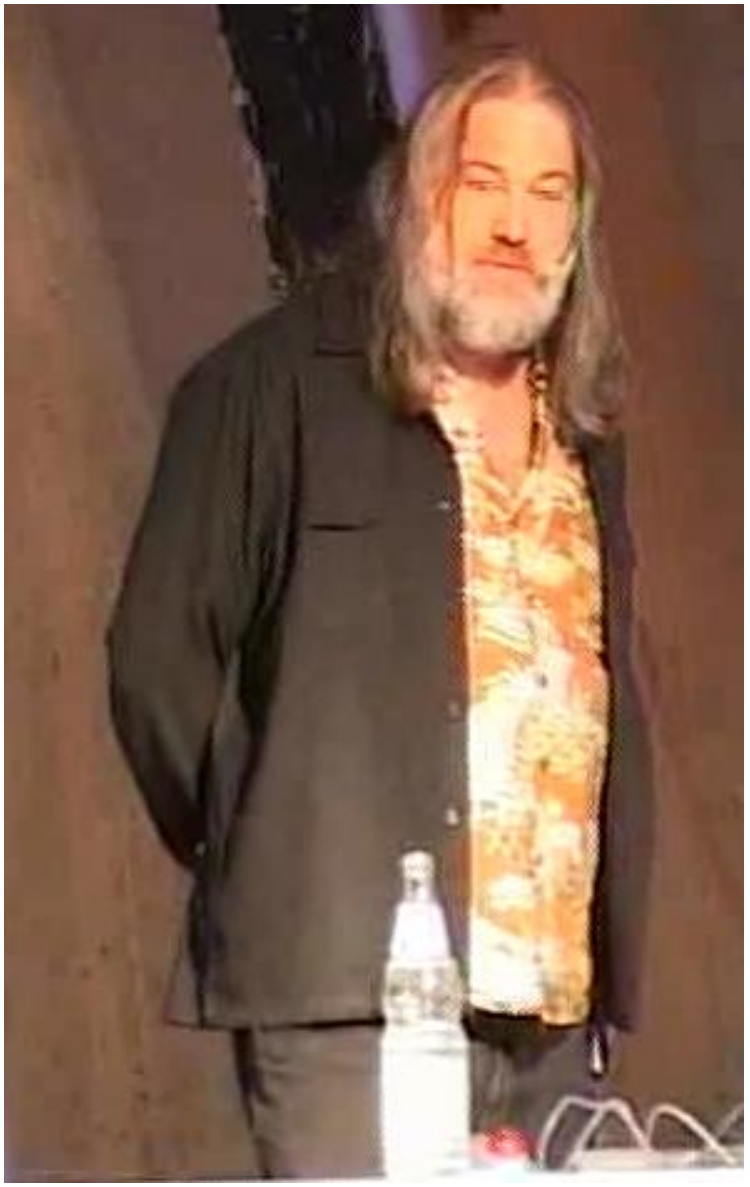
# Scantegrity

Ein System für verifizierbares eVoting

# David Chaums Mission

- “Let's make this really secure democracy stuff happen, because it's the only way we can really protect our world”



# Ablauf des Vortrags

- Güterabwägung bei Wahlen
- Hintergrund: Scan-Voting
- Scantegrity: Funktion
- Probleme / Fazit
- Quellen

# Güterabwägung

- Nachvollziehbarkeit vs. Geheimhaltung
- “integrity” vs. “secrecy”
- Überprüfung der individuellen Stimme

  vs.

  Nachzählung
- Angst vor Wahlfälschung

  vs.

  Angst vor Zwang und Stimmenkauf

# Vereinfachung

N=2 ( Zwei Kandidaten )

Nur ein Anliegen pro Wahl

Keine Mehrfachwahl

# Scan-Voting

- Stimmzettel wird gescannt und ausgewertet
- mark-sense vs. pixel-based
- precinct-read vs. zentrale Auszählung


# Scantegrity – Prinzipien

- Audit-Verfahren für Scan-Wahlsysteme
- End-to-End-Verifizierbarkeit (e2e): Wähler kann Korrektheit seiner Stimme verifizieren
- einfach in bestehende (Scan-) Wahlsysteme integrierbar
- Integrität **und** Geheimhaltung durch Prüflettern

# Elemente von Scantegrity

- Stimmzettel
  - Prüflettern
  - Seriennummer (Abriss)
  - Kandidatennamen
- Ergebnistabelle (Bulletin Board)
  - Zuordnung Seriennummer ⇒ Prüflettern ⇒ Ergebnis
  - Umschläge (papiern oder digital)

# SAMPLE OFFICIAL BALLOT
## GENERAL ELECTION
## POLK COUNTY, FLORIDA
NOVEMBER 7, 2000

## PRESIDENTIAL

### ELECTORS FOR PRESIDENT AND VICE PRESIDENT

(A vote for the candidates will actually be a vote for their electors.)

(Vote for One Group)

**REPUBLICAN**
GEORGE W. BUSH
DICK CHENEY

**DEMOCRATIC**
AL GORE
JOE LIEBERMAN

**LIBERTARIAN**
HARRY BROWNE
ART OLIVER

**GREEN**
RALPH NADER
WINONA LaDUKE

**SOCIALIST WORKERS**
JAMES HARRIS
MARGARET TROWE

**NATURAL LAW**
JOHN HAGELIN
NAT GOLDHABER

**REFORM**
PAT BUCHANAN
EZOLA FOSTER

**SOCIALIST**
DAVID McREYNOLDS
MARY CAL HOLLIS

**CONSTITUTION**
HOWARD PHILLIPS
J. CURTIS FRAZIER

**WORKERS WORLD**
MONICA MOOREHEAD
GLORIA LA RIVA

Write-in For President/Vice President

## CONGRESSIONAL

### UNITED STATES SENATOR
(Vote For One)

- BILL McCOLLUM — REP
- BILL NELSON — DEM
- JOE SIMONETTA — LAW
- JOEL DECKARD — REF
- WILLIE LOGAN — NPA
- ANDY MARTIN — NPA
- DARRELL L. McCORMICK — NPA

Write-in

### REPRESENTATIVE IN CONGRESS 15TH CONGRESSIONAL DIST.
(Vote For One)

- DAVE WELDON — REP
- PATSY ANN KURTH — DEM
- GERRY L. NEWBY — NPA

Write-in

## STATE

### TREASURER
(Vote For One)

- TOM GALLAGHER — REP
- JOHN COSGROVE — DEM

### COMMISSIONER OF EDUCATION
(Vote For One)

- CHARLIE CRIST — REP
- GEORGE H. SHELDON — DEM
- VASSILIA GAZETAS — NPA

## LEGISLATIVE

### STATE REPRESENTATIVE 44TH HOUSE DISTRICT
(Vote For One)

- DAVE RUSSELL — REP
- GREGORY L. WILLIAMS — DEM

## COUNTY

### SHERIFF
(Vote For One)

- LAWRENCE W. CROW, JR. — REP
- KIRK WARREN — DEM

### SUPERINTENDENT OF SCHOOLS
(Vote For One)

- JIM THORNHILL — REP
- DENNY DUNN — DEM

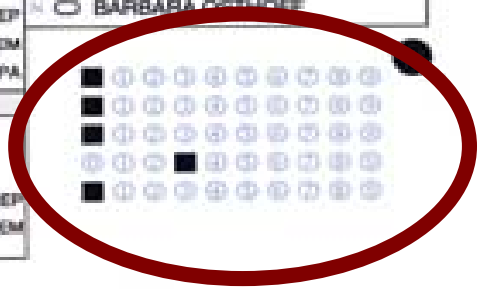
### COUNTY COMMISSIONER DISTRICT 1
(Vote For One)

- DON GIFFORD — REP
- JANET SHEARER — DEM

## COUNTY - NONPARTISAN

### SUPERVISOR OF ELECTIONS
(Vote For One)

- LORI EDWARDS
- BARBARA [illegible]



# Aufbau der Ergebnistabelle

1) Seriennummer
2) Prüfletter PX (vom Stimmzettel)
3) Umschlag X (Zeile von Umschlag Y)
4) Prüfletter PY (Ableitung von X)
5) Umschlag Y (Zeile des Ergebnisses)
6) Ergebnis

# Umschläge

- vor der Wahl versiegelt
- Umschlag X:
  - Aussage, ob PY von PX abweichen wird (“differ”) oder nicht (“same”)
  - Verweis auf Zeilennr. von Umschlag Y
- Umschlag Y:
  - Aussage, ob PY vom Ergebnis abweichen wird
  - Verweis auf Zeilennr. des Ergebnisses

# Swapped / Not Swapped

- Prüflettern in zufälliger Reihenfolge auf dem Stimmzettel

- Prüflettern alphabetisch geordnet (“not swapped”)

  **A -** Clintarak

  **B -** Huckapaul

- Prüflettern nicht alphabetisch geordnet (“swapped”)

  **B -** Clintarak

  **A -** Huckapaul

# Kippende Bits

- Swapped:
  - differ ⇢ same
  - same ⇢ differ
- Not Swapped
  - differ ⇢ differ
  - same ⇢ same

- A ⇾ B ⇾ B
- A ⇾ A ⇾ B
- A ⇾ B ⇾ A
- A ⇾ A ⇾ A

# Beispiel: Bulletin Board

| ***Seriennummer*** | ***PX*** | ***Umschlag X*** | ***PY*** | ***Umschlag Y*** | ***Ergebnis*** |
|---|---|---|---|---|---|
| 12345 | | “same”, 3 | | “differ”, 2 | |
| 98765 | | “differ”, 1 | A | “differ”, 3 | |
| 22339 | A | “same”, 2 | | “differ”, 1 | B = Huckapaul |

- 12345 ist “swapped”
- 98765 ist “not swapped”
- 22339 ist “swapped”

# Doppelte halbe Überprüfung

Zufällig ausgewählte Umschläge X werden geöffnet

Prüflettern PX und PY verglichen

Alle Umschläge Y, auf die nicht verwiesen wurde, werden geöffnet

Prüfletter PY und Ergebnis wird verglichen

*Wahlgeheimnis gewahrt, Integrität gewährleistet*

# Uncertainity

Wähler glaubt, sein Stimmzettel wäre übersehen worden

precinct-scan: Der Wähler kann zusehen, wie seine Stimme gezählt wird

# Doubt

Der Wähler glaubt, sein Stimmzettel wäre falsch gezählt worden

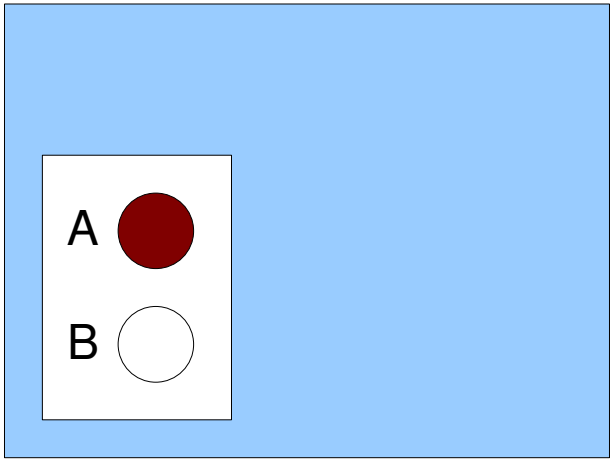
Kann per Internet oder Telefondienst die notierte und gezählte Prüfletter vergleichen

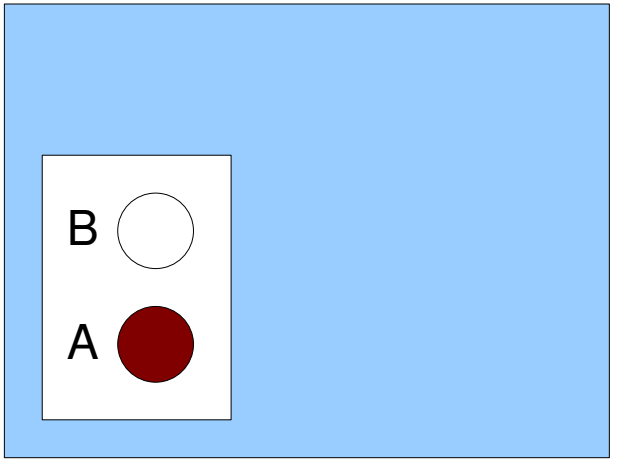
# Fear

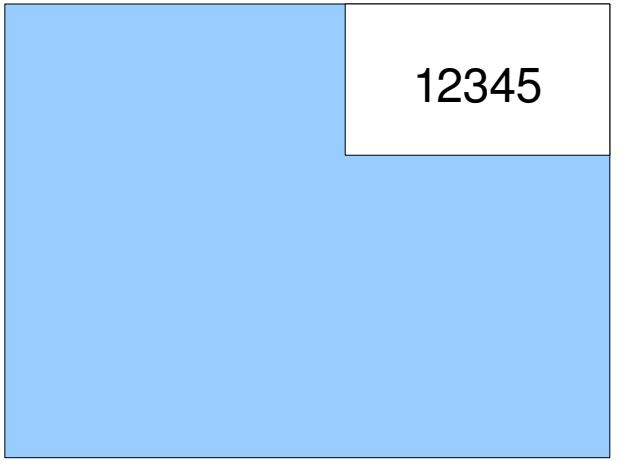
Der Wähler fühlt sich trotzdem betrogen

Persönliche Überprüfung des Stimmzettels

Nutzung semi-transparenter Umschläge



# Beispiel: In Persona Überprüfung

Wähler glaubt B gewählt zu haben, gezählt wurde A

Wähler bringt Abschnitt mit Seriennummer

Vergleich des Abschnitts mit Stimmzettel in Umschlag 1

Echter Stimmzettel und “Kontroll-Stimmzettel” (andere Reihenfolge, aber ebenfalls mit A markiert) kommen in Umschläge 2 und 3

Beide enthalten A, also ist der Wähler widerlegt

# Wahrscheinlichkeiten für N=2

Fälschung einer Stimme: 1 : 4

Fälschung von 10 oder mehr Stimmen: 1 : 1024

Vorrausgesetzung: Genügend Zufall

# Zufall?

- Zufälligkeit ist essentiell
  - swapped oder nicht swapped?
  - Welche Seriennummer wird überprüft
  - Verteilung der Zellen in der Ergebnistabelle
- Methoden:
  - Münzwurf
  - Aktienkurse
  - “Lazy Susan”

# Blinde und Analphabeten

- Stimmzettel ohne Namen (nur Prüflettern)
- Computer liest Namen + Prüflettern vor
- Wähler nennt Prüfletter
- Helfer markiert Prüfletter (!)
- Wähler spricht für sich die Prüfletter auf Band
- Wähler kann per Telefondienst überprüfen

# Verschwierigung

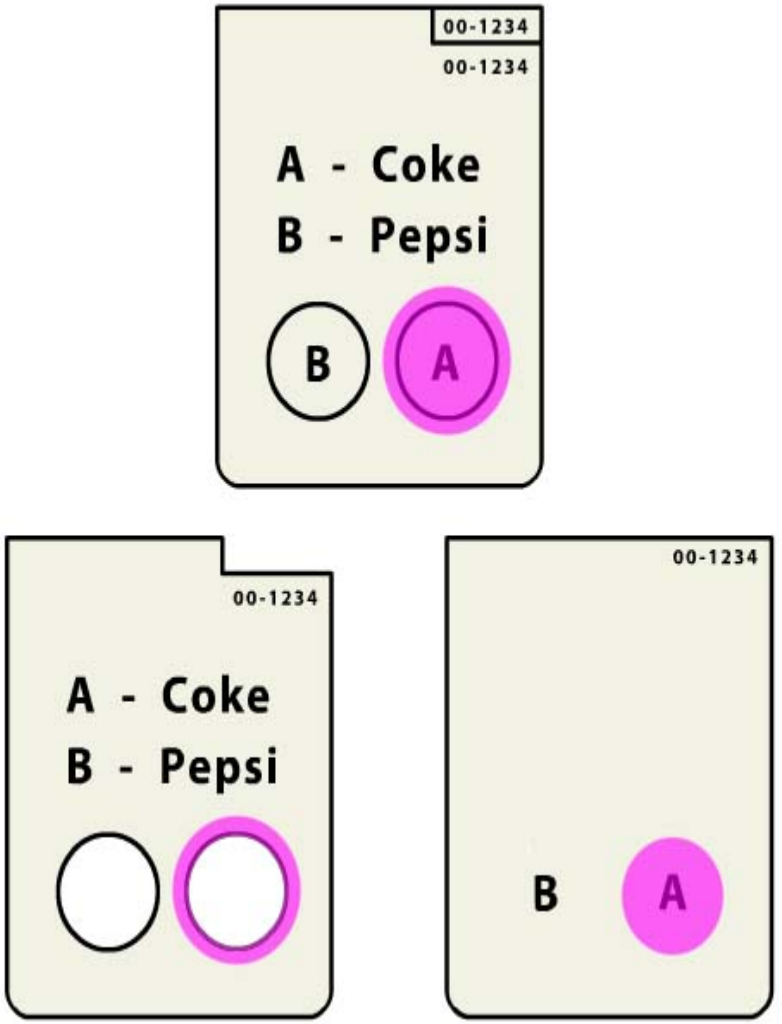
Bei mehr als 2 Kandidaten: Shift statt Swap (z.B. “+4” statt “differ”)

bei Mehrfachwahl: zusätzliche Randomisierung möglicher Sequenzen

bei mehreren Anliegen: Unterscheidung mittels Sequenzen (z.B. AA ... AZ, BA ... BZ)

# Scan-Voting: Beispiel Punchscan

- schablonenartiger, doppelter Stimmzettel
- eine Seite wird vernichtet
- eine Seite wird gescant und kann vom Wähler mitgenommen werden
- Seite kann online mit Scan verglichen werden



# Probleme

- Seriennummern in manchen Ländern illegal
  - allerdings: Fingerabdrücke, Knicke, Kratzer, unsichtbare Tinte, DNA-Spuren, Handschrift...
- Wähler schreibt Buchstaben auf Abriss
- Regierung öffnet alle Umschläge
- Synchronisation zwischen Wählerliste und Scantegrity-Datenbank

# Fazit

Spannende Idee und sehr durchdacht

Gute Synthese aus Papier und Computer

Sehr komplex bei komplexen Wahlen

Hack-Anfälligkeit noch zu ermitteln

# Quellen

Links auf Gültigkeit überprüft am 22.01.2008, 21:15 Uhr)


Chaum, David: Scantegrity - Transparent Integrity for Any Optical-Scan Voting System [Working Draft]. 2007, URL: http://www.scantegrity.org/papers/summary.pdf.

Chaum, David: The Scantegrity System - An Introductory Whitepaper and Example [Working Draft], 2007, URL: http://www.scantegrity.org/papers/whitepaper.pdf.

Sietmann, Richard: Wähler-Selbstkontrolle, in: c't 2007, 19, S.84-89.

Chaum, David: This Can Change Everything, Ort: Berlin, 2007

# Quellen 2

Smith, Warren D.: Chaum's "Scantegrity" secure-voting concept, 2007, URL: http://rangevoting.org/ChaumST.html

Future Tense: Interview with David Chaum, BBC Radio, 2007, URL: http://punchscan.org/press/punchscan%20-%20digital%20planet.mp3

Ausserdem die Screencasts und Präsentationen auf `scantegrity.org` und `punchscan.org`