# Überblick

Scantegrity ist ein elektronisches Wahlsystem, das sich beißende Wünsche zu erfüllen versucht

# Gliederung

- Einleitung
- David Chaum
- Scantegrity
  - Ziele
  - Verfahren
- Aus- / Bewertung

# Einleitung

- Sinn elektronischer Wahlsysteme
- Bisherige Wahlcomputer
- Die eigentlichen Schwachstellen

# David Chaum

- Doktor in Informatik mit dem Nebenfach Betriebswirtschaft an der Universität von Kalifornien, Berkeley
- betreute Aufbaustudiengänge in Betriebswirtschaft an der New Yorker Universität und der Universität von Kalifornien
- Gründete Forschungsgruppe für Kryptographie am "Center for Mathematics and Computer Science (CWI)" in Amsterdam
- 1990 gründete er DigiCash
- bereits 54 technical articles und 17 US Patente angemeldet

# Scantegrity - Ziele

- Anonymität / Wahlgeheimnis erfüllen
- Verifizierbarkeit der abgegebenen Stimmen
- Möglichst hohe Anpassungsfähigkeit an existierende, auf optischen Scannern basierende Systeme

# Scantegrity – Verfahren
## Überblick

- Eingeteilt in 4 Phasen
  - (1) pre-voting
  - (2) voting
  - (3) pre-audit
  - (4) audit

# Scantegrity – Verfahren
## Permutationen

- Eineindeutige Vertauschungsvorschrift / -Abbildung für eine vorgegebene Anzahl von Buchstaben

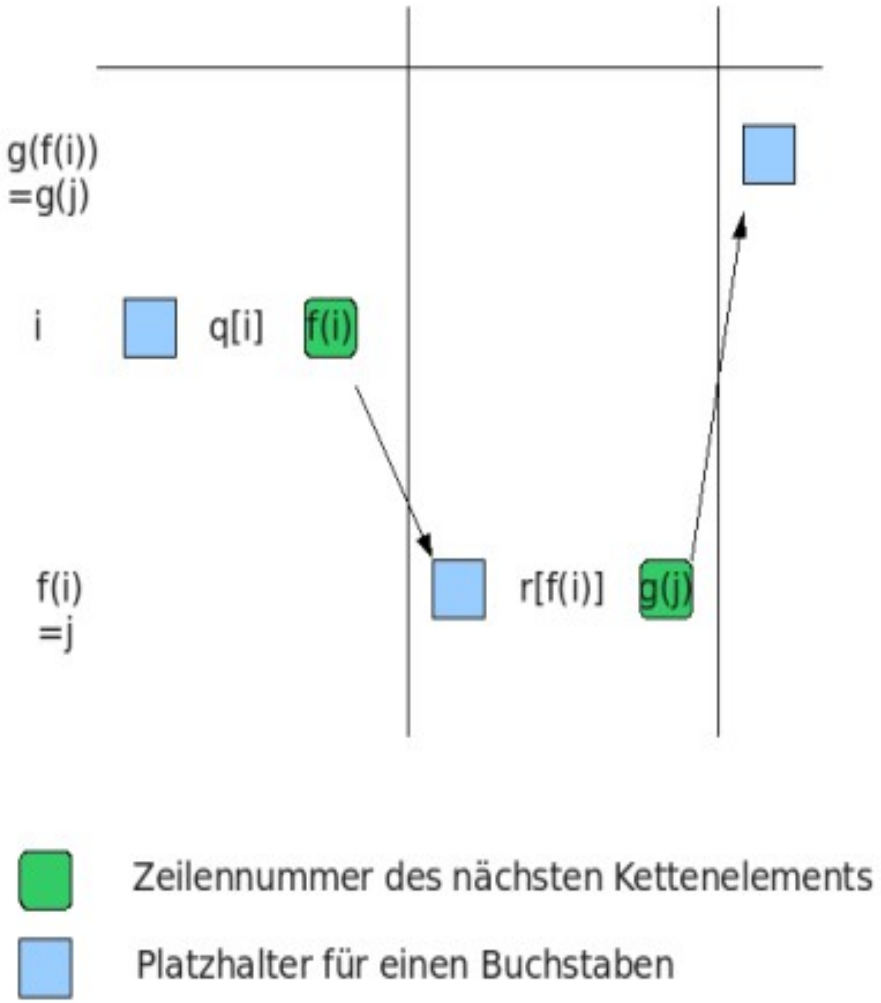
$$\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

- Verknüpfung zweier solcher Abbildungen durch die Hintereinanderausführung der Vertauschungen
- Umkehrabbildung durch Umkehrung der Richtung der Abbildung

$$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

# Scantegrity – Verfahren
## (1) pre-voting

- bulletin-board als Kern von Scantegrity
- Zusammenspiel der Permutationen der Wahlzettel und des bulletin-boards



# Scantegrity – Verfahren
## (2) voting

- Sicht des Wählers
  - (A) wählen und Seriennummer und Buchstabe des Kandidaten notieren
  - (B) Wahl verifizieren
  - (C) bei Unstimmigkeiten den Wahlveranstalter kontaktieren
- Sicht des Wahlveranstalters
  - Technische Voraussetzungen
  - Umstellung / Aufrüstung auf optische Scanner

# Scantegrity – Verfahren
## (2) voting

- Füllen der Platzhalter
  - Erste Platzhalter direkt gefüllt
  - Zweiter Platzhalter mit Ergebnis der Permutation unter dem Buchstaben füllen
  - Gleiches Prinzip für letzte Position

# Scantegrity – Verfahren
## (3) pre-audit

- Stichproben zum Prüfen der Integrität des bulletin-boards
- Verschiedene Szenarien
  - Jeder Bürger erhält 2 Wahlzettel
  - Jeder Bürger darf frei über Stichproben entscheiden
  - Stichproben werden beim Verteilen der Wahlzettel zufällig ausgeführt

# Scantegrity – Verfahren
## (4) audit

- Teilweise Offenbarung der geheimen Daten des bulletin-boards
- Die Wahrscheinlichkeit für einen Betrüger, bei k manipulierten Versuchen nicht entdeckt zu werden: $\frac{1}{2^k}$

# Scantegrity – Verfahren

## Erweiterung auf übliche Wahlprinzipien

- Kernprinzip bleibt stets erhalten
- Mehrere Stimmen innerhalb einer Wahl durch Vervielfachung der Platzhalter
- Mehrere Wahlen auf einem Wahlzettel durch Klonen des bulletin-boards

# Aus- / Bewertung

- Verifizierbarkeit erfüllt
- Anonymität gestärkt
- Verhältnismäßig hohes Maß an Komplexität

# Quellen

- http://www.chaum.com (12.12.2007, 22:19)
- http://de.wikipedia.org/wiki/David_Chaum (12.12.2007, 23:34)
- Scantegrity Whitepaper (12.12.2007, 18:07)