Short Ballot Assumption and Threeballot Voting Protocol

Jacek Cichoń Mirosław Kutyłowski Bogdan Węglorz

Wrocław University of Technology

SOFSEM, Nový Smokovec, 2008

Voting
basic requirements

Design goals

1. low cost
2. easy for voters
3. easy to count
4. flexibility of voting options
5. no vote selling, no cheating

E-Voting
subfields of research

Subfields in e-voting:

- voting machines for polling stations
- remote voting with electronic devices
- novel paper-based methods

E-Voting
necessity

Why do we need e-voting:

- current procedures are not that secure as people believe,
- mobility of voters,
- postal voting enables vote selling,
- voters distrust authorities.

Traditional paper voting
threats

Some manipulation possibilities

1. put an additional mark to make a ballot invalid (Poland),
2. exchange ballots from a ballot box,
3. prevent a voter to come to the polling station.

Postal voting
threats

Postal voting

1. ballot in a sealed envelope, envelope in a second envelope
2. deadline for incoming ballots

Problems

1. destroying envelops from districts where the opponent has majority,
2. selling unfilled ballots.

Voting machines

threats

Voting machines

1. in a polling station: voting machines, no paper ballots filled,
2. advantage - fast and reliable vote counting.

Problems

1. trusted hardware & software?
2. costs (machines unused between elections,...).

Remote voting
threats

Remote voting

1. voting with electronic communication means (Internet, UMTS,...)
2. like postal voting but cheaper and more reliable (confirmations!)

Problems

1. insecure or unreliable devices,
2. (remote) vote selling,
3. voters can be under pressure.

Goals

protocols and improvements

New features

- changing protocol may increase security, efficiency, dependability,...
- examples:
  - local verifiability
    (I can check that MY ballot has been counted),
  - global verifiability
    (I can check overall counting process).

General Situation

Situation

1. no reliable solution so far,
2. implementations: dramatic situation as a rule!
3. electronic devices sometimes make more trouble than help.

General Situation

Situation

1. no reliable solution so far,
2. implementations: dramatic situation as a rule!
3. electronic devices sometimes make more trouble than help.

What to do?

1. rethink paper-based methods
2. design electronic methods that work even if everybody is dishonest

Three Ballot

Idea of Ronald Rivest

An empty ballot

Cichon	○	○	○
Kutylowski	○	○	○
Weglorz	○	○	○

Three Ballot

Idea of Ronald Rivest

A vote for Weglorz

Cichon	●	○	○
Kutylowski	○	○	●
Weglorz	○	●	●

Three Ballot

Idea of Ronald Rivest

A vote for Cichon

Cichon	●	○	●
Kutylowski	○	○	●
Weglorz	○	●	○

Three Ballot
Idea of Ronald Rivest

Cichoń, Kutyłowski, Węglorz

A vote for Kutylowski

Cichon	●	○	○
Kutylowski	○	●	●
Weglorz	○	●	○

Three Ballot

Idea of Ronald Rivest

A ballot with IDs

Cichon	○	○	○
Kutylowski	○	○	○
Weglorz	○	○	○
	7ds8fDSKCds9dsAs	Df88fDdssiDFs87DSs	y&stdtsydDydgstd7er

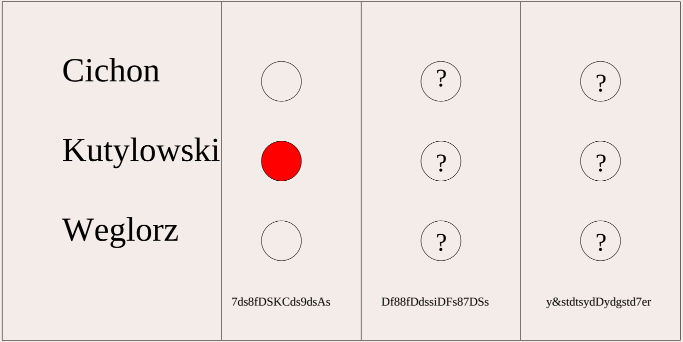
Three Ballot

voting procedure

Protocol steps

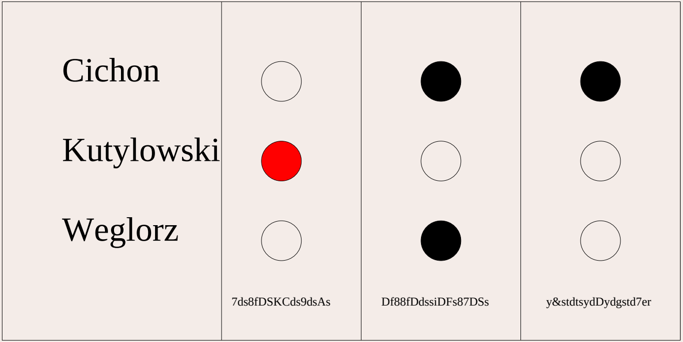
1. a voter fills one bubble in each row,
2. the voter fills one extra bubble in a row of his candidate,
3. the columns are separated,
4. **the voter takes copy of <u>one</u> chosen column**,
5. all three ballots are cast into the ballot box.

A receipt brings no information on a vote



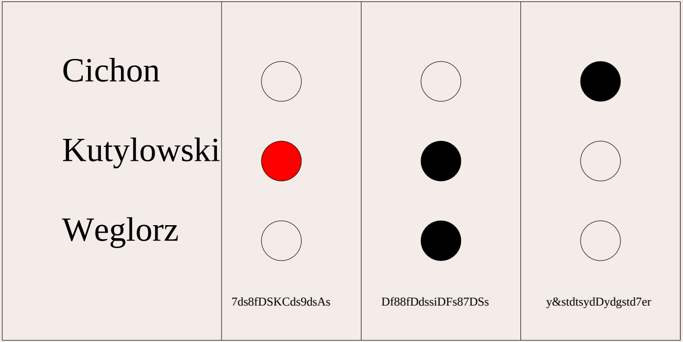
Three Ballot
receipt and vote-selling

A receipt brings no information on a vote



Three Ballot
receipt and vote-selling

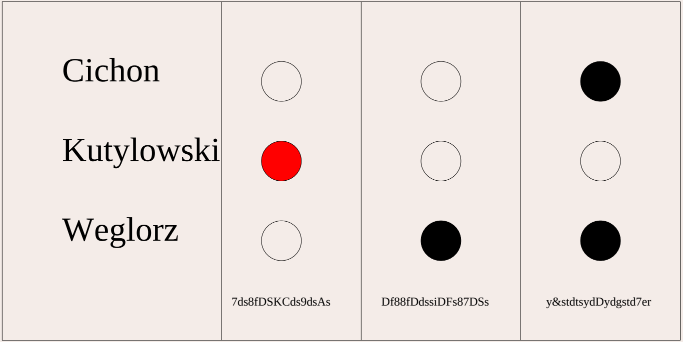
A receipt brings no information on a vote



Three Ballot

receipt and vote-selling

A receipt brings no information on a vote



Three Ballot
attack

The main idea

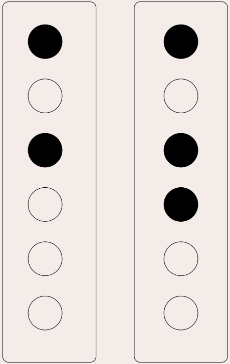
1. perfect security when a single receipt is concerned
2. ... but all ballots from the ballot box are published and knowledge on them can be used in an attack

Idea of the attack

1. given a ballot A which other ballots can be used to compose a valid 3-ballot with A?
2.
3.

Three Ballot
inconsistent ballots

Ballots that cannot originate from the same ballot



Three Ballot

attack, Charlie Strauss

Idea of the attack

1. given a ballot A which other ballots can be used to compose a valid 3-ballot with A?
2. **B is NOT from the same 3-ballot as A if more one row contain filled bubbles both in A and B**
3. if many rows (candidates in a contest), then it is **unlikely** that two random ballots are consistent in this sense.

Three Ballot
attack

Idea of the attack

1. find a receipt A such that there is only one candidate 3-ballot containing A

Three Ballot
attack

Idea of the attack

1. find a receipt A such that there is only one candidate 3-ballot containing A
2. remove the ballots of the 3-ballot found,
3. repeat

Three Ballot
Attack details

Question

- for how many candidates in a contest the scheme is still secure?
- for two candidates attack of this kind hopeless, for (say) 22 candidates almost always successful.

Short Ballot Assumption

Solution proposed- Short Ballot Assumption

The list of candidates on a ballot is short enough in order to guarantee security.

Problem

where is the boundary between secure Threeballot and insecure Threeballot?

Analytic results

summary

Results from the paper

- exact formula for probability that we can compose a valid 3-ballot from a receipt and 2 randomly chosen ballots from a ballot box.
- exact formula for the expected number of candidate 3-ballots

Remarks

asymptotic formulas are useless, we need concrete values for concrete parameter choices!

Three Ballot

Analytic results

Theorem

Let R be a receipt with a filled bubbles in k candidate race and N votes cast. If R contains a filled bubble in row x, then the expected number of non-incidental 3-ballots with a vote for x is at most

$$\frac{2^{k-a}}{3^{k-1}} \cdot \frac{k-a+2}{k} \cdot (N-1)$$

and the expected number of incidental 3-ballots with a vote for x is at most

$$\frac{2^{2k-4}}{3^{2k-2}} \cdot (4c_0 + 2c_1(k-a) - c_2(k-a)(k-a+1)) \cdot (N-1)(N-2) \ ,$$

where $c_0 = (1 + \frac{1}{2^{a+1}})^{\frac{4k-3a+3}{k}}$,
$c_1 = \frac{3(4k-3a+3)}{k^2} - \frac{3}{k}(1 + \frac{1}{2^{a+1}})$, $c_2 = \frac{9}{k^2}$.
If R does not contain a filled bubble in row x, then ...

Three Ballot
Analytic results

Upper estimation for the expected number of non-incidental 3-ballots for candidate x for a receipt R with a filled bubbles, when R does not contain a filled bubble in a row x, $N = 100$,

non-incidental = the ballots used come from the same 3-ballot

	$a = 1$	$a = 2$	$a = 3$	$a = 4$	$a = 5$	$a = 6$	$a = 7$
$k = 5$	1.96	.98	.49	.24	.12		
$k = 6$	1.08	.54	.27	.014	.068	.034	
$k = 7$	.62	.31	.16	.077	.039	.019	.0097

Three Ballot
Analytic results

Upper estimation for the expected number of incidental 3-ballots for candidate x for a receipt R with a filled bubbles, when R does not contain a filled bubble in a row x

	$a=1$	$a=2$	$a=3$	$a=4$	$a=5$	$a=6$	$a=7$
$N=100$							
$k=5$	1250	934	688	494	340		
$k=7$	248	199	160	127	100	76	57
$k=9$	49	41	34	29	24	20	16
$k=10$	22	18.6	15.9	13.6	11.6	9.87	8.27
$N=50$							
$k=7$	60	48	39	31	24	18	14
$k=9$	11.9	9.97	8.39	7.07	5.92	4.90	3.99

Two Candidates Run

assumptions, result

Situation considered

We consider the worst case - all but one voter votes for candidate $\mathcal{A}$, one vote for $\mathcal{B}$.

Goal: find who voted for $\mathcal{B}$ based on receipts and contents of the ballot box.

Two Candidates Run

assumptions, result

Situation considered

We consider the worst case - all but one voter votes for candidate $\mathcal{A}$, one vote for $\mathcal{B}$.

Goal: find who voted for $\mathcal{B}$ based on receipts and contents of the ballot box.

Theorem

Result: for arbitrary receipts X, Y:
for a valid assignment of ballots to voters in which a voter with receipt X casts a vote for $\mathcal{B}$, we can find another solution in which a voter with receipt Y casts a vote for $\mathcal{B}$.

Two Candidates Run

assumptions, result

Situation considered

We consider the worst case - all but one voter votes for candidate $\mathcal{A}$, one vote for $\mathcal{B}$.

Goal: find who voted for $\mathcal{B}$ based on receipts and contents of the ballot box.

Theorem

Result: for arbitrary receipts X, Y:
for a valid assignment of ballots to voters in which a voter with receipt X casts a vote for $\mathcal{B}$, we can find another solution in which a voter with receipt Y casts a vote for $\mathcal{B}$.

Corollary

Three-Ballot scheme for 2-candidate run is safe provided that the number of voters is not very close to 1.

Two Candidates Run
configurations

Proof idea

If person $\mathcal{P}$ has voted for candidate $\mathcal{A}$. Then:

- If $\mathcal{P}$ holds a receipt $\frac{\bullet}{\bullet}$,
  then his other ballots must be $\frac{\bullet}{\circ}$ and $\frac{\circ}{\circ}$.
- If $\mathcal{P}$ holds $\frac{\bullet}{\circ}$,
  then his other ballots must be either $\frac{\circ}{\bullet}$, $\frac{\bullet}{\circ}$, or $\frac{\bullet}{\bullet}$, $\frac{\circ}{\circ}$.
- If $\mathcal{P}$ holds a receipt $\frac{\circ}{\bullet}$,
  then his other ballots must be $\frac{\bullet}{\circ}$, $\frac{\bullet}{\circ}$.
- If $\mathcal{P}$ holds a receipt $\frac{\circ}{\circ}$,
  then his other ballots must be $\frac{\bullet}{\bullet}$, $\frac{\bullet}{\circ}$.

.

Transformation

step 1

Alice used $\frac{\circ}{\bullet}$, $\frac{\bullet}{\bullet}$, $\frac{\circ}{\circ}$, where $\frac{\circ}{\bullet}$ is the receipt

Step 1: replace the ballots of Alice by $\frac{\circ}{\bullet}$, $\frac{\bullet}{\circ}$, $\frac{\bullet}{\circ}$.

deficit of ballots $\frac{\bullet}{\circ}$, $\frac{\bullet}{\circ}$

surplus of ballots $\frac{\bullet}{\bullet}$, $\frac{\circ}{\circ}$ not linked to any voter.

nobody voting for $\mathcal{B}$.

Transformation
step 2

Transformations

Situation deficit of ballots $\frac{\bullet}{\circ}$, $\frac{\bullet}{\circ}$
surplus of ballots $\frac{\bullet}{\bullet}$, $\frac{\circ}{\circ}$ not linked to any voter.
nobody voting for $\mathcal{B}$.

Step 2: find a voter with ballot $\frac{\bullet}{\circ}$, $\frac{\bullet}{\circ}$, $\frac{\circ}{\bullet}$ (with receipt $\frac{\bullet}{\circ}$).
change his choice to $\frac{\bullet}{\circ}$, $\frac{\bullet}{\bullet}$, $\frac{\circ}{\circ}$.

Situation deficit of ballot $\frac{\bullet}{\circ}$
surplus of ballots $\frac{\circ}{\bullet}$, not linked to any voter.
nobody voting for $\mathcal{B}$.

Transformation

step 3

Transformations

Step 2: deficit of ballot $\genfrac{}{}{0pt}{}{\bullet}{\circ}$
surplus of ballot $\genfrac{}{}{0pt}{}{\circ}{\bullet}$, not linked to any voter.
nobody voting for $\mathcal{B}$.

Step 3A: find a voter $\mathcal{X}$ with vote $(\genfrac{}{}{0pt}{}{\circ}{\circ}; \genfrac{}{}{0pt}{}{\bullet}{\bullet}, \genfrac{}{}{0pt}{}{\bullet}{\circ})$
with receipt $\genfrac{}{}{0pt}{}{\circ}{\circ}$
and change it to $(\genfrac{}{}{0pt}{}{\circ}{\circ}; \genfrac{}{}{0pt}{}{\bullet}{\bullet}, \genfrac{}{}{0pt}{}{\circ}{\bullet})$.

no deficit and no surplus of ballots,
$\mathcal{X}$ votes for $\mathcal{B}$.

Conclusions

Short Ballot Assumption

Situation

1. 2 candidates runs - ok,

Conclusions

Short Ballot Assumption

Situation

1. 2 candidates runs - ok,
2. it can be generalized to 3, 4, ... candidates, but the number of voters must grow exponentially

Conclusions

Short Ballot Assumption

Situation

1. 2 candidates runs - ok,
2. it can be generalized to 3, 4, ... candidates, but the number of voters must grow exponentially
3. for 9 candidates it is becoming risky

Conclusions
Short Ballot Assumption

Situation

1. 2 candidates runs - ok,
2. it can be generalized to 3, 4, ... candidates, but the number of voters must grow exponentially
3. for 9 candidates it is becoming risky
4. for 13 candidates very risky

Open problem

Where is the bound exactly (no reconstruction possible with high probability)?

Thanks for your attention!