

# Remotegrity

David Chaum, Jeremy Clark, Aleks Essex,  
Ronald Rivest, Allan Sherman, Poorvi Vora,  
Filip Zagorski

Crypto 2011  
rump session  
August 16, 2011

- The City of Takoma Park, MD, 2009 Municipal Election
- First voter verifiable system used to elect government officials





- We plan to use Scantegrity II again.
- We hope to introduce two innovations in the 2011 election:
  - ① Audiotegrity - audio voting for voters with vision disabilities.
  - ② Remotegrity - mailed form enabled online voting.

# Audiotegrity



- Voters make selection by navigating audio ballots
- Result is a printed Scantegrity paper ballot
- Voters receive printed receipts that they can check online

# Remotegrity - design goals

A method for remote voting based on ballots mailed to voters and cast over the Internet that provides strong protection against:

- client-side malware,
- malfeasance by election officials,
- attacks over the Internet (but not DDOS).

# Election package mailed to voters

FAVORITE MUSICIAN FROM "THE BEATLES"			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1st choice 1ra opción	2nd choice 2da opción	3rd choice 3ra opción
John Lennon	<input type="text" value="580"/>	<input type="text" value="667"/>	<input type="text" value="571"/>
Paul McCartney	<input type="text" value="918"/>	<input type="text" value="970"/>	<input type="text" value="999"/>
<input type="text"/>	<input type="text" value="984"/>	<input type="text" value="862"/>	<input type="text" value="944"/>
Write -In Candidate/ Para añadir a un candidato			

- Scantegrity I ballot
- Authentication card
- Inner return envelope
- Outer postal return envelope

Internet Confirmation Option		
Using this card, you can make extra sure that your votes are in fact posted correctly—by posting them online. All you need do is go to the election website <a href="http://takomapark.org/votemove">takomapark.org/votemove</a> and follow the instructions there for entering your codes, but make sure the site displays this unique number: <b>89AB920CD99</b> (otherwise call the registrar).	<input type="text" value="One-Use-Password #1"/>	<input type="text" value="Lock-In (choose one at random)"/>
The "One-Use-Passwords" on this card to the right, (protected by scratch-off) allow you to post confirmation numbers from your ballot on the website. Even if your ballot were to be lost in the mail, by posting these numbers you ensure that your vote is recorded correctly.	<input type="text" value="One-Use-Password #2"/>	<input type="text" value="Lock-In (choose one at random)"/>
	<input type="text" value="One-Use-Password #3"/>	<b>For auditor use only</b>
If you wish to go even farther, and "audit" the posting of votes by other voters, you can access the website from another computer and use the "Lock-In" codes provided in the rightmost column of this card.	<input type="text" value="One-Use-Password #4"/>	<b>For official use only</b>

# Authentication card properties

- Malware cannot cast ballot for a voter
- **New:** Election authorities cannot cast ballot for a voter (the voter choice of scratch-off is a kind of oblivious transfer)
- **New:** Voter has a physical proof in case of malfeasance

Internet Confirmation Option		
Using this card, you can make extra sure that your votes are in fact posted correctly—by posting them online. All you need do is go to the election website <a href="http://takomopark.org/remotevote">takomopark.org/remotevote</a> and follow the instructions there for entering your codes, but make sure the site displays this unique number: <b>89AB920CD99</b> (otherwise call the registrar).	<input type="text"/>	<input type="text"/>
	One-Use-Password #1	Lock-In (choose one at random)
The "One-Use-Passwords" on this card to the right, (protected by scratch-off) allow you to post confirmation numbers from your ballot on the website. Even if your ballot were to be lost in the mail, by posting these numbers you ensure that your vote is recorded correctly.	<input type="text"/>	<input type="text"/>
	One-Use-Password #2	Lock-In (choose one at random)
If you wish to go even farther, and "audit" the posting of votes by other voters, you can access the website from another computer and use the "Lock-In" codes provided in the rightmost column of this card.	<input type="text"/>	<i>For auditor use only</i>
	One-Use-Password #3	
	<input type="text"/>	<i>For official use only</i>
	One-Use-Password #4	



# Ballot properties (Scantegrity I)

FAVORITE MUSICIAN FROM "THE BEATLES"			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1st choice 1ra opción	2nd choice 2da opción	3rd choice 3ra opción
John Lennon	<input type="text" value="580"/>	<input type="text" value="867"/>	<input type="text" value="571"/>
Paul McCartney	<input type="text" value="918"/>	<input type="text" value="970"/>	<input type="text" value="999"/>
<input type="text"/>	<input type="text" value="984"/>	<input type="text" value="862"/>	<input type="text" value="944"/>

Scantegrity I ballot

- Computer does not learn voter's choice
- Computer cannot modify voter's choice
- Voter can check if her vote is included in a tally

- Scantegrity.org :: Blog :: Remotegrity FAQ  
[https://scantegrity.org/wiki/index.php/  
Remotegrity\\_Frequently\\_Asked\\_Questions](https://scantegrity.org/wiki/index.php/Remotegrity_Frequently_Asked_Questions)