Scratch, Click & Vote

Mirosław Kutyłowski, Filip Zagórski

Institute of Mathematics and Computer Science
Wroclaw University of Technology, Poland

Ministry of Interior and Admministration of Poland

IACR Voting System Session
Santa Barbara, CA, 19 VIII 2008

Scratch, Click & Vote

- Miroslaw Kutylowski, Filip Zagorski
  Scratch, Click & Vote: E2E voting over the Internet
  `http://eprint.iacr.org/2008/314`

Scratch, Click & Vote – properties

- verifiable hybrid voting scheme (ballots are sent to voters, voting over the Internet)
- voter's computer is not trusted
- PC does not learn voter's choice
- PC cannot change voter's choice even into a random one (virus immunity)
- receipt obtained by a voter does not prove voter's choice

Scratch, Click & Vote – idea

- backend of the scheme is based on Punchscan and ThreeBallot ballot ideas – assures veryfiability
- frontend – assures immunity against evil PC
- there are two authorities in the system:
  - **Election Authority** responsible for voting cards preparation,
  - **Proxy** prepares coding cards, Proxy is “a virtual ballot box”

Terminology

- *voting card* – sheet of paper which a voter obtains from the Election Authority
- *ballot* – part of a filled up *voting card* which is cast by a voter
- example: ThreeBallot – voting card consists of three ballots

PS, PaV, STG, STG II

receipt	scanner/ballot box	bulletin board	partially decoded	results
		x	y	c
		x	y	c
		x	y	c
		x	y	c
R	R	x	y	c
		x	y	c
		x	y	c
		x	y	c
		R	y	c

- similar backends are used in Punchscan (PS), Pret a Voter (PaV), Scantergrity (STG), Scantegrity II (STG II)

PS, PaV, STG, STG II

receipt	scanner/ballot box	bulletin board	partially decoded	results
		x	y	c
		x	y	c
		x	y	c
		x	y	c
R	R	x	y	c
		x	y	c
		x	y	c
		x	y	c
		R	y	c

- verifiability step 1: voter checks if her receipt R appears on the bulletin board (Punchboard)

PS, PaV, STG, STG II

receipt	scanner/ballot box	bulletin board	partially decoded	results
		x	y	c
		x	$d_1(R)$	c
		x	y	c
		x	y	c
R	R	x	y	c
		x	B	c
		x	y	c
		x	y	$d_2(B)$
		R	y	c

- veryfiability step 2: veryfication of decoding is performed (post-election Audit)

ThreeBallot, VAV

receipt scanner/ballot box bulletin board = results

R/S/T

- Alice obtains voting card which contains three ballots R, S, T

ThreeBallot, VAV

receipt	scanner/ballot box	bulletin board = results
R/S/T	R & S & T	

- Alice cast a vote - tripple R, S, T, takes a receipt – one ballot: $R/S/T$

ThreeBallot, VAV

receipt	scanner/ballot box	bulletin board = results
		x
		T
		x
		x
R/S/T	R & S & T	x
		x
		S
		x
		R

- EA does not know which one; EA has to publish all of them among other ballots

ThreeBallot, VAV

receipt	scanner/ballot box	bulletin board = results
		x
		T
		x
		x
T	R & S & T	x
		x
		x
		x
		x

- Alice checks if her ballot appears on the bulletin board

Scratch, Click & Vote

receipt	Proxy	bulletin board	partially decoded	results
		x	y	c
		T	y	c
		x	y	c
		U	y	c
R/S/T/U	R & S & T & U	x	y	c
		x	y	c
		S	y	c
		x	y	c
		R	y	c

Scratch, Click & Vote

receipt	Proxy	bulletin board	partially decoded	results
		x	y	c
		T	y	c
		x	y	c
		U	y	c
R/S/T/U	R & S & T & U	x	y	c
		x	y	c
		S	y	c
		x	y	c
		R	y	c

- SCV – simple merge of Punchscan and ThreeBallot backends... but SCV is remote voting, we need different ballot layout.

Voter vs PC part I

- If a machine has the same knowledge as a voter:
  - machine knows exactly how voter voted
  - machine can change voter's choice (in some schemes)
  - online vote selling possible
  - virus attacks possible
- Solution: voter obtains additional information by an independent channel – "voting card" (paper is back?!) prepared by an Election Authority

Voter vs PC part II

- Machine cannot change voter's choice – voter obtains a receipt, which can be used to detect machine's misbehaviour.
- But at the same time, "voting card" and a receipt cannot be used to prove voter's choice
- Achieving these two properties is the hardest part in the system design.

Voter vs Election Authority

- Voter obtains voting card (ballot) from Election Authority
- How does voter know if her voting card is correctly encoded? Pre-election Audit
- How can one protect voter's privacy?
  Use ballot box votes are casted through Proxy

Coding card

- Voter obtains a *voting card* from Election Authority
- Voter obtains many *coding cards* from "Proxy" (many Proxies may be used)
- Voter lays them side by side

Candidate	*R*	*S*	*T*	*U*
2 Jerry				
3 Edgar				
0 Ervin				
1 Donald				
S_l				

voting card (from EA)

	n	Y	n	n
	n	Y	n	n
	Y	n	n	n
	n	n	n	Y
	S_r			

coding card (from Proxy)

Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

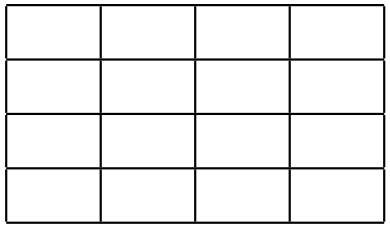
Vote casting

- Voter clicks on the screen on boxes which correspond to `Y` next to her candidate
-

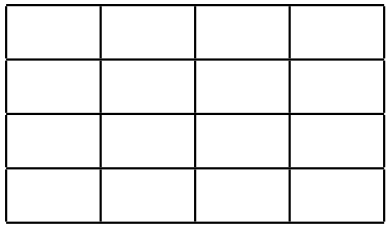
voting card

Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

PC screen



tranform (by Proxy)



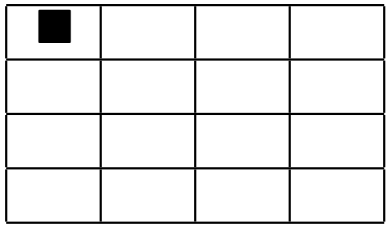
Vote casting

- Voter clicks on the screen on boxes which correspond to `Y` next to her candidate
-

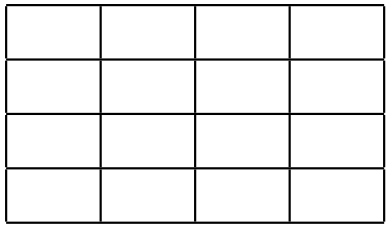
voting card

Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

PC screen



tranform (by Proxy)



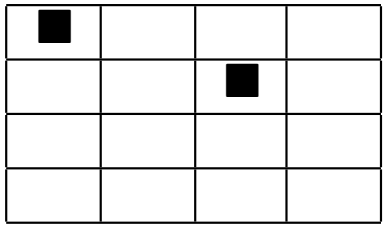
Vote casting

- Voter clicks on the screen on boxes which correspond to `Y` next to her candidate
-

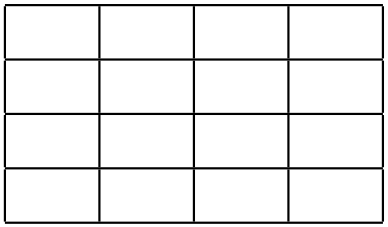
voting card

Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

PC screen



tranform (by Proxy)



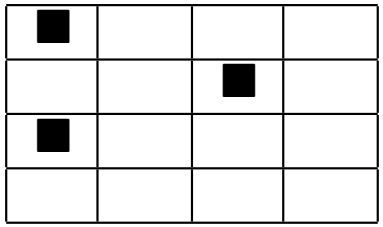
Vote casting

- Voter clicks on the screen on boxes which correspond to `Y` next to her candidate
-

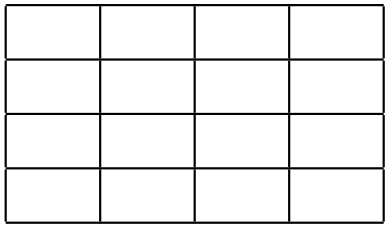
voting card

Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

PC screen



tranform (by Proxy)



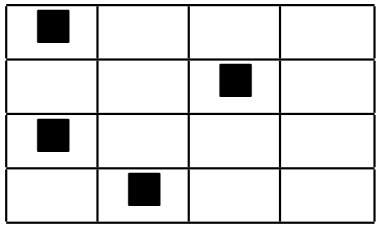
Vote casting

- Voter clicks on the screen on boxes which correspond to `Y` next to her candidate
-

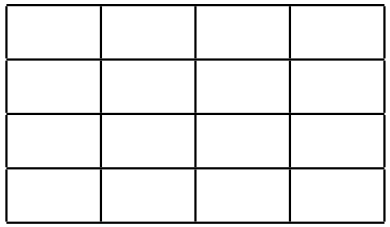
voting card

Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

PC screen



tranform (by Proxy)



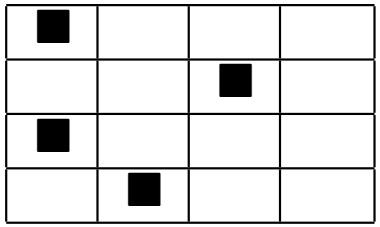
Vote casting

- Voter enters S_r (coding card serial number), proxy "translates" voter's choice into FourBallot form
-

voting card

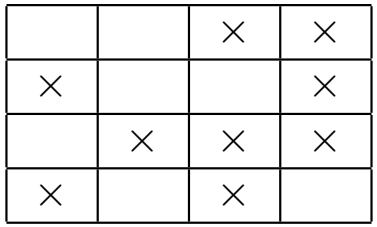
Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

PC screen



S_r

tranform (by Proxy)



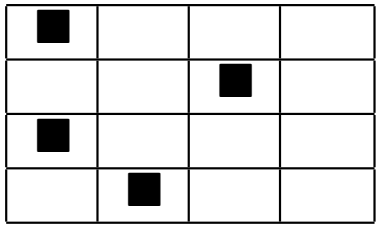
Vote casting

- Voter enters S_l (voting card serial number), Proxy sends FourBallot form to the Election Authority
-

voting card

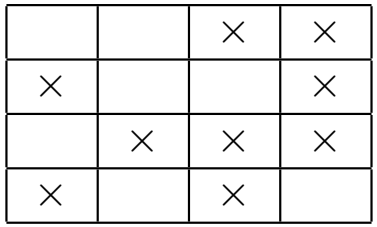
Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

PC screen



S_r

tranform (by Proxy)



S_l

Vote casting

- Voter obtains as a receipt one of the FourBallot form ballots (oblivious transfer like protocol used)

voting card

Candidate	*R*	*S*	*T*	*U*
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			

tranform (by Proxy)

		×	×
×			×
	×	×	×
×		×	

S_l

receipt

T
×
×
×

t

- $t = sign_{EA}(T, S_l)$ - confirmation token (like in Sure Vote)

Security - PC/virus

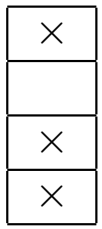
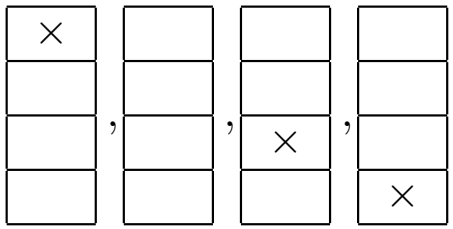
- Voter's PC can change voter's choice (with some probability):
  - PC does not know which row corresponds to the chosen candidate
  - modification can be detected by Proxy – $\frac{1}{3k}$, where k is the number of candidates
  - modification can be detected by voter – receipt ($\frac{1}{4}$)

Security - Proxy, Election Authority

- Proxy can change voter's choice into a random one, but then a receipt will change - detection with probability $\frac{1}{4}$
- Election Authority – neglible probability: Pre- and Post-election audits

Security - other attacks

- There are known attacks on ThreeBallot (Strauss, Appeal):
  - FourBallots is much more immune – better probability distribution – Strauss' attack ineficient
  - moreover, it is easy to implement following modification (only electronic version) – instead of publishing every ballot, every ballot is split into masked ballots:

a ballot column:  , masked ballot columns: 

- Thank you for your attention