Elektronisch wählen

Rob van Stee

14. Januar 2008

Wahlcomputer auf dem Prüfstand

BNN 8/1/8

Wiesbaden (BNN/dpa). Der Chaos Computer Club will den Einsatz von Wahlcomputern bei der hessischen Landtagswahl wegen angeblich gravierender Sicherheitsmängel verhindern. Dazu habe eine hessische Wählerin mit Unterstützung des Clubs einen Antrag auf Erlass einer Einstweiligen Verfügung beim Staatsgerichtshof in Wiesbaden eingereicht, teilte der Verein von Hackern, mit.

Zur Begründung hieß es, die Wahlcomputer seien unsicher und könnten manipuliert werden. Unterdessen muss Regierungschef Koch weiter um seine Mehrheit im Landtag bangen. (Siehe Zeitgeschehen.)

Überblick

- Hintergründe
- Formen
- Software-unabhängige Systeme
- Vollständig überprüfbare Systeme

  Beispiele
  - Punchscan
  - Bingo-Voting

Wieso elektronisch wählen?

- Geschwindigkeit
- Arbeit sparen
- Keine Zähl- oder Rechenfehler
- Geld sparen: Papier, Arbeitskräfte
- Größere Wahlbeteiligung
  - Einfachheit (aber nicht für alle…)
  - Unterstützung für Behinderte
- Bessere **Überprüfung** der Auszählung

„Mal kurz nachschauen, wie meine Stimme gezählt wird…“

Überprüfung

Mit Hilfe von Kryptografie wird erreicht, dass man folgendes überprüfen kann:

- Stimme wurde richtig gespeichert
- Stimme wurde gezählt

Diese Möglichkeit hat man bei einer Papierwahl nicht, wenigstens nicht so leicht (Beobachtung möglich)

Hauptproblem bei elektronischen Wahlen (in Theorie)

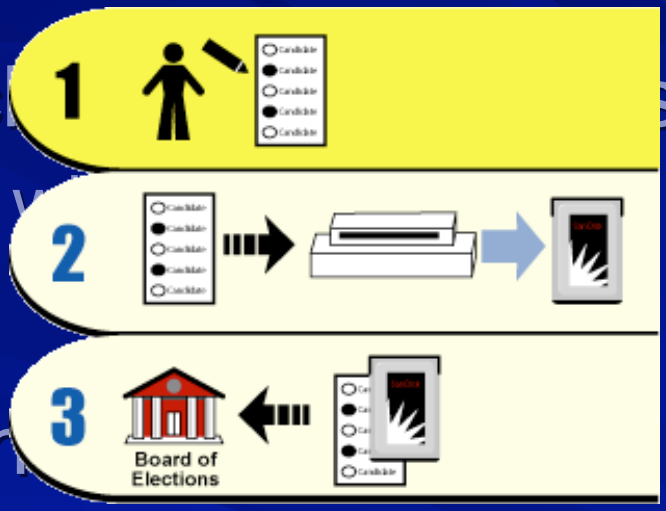
Geheimhaltung vs. **Überprüfbarkeit**

Es darf nicht nachweisbar sein, wo jede Stimme herkommt

Man muss beweisen können, wie viele Stimmen jeder Kandidat /jede Partei bekommen hat

Formen von E-Wahlen

- Elektronisc systeme in Sälen (Wer
- Web-Polls
- Internetwah

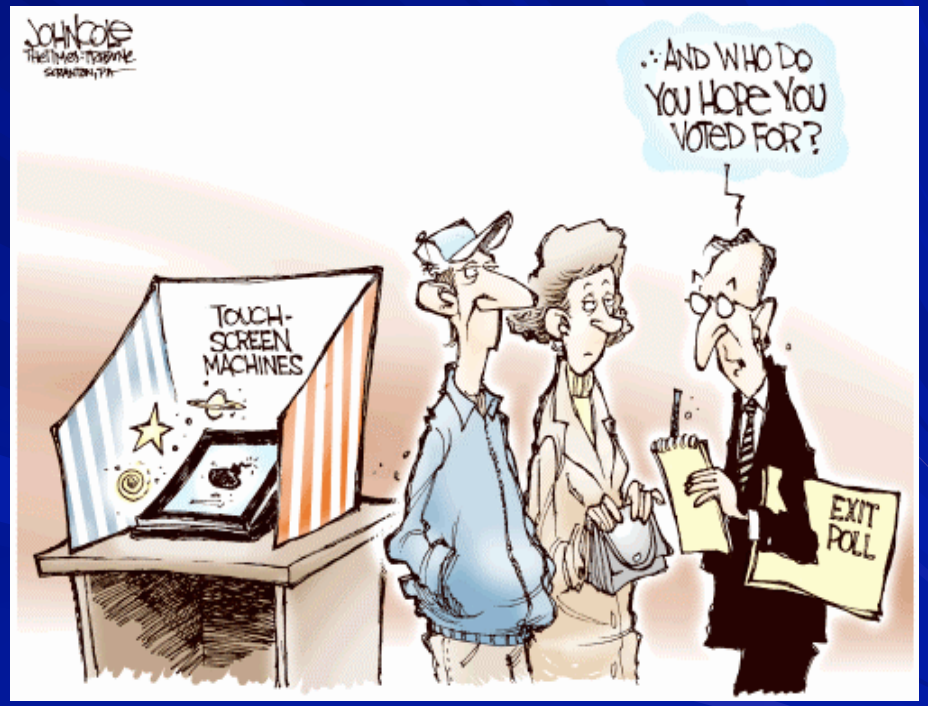


- Papierbasierte Systeme (Zählmaschinen)
- Wahlmaschinen
  - Eventuell mit Ausdruck von Stimmzetteln

DRE-Wahlmaschinen

=Direct Recording Electronic

- Stimmabgabe, Speicherung und Zählung elektronisch
- Keine Nachzählung möglich (sinnlos)
- Kaum Kontrolle möglich

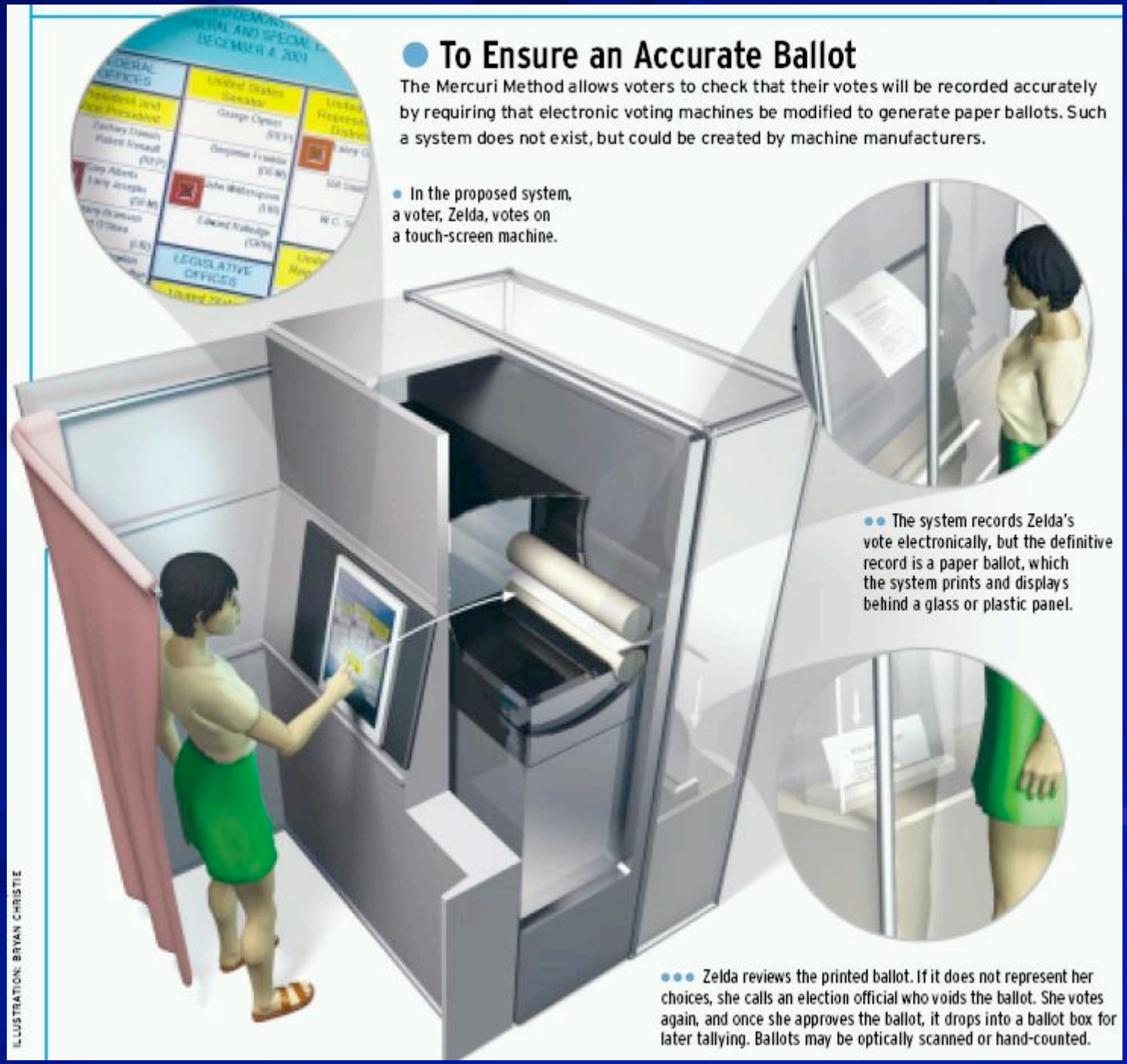


Software-Unabhängigkeit

Software-unabhängig*: eine unbemerkte Änderung oder Fehler in der Software kann nicht zu einer unerkennbaren Änderung oder Fehler im Wahlergebnis führen* [Rivest & Wack, 2006]

Beispiele :

- DRE + Voter Verified Paper Audit Trail (VVPAT) [Mercuri, 1992]
- kryptografische Systeme


To Ensure an Accurate Ballot
The Mercuri Method allows voters to check that their votes will be recorded accurately by requiring that electronic voting machines be modified to generate paper ballots. Such a system does not exist, but could be created by machine manufacturers.
In the proposed system, a voter, Zelda, votes on a touch-screen machine.
The system records Zelda's vote electronically, but the definitive record is a paper ballot, which the system prints and displays behind a glass or plastic panel.
Zelda reviews the printed ballot. If it does not represent her choices, she calls an election official who voids the ballot. She votes again, and once she approves the ballot, it drops into a ballot box for later tallying. Ballots may be optically scanned or hand-counted.
ILLUSTRATION: BRYAN CHRISTIE

Vollständig überprüfbare Systeme

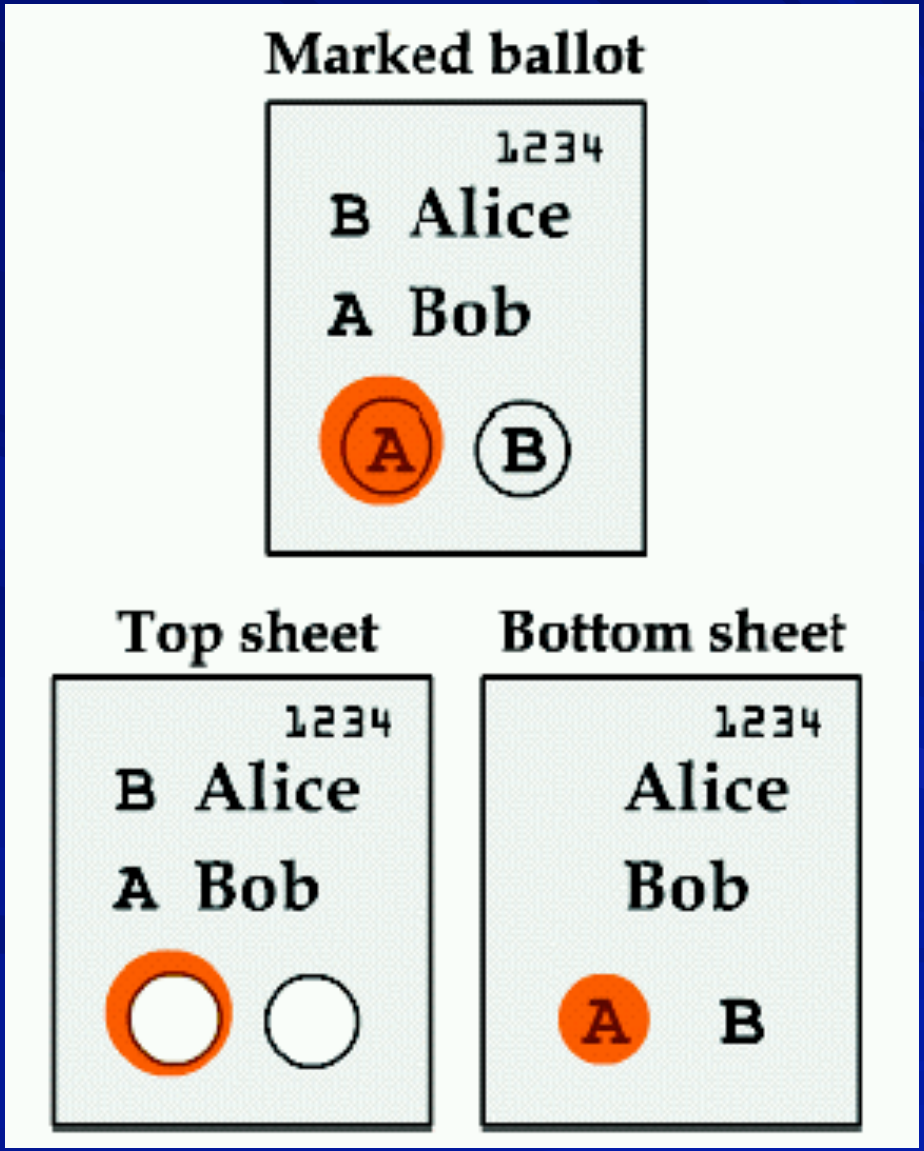
(end-to-end auditable systems)

- Wähler kann prüfen, ob seine Stimme richtig gespeichert und mitgezählt wurde
- Jeder kann prüfen, ob die Ergebnisse richtig zusammengezählt wurden
- Keiner kann beweisen, was er gewählt hat!

Punchscan [Chaum 2006]

- Stimmzettel bestehen aus **zwei Hälften**
  - Erste Hälfte: Kandidaten + Symbole
  - Zweite Hälfte: nur Symbole
  - Beide Hälften: Seriennummer
- Symbole sind auf beiden Hälften gleich, aber in wechselnden Reihenfolgen
- Erste Hälfte hat Löcher, so dass Symbole auf der zweiten Hälfte auch sichtbar sind
- Wähler markiert immer beide Seiten

Beispiel Stimmzettel



Punchscan

- Der Wähler wählt einen von beiden Zetteln aus und vernichtet ihn (shredden)
- Den anderen Zettel scannt er ein und nimmt ihn mit nach Hause (!)
  - Ergebnisse werden (nur) elektronisch gespeichert

Datenbank

- Es gibt eine Datenbank mit folgende Informationen:
  - Seriennummer
  - Reihenfolge der Symbolen auf beide Hälften
- Diese Datenbank ist geheim!
- Eine verschlüsselte Version wird vor der Wahl veröffentlicht

Commitments

Verschlüsselung

- Wahlveranstalter generieren zusammen einen zentralen Schlüssel
  - Personen aus verschiedenen Parteien (entgegengesetzte Interessen)
  - Schlüssel basiert z.B. auf allen usernames und passwords zusammen
- Schlüssel wird benutzt zur Kodierung
  - AES128 (Advanced Encryption Standard / Rijndael)

Verschlüsselung

- Jeder Stimmzettel hat einen **eigenen** Schlüssel!
  - Kodierung von zentralen Schlüssel + Seriennummer mit AES

1. Überprüfung: vor der Wahl

Randomized partial checking:

- Prüfer wählt willkürliche Teilmenge der Seriennummern aus
- Für diese Stimmzettel bekommt er
  - Reihenfolge der Symbole (beide Hälften)
  - Schlüssel dieses Zettels
- Verschlüsselung sollte übereinstimmen mit vorher veröffentlichter Datenbank

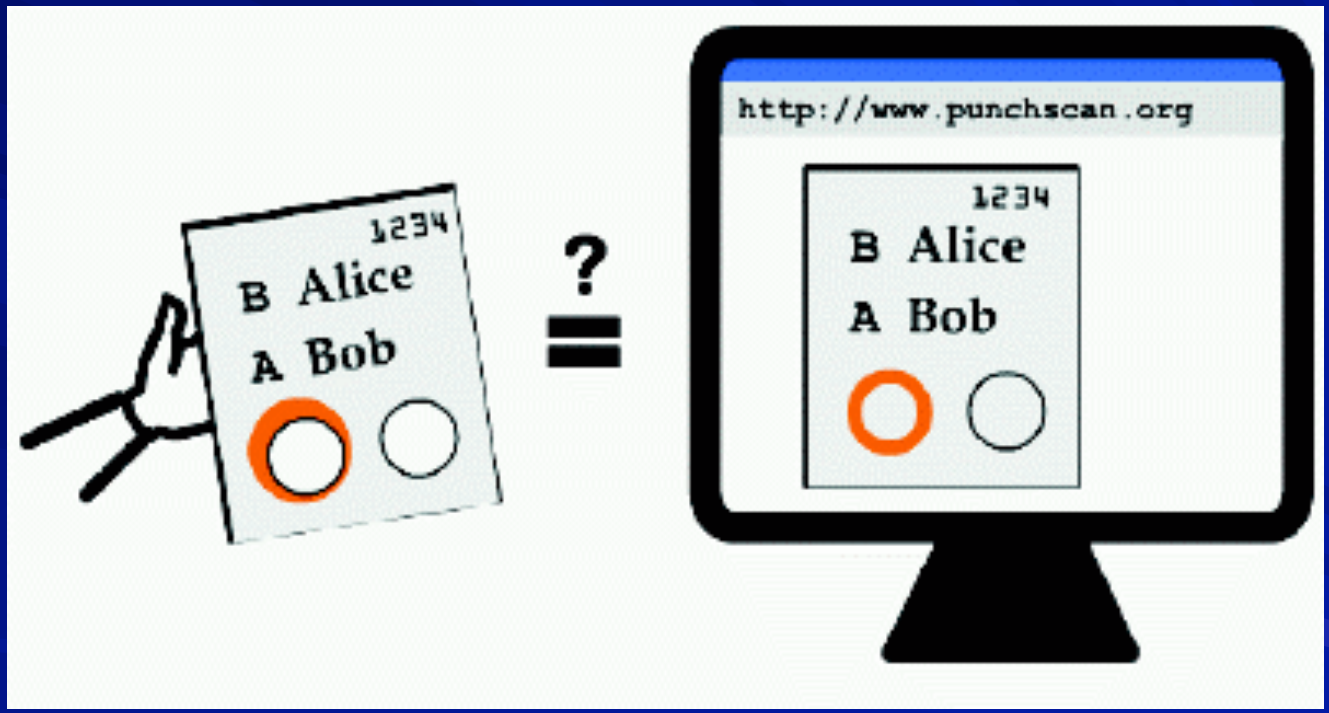
Zero-Knowledge Beweis

2.Überprüfung: durch Wähler

Für jeden eingescannten Stimmzettel wird veröffentlicht:

- Welche Hälfte der Wähler behalten hat
- Symbolreihenfolge dieser Hälfte (laut Datenbank)
- Wievieltes Symbol der Wähler markiert hat

2.Überprüfung



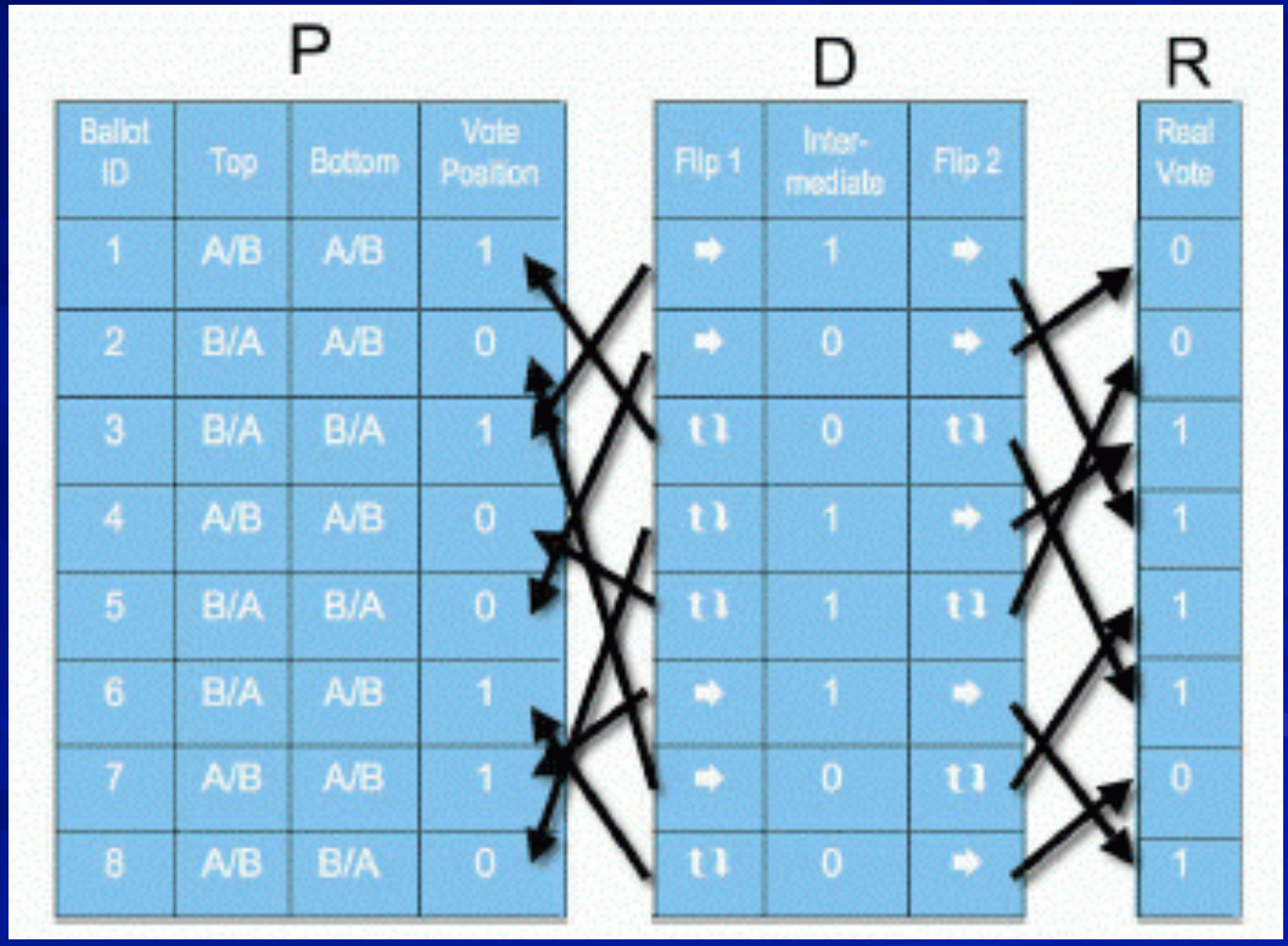
Was jetzt noch fehlt

Werden die
Stimmen auch
richtig gezählt?

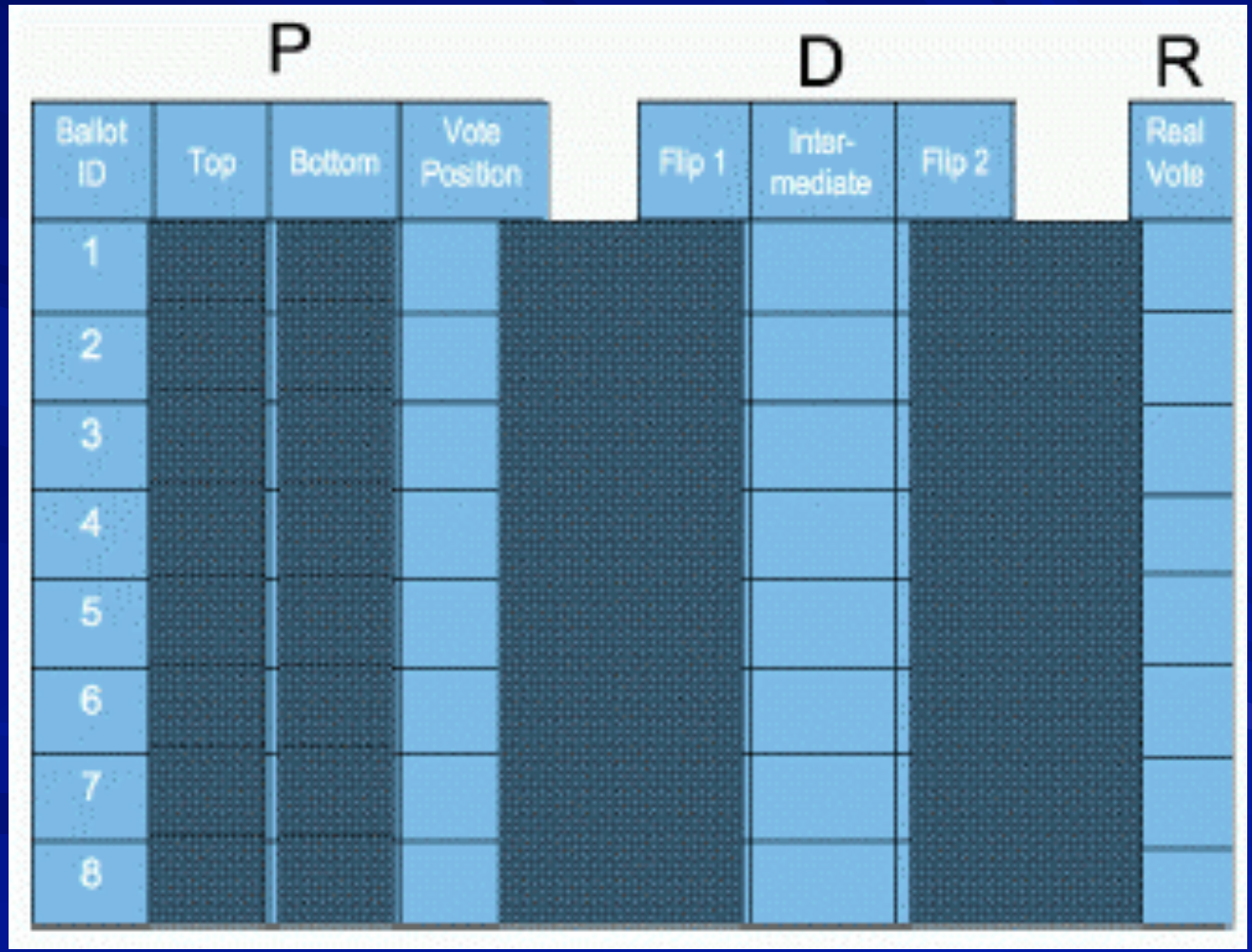
Stimmen zählen

- Die Zählung besteht aus **zwei Schritten** (schon vor der Wahl festgelegt u. geprüft!)
- In beiden Schritten passiert folgendes:
  - *Partielle* Entzifferung
  - Mischung der Stimmzettel
- Nach zwei Schritten: Ergebnis bekannt
- Keine öffentliche Verbindung zwischen Stimmzettel und Stimme!

Punchboard


P
D
R
Ballot ID
Top
Bottom
Vote Position
Flip 1
Inter-mediate
Flip 2
Real Vote
1 A/B A/B 1 → 1 → 0
2 B/A A/B 0 → 0 → 0
3 B/A B/A 1 ↓↑ 0 ↓↑ 1
4 A/B A/B 0 ↓↑ 1 → 1
5 B/A B/A 0 ↓↑ 1 ↓↑ 1
6 B/A A/B 1 → 1 → 1
7 A/B A/B 1 → 0 ↓↑ 0
8 A/B B/A 0 ↓↑ 0 → 1

Veröffentlicht vor der Wahl



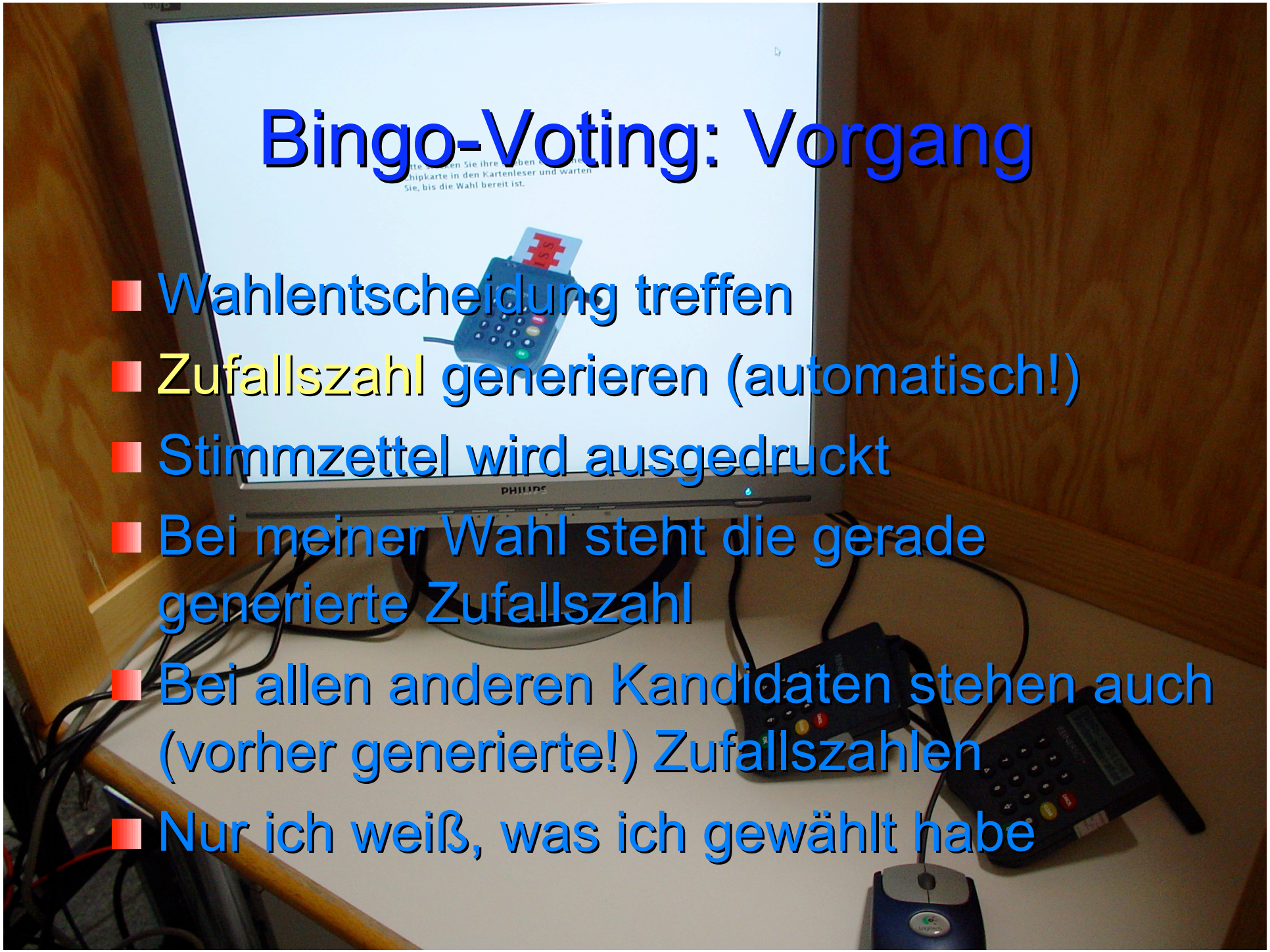
3. Überprüfung: Nach der Wahl

- Die erste **oder** die zweite Mischung + Entzifferung wird veröffentlicht
- Welche Hälfte? **Zufall**!
  - Wahlveranstalter weiß nicht, welche Mischung er später veröffentlicht
  - Beide Hälften müssen stimmen
- Jeder kann dann prüfen, ob in dieser Mischung alles stimmt

Mögliche Probleme

- Stimmzettel werden sehr kompliziert für große Wahlen (viele Kandidaten, parallele Wahlen…)
- 85% der Teilnehmer wählt die obere Hälfte: sollte 50% sein
- Besser, wenn Zufall nicht von den Teilnehmern abhängt
- Alternative: Bingo-Voting [Bohli, Müller-Quade, Röhrich 2007]

Bingo-Voting: Vorgang



- Wahlentscheidung treffen
- Zufallszahl generieren (automatisch!)
- Stimmzettel wird ausgedruckt
- Bei meiner Wahl steht die gerade generierte Zufallszahl
- Bei allen anderen Kandidaten stehen auch (vorher generierte!) Zufallszahlen
- Nur ich weiß, was ich gewählt habe

Beispiel Stimmzettel

Alice	29456349765
Bob	34875634953
Carol	12098734473

- Funktioniert auch mit mehreren Stimmen pro Kandidat
- Beispiel: Studentenparlament Karlsruhe

Bingo-Voting

- Nach der Wahl werden alle Stimmzettel veröffentlicht (elektronisch)
- Jeder kann prüfen, ob sein Stimmzettel dabei ist
- Niemand kann beweisen, wie er gewählt hat

Bingo-Voting

- Vorher generierte Zufallszahlen werden verschlüsselt aufbewahrt
- Für jeden Kandidat gibt es *n* Zufallszahlen
- Anzahl von Zufallszahlen die noch übrig sind = Anzahl Stimmen für diesen Kandidat
- Nicht benutzte Zufallszahlen werden nachher veröffentlicht

Zusammenfassung

- Hauptproblem bei elektronischen Wahlen ist Geheimhaltung kombinieren mit Überprüfbarkeit
- DREs + VVPAT sind dafür (noch) nicht gut geeignet (EVEREST-Bericht)
- Vollständig überprüfbare Systeme sind besser
- Beispiele: Punchscan, Bingo-Voting

Vielen Dank!