Signatures aveugles:

Une approche pour éviter la confiance aveugle

Eric Dubuis, Rolf Haenni

Haute école spécialisée bernoise

Blinde Signaturen

Ein E-Voting-Ansatz ohne blindes Vertrauen

Rolf Haenni, Eric Dubuis, Stephan Fischli, Reto König

Berner Fachhochschule

Inhaltsverzeichnis

1. Einführung
2. Blackbox vs. Transparenz
3. E-Voting mit blinden Signaturen
4. Das Problem des Stimmenkaufs
5. Fazit & Schlusswort

Rechtliche Grundlagen

StGB Art. 281: Wahlfälschung

Wer ein Stimmregister fälscht, beseitigt oder vernichtet,

wer unbefugt an einer Wahl oder Abstimmung [...] teilnimmt,

wer das Ergebnis einer Wahl oder einer Abstimmung [...] fälscht, insbesondere durch Hinzufügen, Ändern [...] oder Streichen von Stimmzetteln [...], oder durch unrichtiges Auszählen [...] des Ergebnisses,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Rechtliche Grundlagen

StGB Art. 283: Verletzung des Wahlgeheimnisses

Wer sich durch unrechtmässiges Vorgehen Kenntnis davon verschafft, wie einzelne Berechtigte stimmen oder wählen,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Anforderungen

Democracy

Eligibility > nur authorisierte Wähler können eine Stimme abgeben
Uniqueness > authorisierte Wähler können max. 1 Stimme abgeben
Fairness > vor dem Ende der Wahl werden keine Ergebnisse bekannt

Accuracy

Integrity > abgegebene Stimmen können nicht verändert werden
Completeness > jede gültige abgegebene Stimme wird gezählt
Soundness > ungültige Stimmen werden nicht gezählt

Privacy

Anonymity > eine Stimme kann nicht mit dem Wähler verlinkt werden
Receipt-Freeness > niemand kann beweisen, wie er gestimmt hat

Blackbox E-Voting

E-Voting-Systeme funktionieren oft nach dem Prinzip einer “Blackbox”:

> Die elektronische Stimme wird abgeschickt und danach in eine “elektronische Wahlurne“ gelegt

> Die elektronische Urne ist geschützt und der Zugriff stark eingeschränkt

> Am Ende der Wahl zählt eine “Zählsoftware” die Stimmen in der Urne und gibt das Resultat aus

Gefahren einer Blackbox

Der einzelne Wähler kann die korrekte Auszählung und das Resultat nicht überprüfen

> Grosse Manipulationsgefahr (intern/extern)

> Entwickler und Betreiber des Systems können erpresst oder gekauft werden

> Hacker können sich Zugriff verschaffen oder Malware einschleusen

> Die Wähler können dem System nicht vertrauen

Weitere Anforderungen

Individual Verifiability

Der Wähler kann überprüfen, dass seine Stimme angekommen ist und korrekt mitgezählt wurde

Universal Verifiability

Unabhängige Parteien oder einzelne Wähler können überprüfen, ob die abgegebenen Stimmen korrekt gezählt wurden

Situation in Deutschland

Leitfaden zum BVerfG-Urteil

1. Der Grundsatz der Öffentlichkeit der Wahl [...] gebietet, dass alle wesentlichen Schritte der Wahl öffentlicher Überprüfbarkeit unterliegen, [...].
2. Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.

dt. BVerfG, 3. März 2009

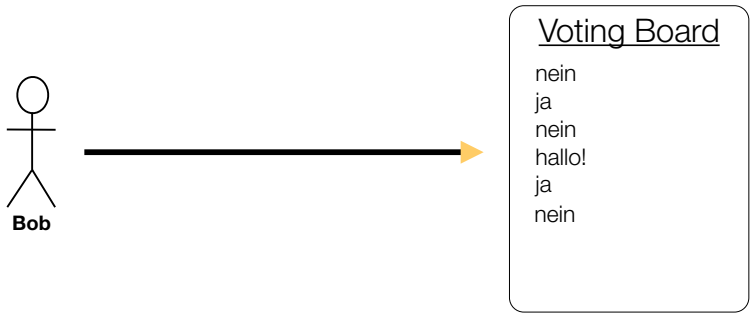
Blackbox E-Voting

“Security by Obscurity”

Transparentes E-Voting

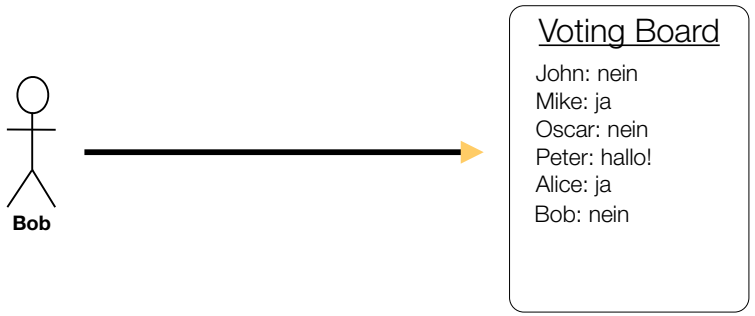
“Security by Transparency”

Bulletin Board I



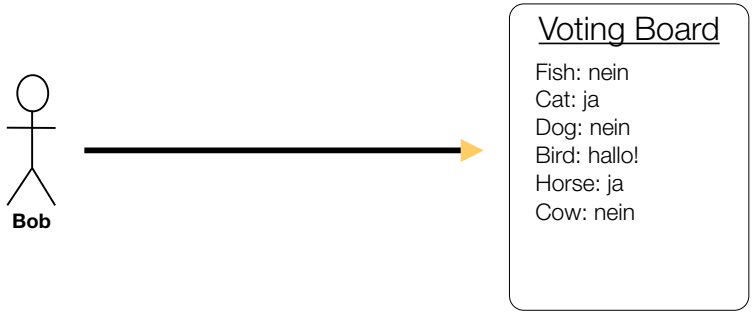
Integrity Soundness Completeness Eligibility Ind.Verifiability
Fairness Anonymity Receipt-Freeness Uniqueness Univ.Verifiability

Bulletin Board II



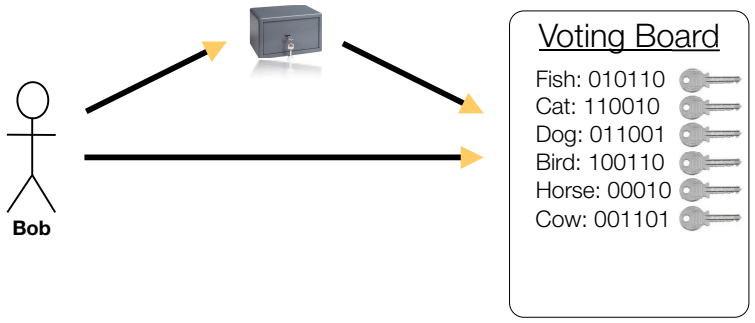
Integrity *Soundness* *Completeness* Eligibility Ind.Verifiability
Fairness *Anonymity* *Receipt-Freeness* Uniqueness *Univ.Verifiability*

Bulletin Board III



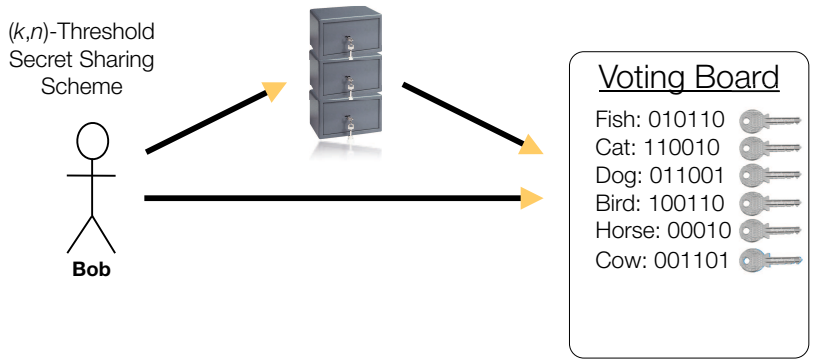
Integrity *Soundness* *Completeness* Eligibility *Ind.Verifiability*
Fairness Anonymity Receipt-Freeness *Uniqueness* *Univ.Verifiability*

Bulletin Board IV



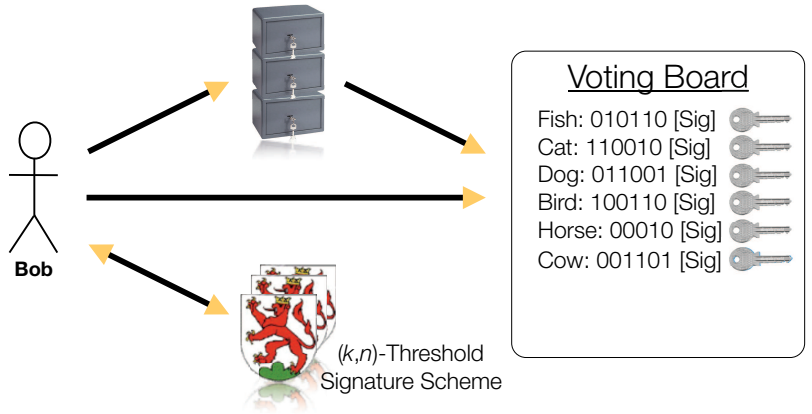
Integrity *Soundness* *Completeness* Eligibility *Ind.Verifiability*
Fairness *Anonymity* Receipt-Freeness Uniqueness *Univ.Verifiability*

Bulletin Board V



Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	*Anonymity*	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

Bulletin Board VI



Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	*Anonymity*	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

Blinde Signaturen

Bei einer blinden Signatur wird eine Nachricht m digital unterschrieben, ohne dass der Unterschreibende die Nachricht sieht

> zuerst wird die Nachricht “versalzen” $\underline{m} = \text{salt}(m,r)$

> die versalzene Nachricht wird signiert $\underline{s} = \text{sign}(\underline{m},d)$

> die versalzene Signatur wird “entsalzen” $s = \text{unsalt}(\underline{s},r)$

> die Signatur kann normal überprüft werden $\text{verify}(m,s,e)$

Dabei muss gelten: $\text{unsalt}(\text{sign}(\text{salt}(m,r),d),r)=\text{sign}(m,d)$

Blinde Signaturen mit RSA

Beim RSA-Verfahren können blinde Signaturen wie folgt generiert werden:

> zuerst wird die Nachricht “versalzen” $\underline{m} = m \times r^e$

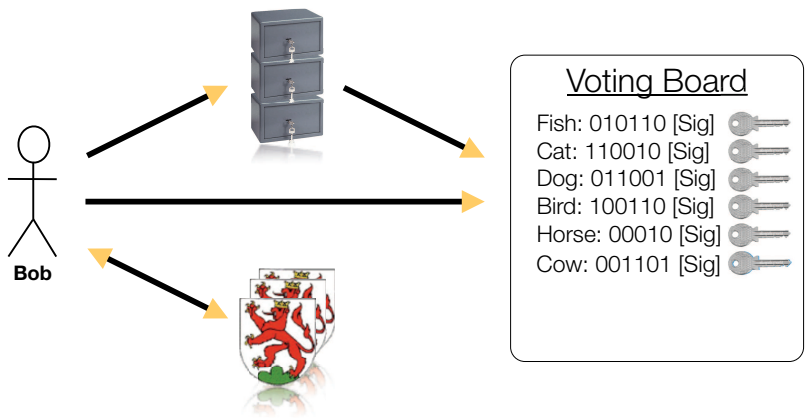
> die versalzene Nachricht wird signiert $\underline{s} = \underline{m}^d$

> die versalzene Signatur wird “entsalzen” $s = \underline{s} \times r^{-1}$

> die Signatur kann normal überprüft werden $m = s^e$?

Dabei gilt: $((m \times r^e)^d) \times r^{-1} = m^d$

Bulletin Board VII



Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	Anonymity	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

Rechtliche Grundlagen

StGB Art. 283: Wahlbestechung

Wer einem Stimmberechtigten ein Geschenk oder einen andern Vorteil anbietet [...] oder zukommen lässt,damit er in einem bestimmten Sinne stimme oder wähle, [...], oder damit er an einer Wahl oder Abstimmung nicht teilnehme,

wer sich als Stimmberechtigter einen solchen Vorteil versprechen oder geben lässt,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Rechtliche Grundlagen

StGB Art. 282bis: Stimmenfang

Wer Wahl- oder Stimmzettel planmässig einsammelt, ausfüllt oder ändert,

wer derartige Wahl- oder Stimmzettel verteilt,

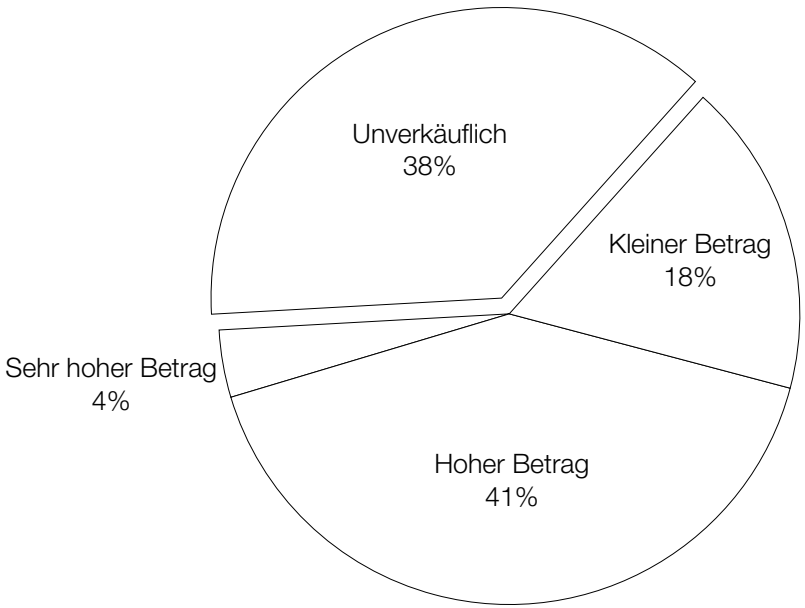
wird mit Busse bestraft.

Umfrage Stimmenkauf I

Nehmen Sie an, Sie erhalten von Ihrer Gemeinde die Zugangsdaten (Username/PIN/etc.), um bei der nächsten eidg. Abstimmung Ihre Stimme elektronisch über das Internet abzugeben.

Stellen Sie sich zudem vor, es gäbe eine Web-Seite, auf welcher Sie Ihre Zugangsdaten diskret (z.B. über Paypal) verkaufen können.

Für welchen Betrag wären Sie bereit, Ihre Zugangsdaten zu verkaufen?

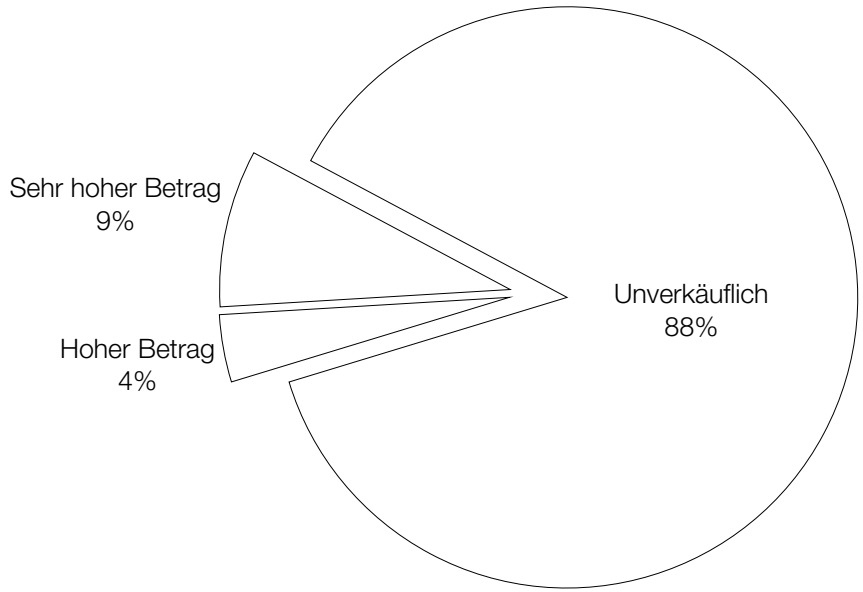


Total: 80 Studierende der Berner Fachhochschule

Umfrage Stimmenkauf

Nehmen Sie an, Sie hätten vom Staat eine elektronische ID (d.h. ein digitales Zertifikat) erhalten, welche Sie für alle zukünftigen elektronischen Abstimmungen einsetzen können, wie auch für alle anderen Online-Dienste der Gemeinde, des Kantons und des Bundes (Führerschein, Steuererklärung, etc.).

Für welchen Betrag wären Sie bereit, Ihre elektronische ID zu verkaufen?



Total: 80 Studierende der Berner Fachhochschule

Vote Updating

Das E-Voting System in Estland erlaubt eine mehrmalige elektronische Stimmabgabe, wobei nur die letzte Stimme zählt

> beim Verkauf der Zugangsdaten kann die verkaufte Stimme durch eine zweite Stimme annuliert werden

> eine unter direktem Zwang abgegene Stimme kann durch eine zweite Stimme annuliert werden

> bei einem quittungsfreien System kann eine verkaufte Stimme durch eine zweite Stimme annuliert werden

Hybrides E-Voting

In einem hybriden E-Voting System kann eine elektronisch abgegebene Stimme durch eine zweite Stimme an der Urne (oder per Briefwahl) annuliert werden

> eine unter direktem Zwang abgegene Stimme kann durch eine zweite Stimme an der Urne annuliert werden

> beim Verkauf der Zugangsdaten kann die verkaufte Stimme durch eine zweite Stimme an der Urne annuliert werden

> ein nicht-quittungsfreies System wird quittungsfrei

Stimmenkauf

Lösungsansätze

1. Der Wähler-Authentifizierung eines E-Voting-Systems sollte mit Hilfe eines digitalen Zertifikates realisiert sein

2. Eine elektronische Stimme sollte entweder
   > durch eine andere elektronische Stimme
   > durch eine Stimme an der Urne
   > durch eine brieflich abgegebene Stimme

   annuliert werden können

Fazit

1. “Security by Transparency” statt “Security by Obscurity”
2. Transparenz mit Hilfe eines Bulletin Boards ermöglicht das individuelle und universelle Verifizieren
3. Blinde Signaturen lösen den Konflikt zwischen genauer Authentifizierung und Anonymität
4. Authentifizierung mitttels elektronischer ID (Zertifikat) reduziert das Risiko des Stimmenverkaufs
5. Vote Updating und hybride Systeme sind gute Lösungs-Ansätze für das Problem des Stimmenkaufs

Schlusswort

“We will work together to ensure the public trust and establish a system of transparency [...].”

Barack Obama, 21. Januar 2009