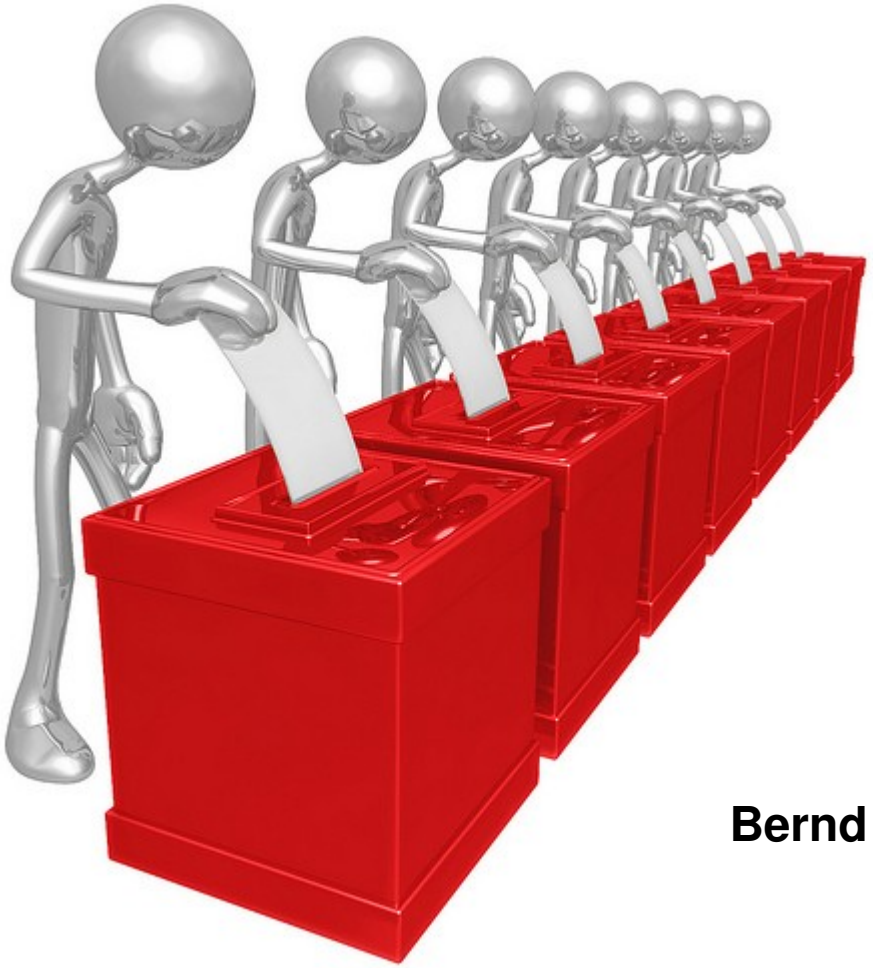


e-Voting für geschlossene Benutzergruppen

Bernd R. Fix `<bernd.fix@aspector.com>`

Warum ist dies ein Ketzervortrag?

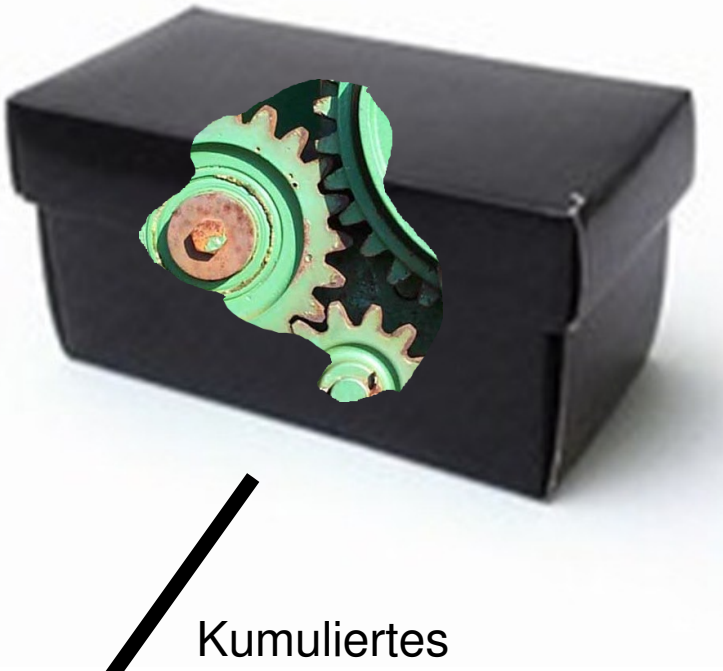
[...] weil Wahlcomputer ***grundsätzlich*** böse sind und wir als CCC doch genau wissen, dass es sichere elektronische Wahlen nicht geben ***kann*** [...]

Ich halte es mit der Hackerethik:

Misstraue Autoritäten ...

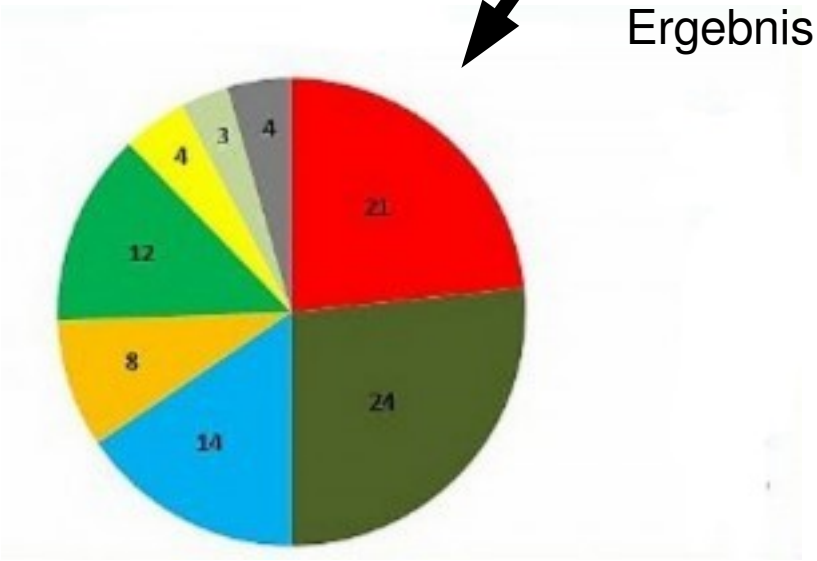
... auch und gerade den Selbsterschaffenen wie dem CCC

Individuelle Wählerstimmen



Kumuliertes Ergebnis

Vertrauen?



Vertrauen in den Wahlprozess

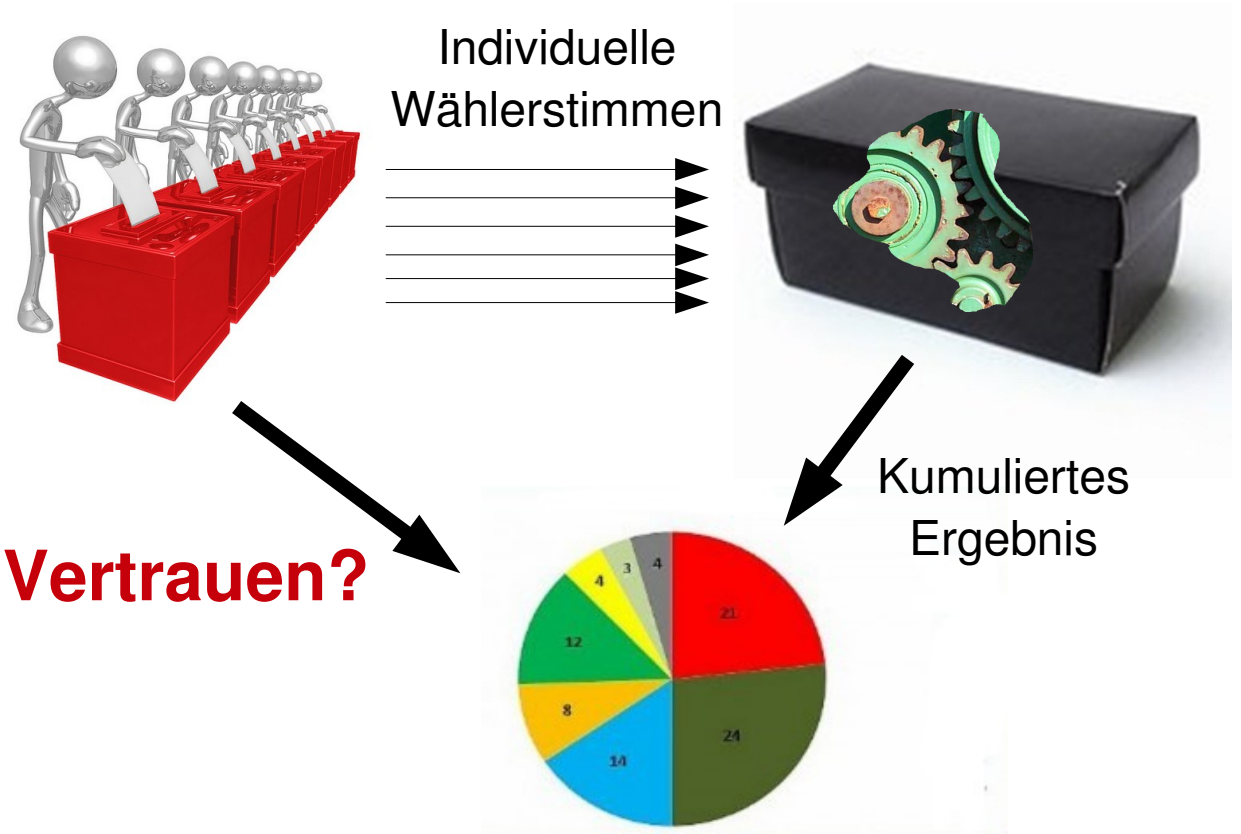
- **Korrektheit der Auszählung**
  - Jede abgegebene Stimme wurde korrekt verbucht
  - Alle gezählten Stimmen sind berechtigte Stimmen
  - Jeder Wahlberechtigte hat nur eine einzige Stimme
- **(Wahrung des Wahlgeheimnisses)**

Wahlgeheimnis – wozu?

Das ***Wahlgeheimnis*** wird vor allem in den Gesellschaften für wichtig erachtet, in den Menschen auf Grund ihrer politischen Einstellung *benachteiligt*, *verfolgt*, *eingesperrt*, *gefoltert* oder sogar *ermordet* wurden oder werden...

Böse ausgedrückt: Die Notwendigkeit eines ***Wahlgeheimnisses*** ist eher ein Ausdruck einer fehlenden Maturität der Gesellschaft als ein demokratisches Gut, das es zu erhalten gilt...

Warum basiert das *Vertrauen in das Ergebnis* auf dem *Vertrauen in den Wahlprozess*?



Warum basiert das *Vertrauen in das Ergebnis* auf dem *Vertrauen in den Wahlprozess*?

Ein Wähler kann das Ergebnis nicht selbst kontrollieren, ...

- ... weil Stimmen durch Abgabe des Wahlzettels in der Urne ***anonymisiert*** werden. (***Wahlgeheimnis***)
- ... weil nur ***akkumulierte*** Stimmen und nicht alle einzelnen Wahlzettel (inklusive der Wählerlisten) veröffentlicht werden. (***Verlust der Zählbarkeit***)

Vertrauen in das Ergebnis = Vertrauen in den Wahlprozess

***Was wäre*, wenn jeder das Wahlergebnis *direkt* kontrollieren könnte?**
(ohne Verletzung des Wahlgeheimnisses)

⇒**Es wäre kein Vertrauen in den Wahlvorgang mehr nötig – d.h. *die Art der Wahl wird irrelevant*...**

Kürzel	1	2	3	4	5	6	Gültig		
08/15	X						J		
Brummbär			X				J		
The Reaper		X					J		
Nur ich allein						X	J		
Martin89			X				J		
Don't vote							N		
Kuschelhase	X						J		
As45fw34sf			X				J		
Blödmann	X		X				N		
Carsten S.					X		J		
Ferrari					X		N		
Der Hamster			X				J		
Max Headroom			X				J		
Summe:	**2**	**1**	**5**	**0**	**1**	**1**	**10/12/1**		

Zu lösende Probleme:

- Nur berechtigte Wähler dürfen ihren Wahlzettel abgeben
- Jeder berechtigte Wähler hat nur eine Stimme

Die Problemlösung darf das Wahlgeheimnis nicht verletzen!

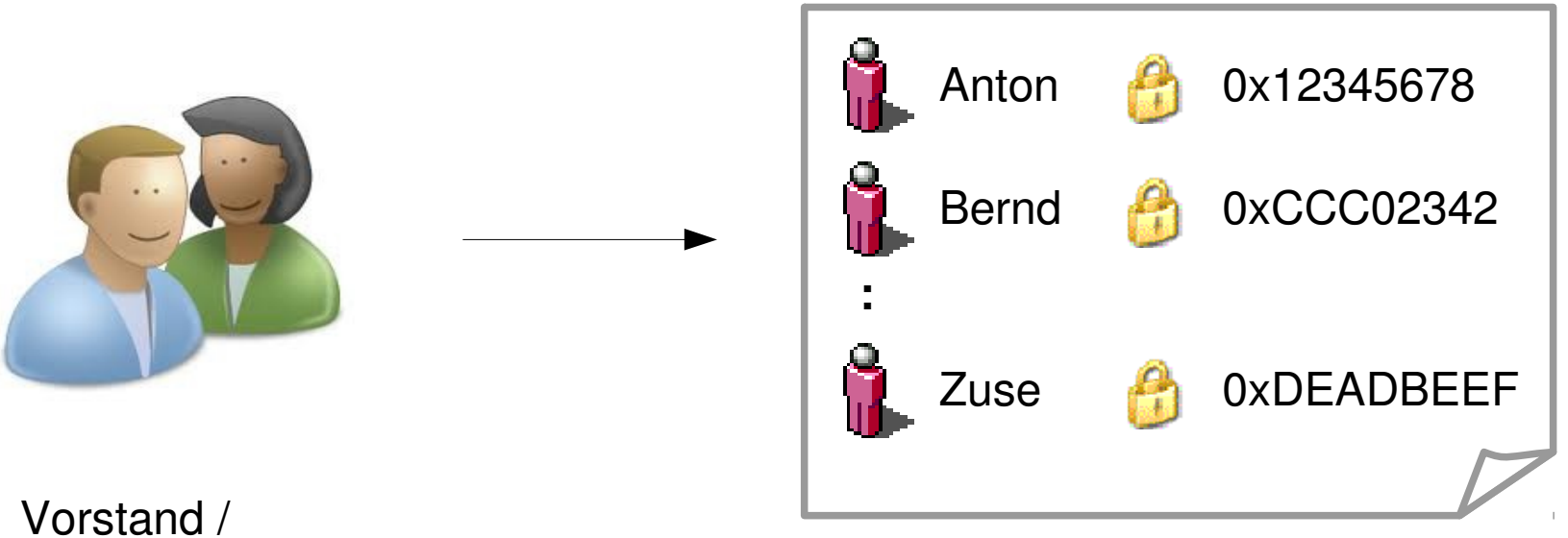
Lösungsansatz verwendet ***PKI***, ...

... aber ***ohne zentrale Authoritäten***, d.h. es gibt ***keinen MasterKey***, mit dessen Kenntnis die Wahl in irgendeiner Form manipuliert werden kann.

Ablauf einer digitalen Abstimmung

Schritt 1: Wählerverzeichnis veröffentlichen

Die Liste aller wahlberechtigten Wähler wird zusammen mit dem (Verweis auf den) öffentlichen RSA-Schlüssel des Wählers publiziert.



Vorstand / Wahlausschuss

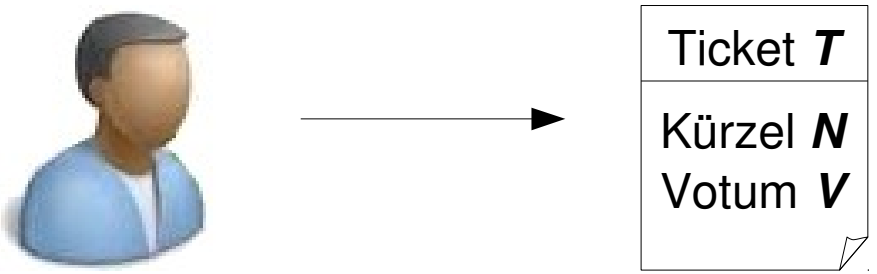
veröffentlicht

Wählerverzeichnis

Ablauf einer digitalen Abstimmung

Schritt 2: Ausüben der Wahl

Jeder Wähler erfindet ein eindeutiges, aber nur ihm bekanntes Kürzel ***N*** und erstellt sein Votum ***V***. Daraus wird durch Verkettung das Wahlticket ***T*** erstellt.



Wähler erstellt Wahl-Ticket

Ablauf einer digitalen Abstimmung

Schritt 3: Wahlticket in Umschläge verpacken

Jeder Wähler ***W*** steckt sein Wahlticket ***T*** in Umschläge U_i – jeweils einen Umschlag für jeden Wähler (einschliesslich sich selbst) im Wählerverzeichnis. Er unterschreibt jeden Umschlag mit seiner Signatur S_i und stellt die Liste in das öffentliche Repository.

$$U_i = (T \bullet R_i^{e_i}) \; mod \; m_i$$

$$S_i = U_i^{d} \; mod \; m$$

R_i = Zufallszahl

$\{ e_i, m_i \}$ = öffentlicher Schlüssel des i.ten Wählers

$\{ d, m \}$ = geheimer Schlüssel des Wählers ***W***

Ablauf einer digitalen Abstimmung

Schritt 4: Blindsignatur der Umschläge

Jeder Wähler ***W*** holt sich alle Umschläge alle Wahlberechtigten aus dem Repository und extrahiert daraus die Umschläge, die für seinen Schlüssel erstellt wurden. Jeder dieser Umschläge $\boldsymbol{U_j}$ wird blind signiert, nachdem anhand der Signatur $\boldsymbol{S_j}$ Herkunft und Korrektheit des Umschlages geprüft wurden. Die Liste aller Blindsignaturen $\boldsymbol{B_j}$ wird wieder in das öffentliche Repository eingestellt.

$$B_j = U_j^{\,d} \ \mathit{mod}\ m$$

$\{ d, m \}$ = geheimer Schlüssel des Wählers ***W***

Ablauf einer digitalen Abstimmung

Schritt 5: Erstellen des Wahlzettels

Jeder Wähler holt sich alle Blindsignaturen aller Wahlberechtigten aus dem Repository und extrahiert daraus die Blindsignaturen B_i , die für seine eigenen Umschläge U_i erstellt wurden. Mit Hilfe der Zufallszahl R_i wird jetzt aus der Blindsignatur eine echte Unterschrift S_i^* für das Ticket T errechnet. Aus dem Ticket T und der Liste der S_i^* erstellt der Wähler den Wahlzettel, der ***anonym*** in das Repository eingestellt wird.

$$S_i^* = (B_i \bullet R_i^{-1}) \ \ mod \ \ m_i$$

R_i = Zufallszahl aus Schritt 3

$\{ .. , m_i \}$ = öffentl. Schlüssel des i.ten Wählers

Ablauf einer digitalen Abstimmung

Schritt 6: Wahlergebnis / Prüfen der Wahl

Jeder Prüfer holt sich alle Wahlzettel aller Wahlberechtigten aus dem Repository und prüft anhand der Unterschriften S_i^* die Gültigkeit des Tickets ***T***, das im Wahlzettel enthalten ist. Stimmen aus gültigen Tickets werden im Wahlergebnis gelistet und die gültigen Stimmen abschliessend zum Wahlergebnis kumuliert.

Jeder Wähler kann zusätzlich anhand seines Kürzels ***N*** sein eigenes Wahlticket im Wahlergebnis finden und prüfen.

Ablauf einer digitalen Abstimmung

Schritt 7: Revoken eines Wahlzettels

Stellt ein Wähler fest, das sein Wahlzettel nicht das von ihm intendierte Ticket enthält (sein Ticket wurde manipuliert, weil z.B. sein Rechner gepwnd wurde), dann kann er durch Veröffentlichung seiner Zufallszahlen $\boldsymbol{R}_i$ seinen Wahlzettel revoken.

Die Revokation kann von jedem geprüft werden, indem die Blindsignaturen $\boldsymbol{B}_i$, die Signaturen $\boldsymbol{S}_i^*$ und die Zahlen $\boldsymbol{R}_i$ miteinander verrechnet werden und das Ergebnis geprüft wird.

[N.B.: Die Zahlen $\boldsymbol{R}_i$ weisen einen inneren Zusammenhang auf, der aus den Zahlen selbst nicht rekonstruiert werden kann.]

Kürzel	1	2	3	4	5	6	Gültig	Wahlzettel	Revokation
08/15	X						J		
Brummbär			X				J		
The Reaper		X					J		
Nur ich allein						X	J		
Martin89			X				J		
Don't vote							N		
Kuschelhase	X						J		
As45fw34sf			X				J		
Blödmann	X		X				N		
Carsten S.					X		J		
Ferrari					X		N		
Der Hamster			X				J		
Max Headroom			X				J		
Summe / Alle:	2	1	5	0	1	1	10/12/1		

Alle Umschläge aller Wähler: **Alle Blindsignaturen aller Wähler:**

Wie ist der Stand der Dinge (a.k.a. „Gibt es das schon?“)

- „Erfunden“ von mir im Sommer 2004 als Gedankenspiel
- Java/OpenPGP - basierter Prototyp seit Frühjahr 2009
- Kann ohne extremen Aufwand zu einer benutzbaren Lösung aufgebohrt werden
- Veröffentlichung als Open-Source-Software geplant

Noch Fragen?

e-Voting für geschlossene Benutzergruppen

Bernd R. Fix `<bernd.fix@aspector.com>`