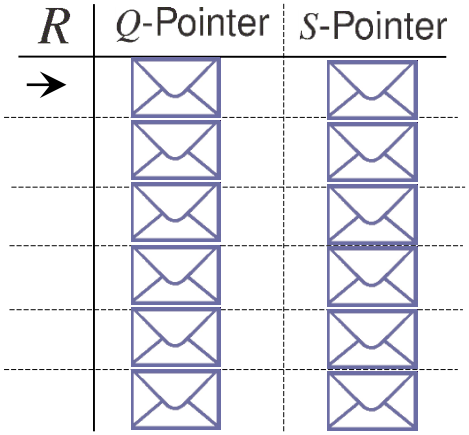
vote-ballot gets destroyed

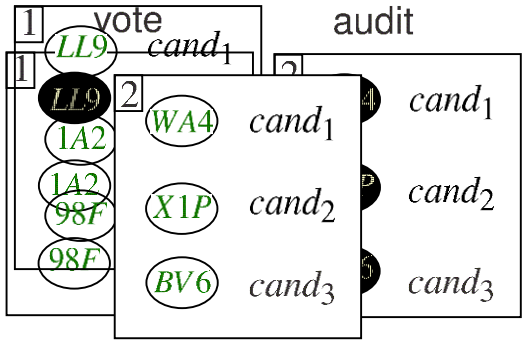
decoder pen

Workstation

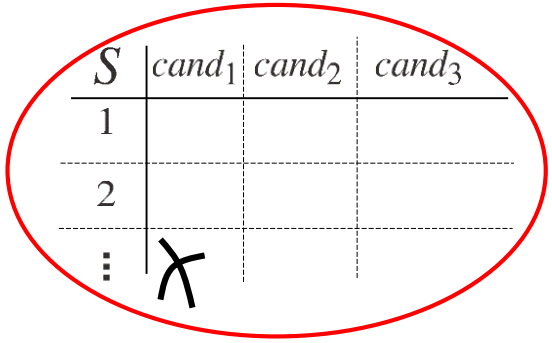
- for *vote*-ballot:
  - reveals code in Q-table
  - flags row in R-table
  - flags entry in S-table







result



makes codes visible
darkens paper
→ scanner can detect marked candidate (and ill-formed ballots)

Scantegrity II - Post-Voting phase

audit

2

WA4 $cand_1$

X1P $cand_2$

BV6 $cand_3$

Workstation

- for *vote*-ballot:
  - reveals code in Q-table
  - flags row in R-table
  - flags entry in S-table
  - opens either Q- or S-pointer (public coin flip)

complete link is not revealed

- for *audit*-ballot:

  opens all commitments

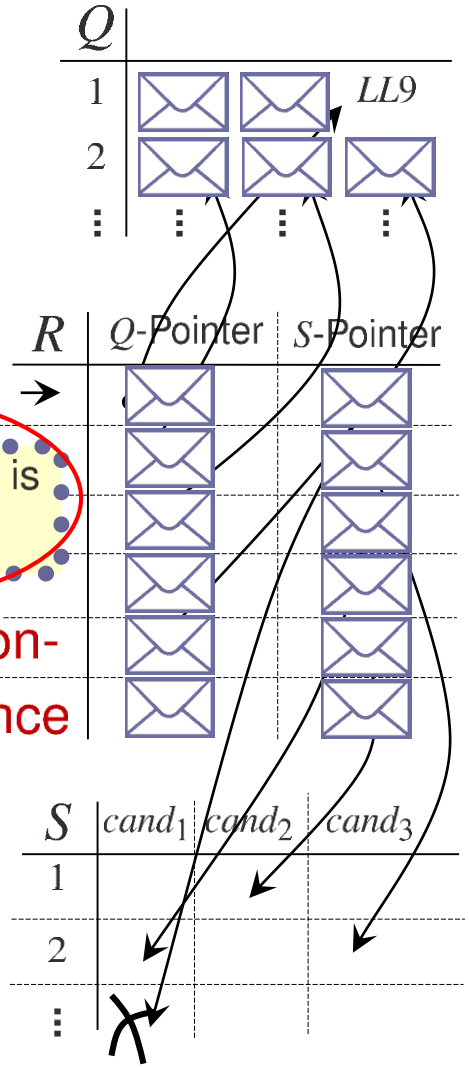
Coercion-resistance

guarantess that there is a link from $LL9$ to $cand_1$

guarantees that $code \mapsto candidate$ is correct

in particular: no link from $LL9$ to another candidate

Verifiability



Checking the Tally

- How can we audit the election tally?
  - Table S has counts for each candidate
  - Check flags mapped unchanged from table Q through R to S

Ballot ID			
0001		WT9	
0002	J3K		
0003		CH7	
0004	KWK	H7T	WJL
0005			LTM

Table **Q**

Flag	Q-Pointer	S-Pointer
		(2,1)
	(0003,3)	
✓		(4,3)
		(3,3)
✓	(0001,2)	
✓	(0005,3)	
	(0004,2)	(5,3)
		(2,3)
	(0004,3)	(3,1)
	(0002,3)	
	(0001,1)	
	(0002,2)	
	(0004,1)	(1,2)
✓		(5,1)
	(0005,2)	

Table **R**

Alice	Bob	Carl
	✓	
✓		✓
✓		

Table **S**

Checking the Tally (2)

- Use Table R:
  - For each row, randomly ask to open either Q- or S- pointer
  - Q-pointer connects a revealed code in table Q- to a flagged row of table R OR connects hidden code to unflagged row
  - Each revealed S-pointer either connects a flagged element in R to a flagged element in S or an unflagged element to an unflagged element

Checking Receipts

- How can a voter check that her vote was counted?
- Use Table Q:
  - Ballot id identifies row
  - Check confirmation code matches her receipt
  - If not, file a dispute

Dispute Resolution

- Voter claims confirmation code on her receipt does not match one in Table Q
- Step 1: Election officials can publicly open commitments to other codes on the voter's ballot; if they don't match claimed code eliminate dispute

Dispute Resolution (2)

- Step 2: Statistical trigger for deeper investigation

Example:

N = # candidates = 5

C = codespace = 8000

D = #disputes = 1000

p = prob of randomly guessing code = 0.0005

G = # of plausible discrepancies

E[G] = m = Dp = 0.5

Dispute Resolution (2)

Set trigger = t such that the prob of obtaining at least t plausible discrepancies if all filed disputes are random guesses is less than 1%

$Pr[G - m >= r] <= (em/r)^r$

Using r = 4.5: Pr[G>=5] <= 0.0046 <0.01

So set t = 5

If at least 5 out of the 1000 disputes filed are plausible discrepencies, then an investigation should be instigated

Possible Attacks + Defenses

- Adversary adds a mark to an empty cast ballot (i.e. voter abstained)
  - Voter can detect manipulation but has no proof that she abstained
  - Defense: Add a “None of the above” option
- Repeated confirmation codes on a ballot
  - Defense: Random half of ballots are audited; fraudulent ballots will be detected

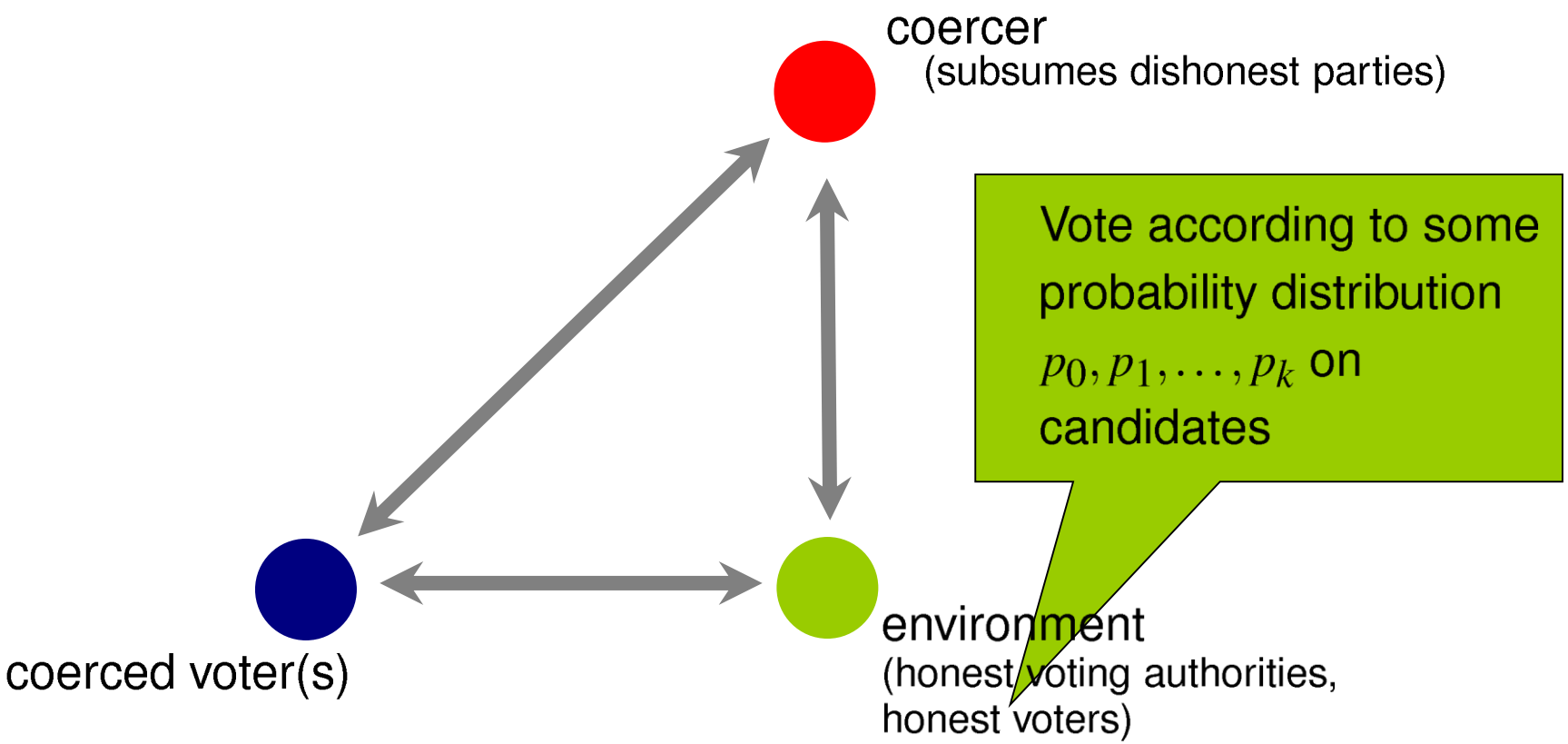
Possible Attacks + Defenses

- Adversary modifies vote tally by flipping flags in tables Q, R, S
  - Defense: Detected by randomized partial checking of Q- and S- pointers in R; probability that adversary modifies k pointers without being detected in $1/2^k$

Outline of the Talk

- The Scantegrity II voting system
- Definition of Coercion-Resistance
- Coercion-Resistance of Scantegrity II

KTV Definition: Voting Systems



Written: $(c||v||e)$

Formally, this is a system of Interactive Turing Machines (ITMs)

Coercion-Resistance: KTV Definition Intuition

Imagine that the coerced voter has a *goal* γ
(which she would try to achieve if she were not coerced)

a set of runs

For instance:

- the voter abstains from voting
- the voter votes for candidate C and this vote is counted

I want you to run the program v
(perform the actions v)

$\forall$ *coercion strategy* $v \in V$

$\exists$ *counter-strategy* $v' \in V$

- not to v[illegible]
- to vote for C
- to vote for a candid[illegible] mined dynamically
- to cast a ballot forme[illegible] tain way

I could run v' instead:
I would achieve my goal γ and
the coercer cannot distinguish
whether I run v or v'!

threat resistance

vote-selling resistance

Coercion-Resistance: KTV Definition

Formally: δ-Coercion-Resistance with respect t

$\forall$ *coercion strategy* $v \in V$ $\exists$ *counter-strategy* $v' \in$

(1) If the coerced voter runs v', she achieves he

$\forall\ c:\quad Prob(\ \text{run of } (c||v'||e) \text{ is in } \gamma\ )$ is

(2) The coercer can distinguish with probability one of v, v' the coerced voter ran:

$\forall\ c:\ |Prob((c||v||e) \to 1) - Prob((c||v'||e) \to 1)| \leq \delta + \text{negl.}$

$b \xleftarrow{R} \{0,1\}$
if $b = 1$ then
  $b' \leftarrow (c||v||e)$
else
  $b' \leftarrow (c||v'||e)$
If $b = b'$ then `success`
  else `fail`

`advantage` $\leq \delta$+negl.

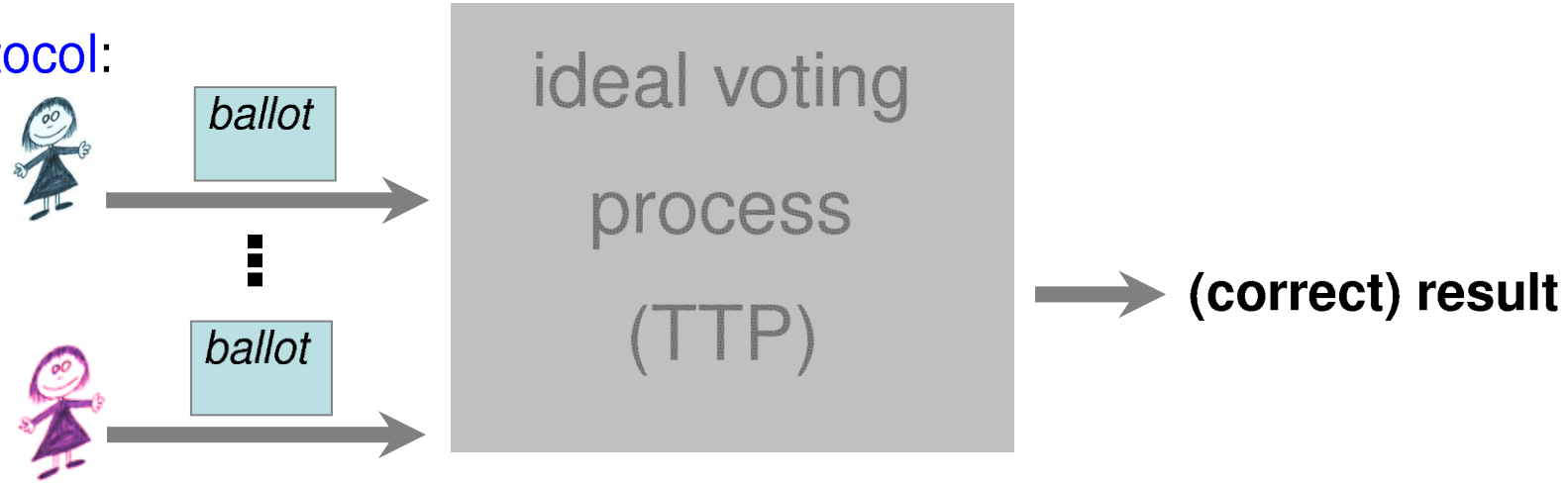
coercer thinks that coerced voter obeyed

Intuition behind δ:

- If I follow the instructions, the chance of getting paid is at most δ higher.
- If I do not follow the instructions (but achieve my goal), the chance of getting punished is at most δ higher.

Ideal Protocol

Ideal Protocol:



To what extent is it coercion-resistant?

Vote for *B!*

I just vote for *A!*

What happens if nobody votes for *B?*

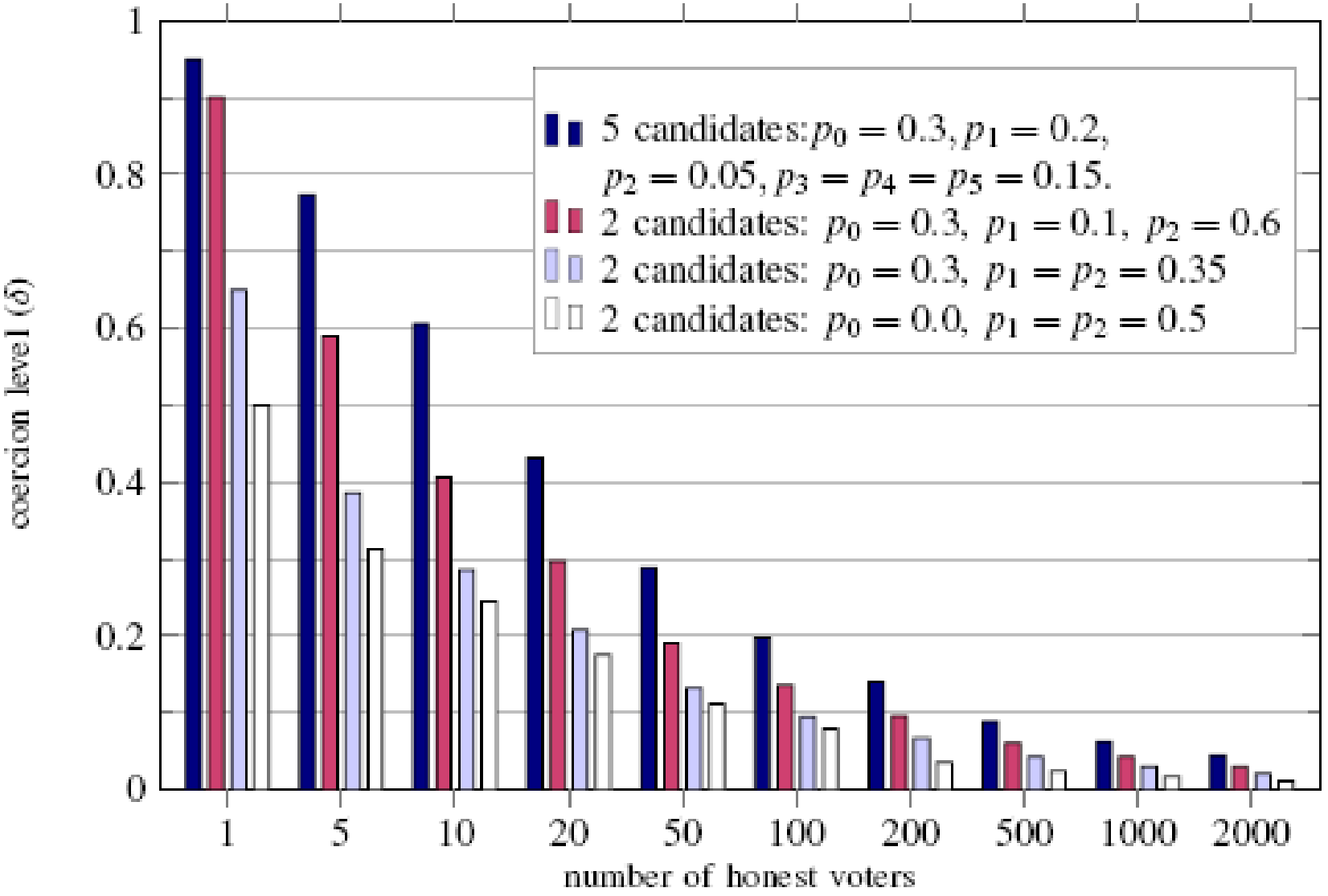
knows that

disobeyed

So, there is a certain probability for that.

$\Rightarrow \delta > 0$

Ideal Protocol: δ-Coercion-Resistance



Outline of the Talk

- Definition of Coercion-Resistance
- The Scantegrity II voting system
- Coercion-Resistance of Scantegrity II

Coercion-resistance of Scantegrity II

γ_i: the set of runs, where the coerced voter votes for candidate i if the coerced voter is instructed to vote

δ_{ideal}: as in the ideal protocol

Theorem:

Under the assumption that the workstation and one official are honest, Scantegrity II is δ_{ideal} coercion-resistant with respect to γ_i.

necessary

Proof:

Non-trivial, information theoretic reasoning that additional data (e.g., commitments on the tables, codes) does not help the coercer in distinguishing whether the coerced voter follows his strategy or not.

Coercion-Resistance Result

- Coercer gets receipts of all coerced voters
- Not resistant to forced abstention attacks
  - Unless “None of the above” is an option
- Not resistant if workstation is compromised
  - Need PRNG and scanner to be honest
- Not resistant unless at least one election official is honest
  - Secret sharing used to seed PRNG

Thank you!

- Thanks to Ralf Kuesters for providing a number of slides