End-to-End verifizierbare Wahlverfahren in Hinblick auf den Grundsatz der Öffentlichkeit der Wahl

Katharina Hupf, Anastasia Meletiadou
Universität Koblenz-Landau
Universitätsstraße 1
56070 Koblenz
{hupfi | nancy}@uni-koblenz.de

Abstract: Laut dem Urteil des Bundesverfassungsgerichts muss für den Einsatz elektronischer Wahlgeräte gelten, dass „die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können"[BuG]. In diesem Papier werden wir bekannte End-to-End verifizierbare e-Voting-Protokolle in Hinblick auf deren öffentliche Verifizierbarkeit untersuchen. Welche Möglichkeiten hat ein Wähler die Korrektheit seiner Stimmabgabe und der Stimmauszählung zu überprüfen oder sogar eine getätigte Manipulation zu erkennen? Dabei definieren wir Kriterien, die aus den Anforderungen des Bundesverfassungsgerichtsurteils resultieren, wie z.B. die Erfüllung der Integrität der Stimme oder Benutzerfreundlichkeit (Usability), evaluieren die vorgestellten Wahlprotokolle anhand dieser Kriterien und identifizieren mögliche Schwachstellen.

1 Einleitung

Im März diesen Jahres hat das Bundesverfassungsgericht (BVerfG) den Einsatz der Nedap Wahlcomputer (Typ ESD1 und ESD2) bei Bundestagswahlen für verfassungswidrig erklärt. Die Richter begründeten ihr Urteil mit dem Verstoss der eingesetzten Wahlcomputer gegen den Grundsatz der Öffentlichkeit der Wahl. Der Bürger muss laut Urteilsspruch *„die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung"* überprüfen können [BuG]. Auch wenn sich das Urteil des BVerfG explizit auf den Einsatz der Nedap Wahlcomputer im Rahmen von Bundestagswahlen bezieht, kann der Grundsatz der Öffentlichkeit der Wahl als allgemeingültige Anforderung für den zukünftigen Einsatz von Wahlcomputern abgeleitet werden. Dies hat – unabhängig von dem Medium der Wahl (traditionell mit Papier und Stift oder an der Wahlmaschine) – folgende Anforderungen zur Konsequenz:

- Der Wähler muss überprüfen können, dass sein Stimmzettel unverfälscht in die Wahlurne aufgenommen wurde (**Integrität der Stimme**).
- Der Wähler muss überprüfen können, dass die Stimmauszählung korrekt erfolgt ist (**Integrität der Stimmauszählung**).

Der Grundsatz der Öffentlichkeit der Wahl darf andere Wahlgrundsätze jedoch nicht verletzen, insbesondere nicht den Grundsatz der geheimen Wahl. Der Wähler darf somit nicht in der Lage sein, seine Wahlentscheidung gegenüber Dritten zu beweisen (**Anonymität der Stimme**). Ein möglicher Lösungsansatz diese widerstreitenden Anforderungen wie die Anonymität der Stimme und den Grundsatz der Öffentlichkeit der Wahl in Einklang zu bringen, sind *End-to-End (E2E) verifizierbare Wahlverfahren*. Diese Wahlverfahren implementieren Methoden zur Verifikation, dass die abgegebene Stimme dem Wunsch des Wählers entspricht (*cast as intended*), dass die Stimme korrekt abgespeichert wird (*recorded as cast*) und dass die Stimmen korrekt ausgezählt werden (*counted as recorded*) [AN06]. Ein weiterer wichtiger Aspekt bei der Unterstützung des Wählers die Schritte der Wahlhandlung zu verfolgen, ist die **Benutzerfreundlichkeit** eines Systems. Im Rahmen dieses Artikels werden stellvertretend für die Vielzahl an E2E verifizierbaren Wahlverfahren Three Ballot [Riv06], Punchscan [SP06], Bingo Voting [JB07] und Prêt-à-Voter [Rya05] eingehender beleuchtet und entsprechend der Erfüllung der oben genannten Anforderungen untersucht. Die Wahl fiel dabei auf Bingo Voting, da dieses als Sieger des 2. Deutschen IT-Sicherheitspreises 2008 insbesondere in Deutschland eine Vorreiterrolle in Bezug auf E2E-verifizierbare Wahlverfahren einnimmt. Aber auch Punchscan und Prêt-à-Voter sind prominente Vertreter E2E-verifzierbarer Wahlverfahren und werden daher in diesem Artikel betrachtet. Das ThreeBallot-Wahlverfahren wurde untersucht, da es im Gegensatz zu den anderen Wahlverfahren die Anonymität der Stimme ohne Einsatz von Kryptographie gewährleistet.
Dieser Artikel gliedert sich wie folgt: In Kapitel 2 werden zunächst die analysierten Wahlverfahren in ihren Grundzügen erläutert und daraufhin in Kapitel 3 anhand der oben genannten Kriterien evaluiert und insbesondere in Hinblick auf ihre Schwachstellen und den daraus resultierenden Bedrohungen für die Integrität des Wahlvorgangs untersucht. Abschließend werden die Ergebnisse in Kapitel 4 zusammengefasst und bewertet.

2 E2E verifizierbare Wahlverfahren

Im folgenden Abschnitt werden E2E verifizierbare Wahlverfahren vorgestellt. Stellvertretend werden die Systeme Three Ballot [Riv06], Punchscan [SP06], Bingo Voting [JB07] und Prêt-à-Voter [Rya05] in deren Grundzüge betrachtet. Die Verfahren werden entlang der Phasen der Wahlvorbereitung, Stimmabgabe und Wahlnachbereitung analysiert, sofern diese existieren. Für tiefergehende Erläuterungen sei auf die angegebene Literatur verwiesen.

2.1 ThreeBallot [Riv06]

Wahlvorbereitungsphase: Die Stimmzettel werden von der Wahlleitung erzeugt.

Wahl: Der Wähler wählt per Zufall drei Stimmzettel. Diese sind bis auf eine eindeutige Seriennummer identisch und enthalten eine Liste aller Kandidaten in fester Reihenfolge.

Jede Zeile repräsentiert einen Kandidaten. Der Wähler füllt die Stimmzettel nach folgendem Prinzip aus: Stimmt er für einen Kandidaten, so macht er in dieser Zeile genau zwei Kreuze. Stimmt er gegen einen Kandidaten, so macht er in dieser Zeile genau ein Kreuz. Mehr als zwei Kreuze und weniger als ein Kreuz pro Zeile sind nicht erlaubt. Anschließend werden alle drei Stimmzettel von einer Wahlmaschine auf Korrektheit geprüft. Sind die Stimmzettel korrekt ausgefüllt, so wählt der Wähler einen beliebigen der drei Stimmzettel aus und erhält als Beleg eine Kopie von diesem. Die Wahlentscheidung ist anhand des Belegs nicht zu schlußfolgern. Anschließend werden alle drei Stimmzettel in die Wahlurne gegeben.

Wahlnachbereitung: Nach der Wahl werden alle Belege zusammen mit der Anzahl der Personen, die gewählt haben, auf einem Bulletin Board [RC97] veröffentlicht. Der Wähler kann seinen Stimmzettel anhand der Seriennummer identifizieren und überprüfen, ob sein Stimmzettel korrekt gespeichert wurde. Da alle Stimmzettel in unverschlüsselter Form vorliegen, kann darüber hinaus jeder Wähler die Stimmauszählung auf Korrektheit überprüfen.

2.2 Punchscan [SP06]

Wahlvorbereitungsphase: Die Stimmzettel werden von der Wahlleitung erzeugt. Ebenso werden die Informationen zur Auswertung der Stimmzettel bei der Stimmauszählung generiert und mittels Commitments festgeschrieben.

Wahl: Jeder Wähler erhält zwei Stimmzettel mit identischer Seriennummer. Der obere Stimmzettel enthält in beliebiger Reihenfolge eine Zuordnung von Kandidaten zu Symbolen. Der untere Stimmzettel enthält ebenfalls in beliebiger Reihenfolge eine Liste aller Symbole, welche durch Sichtlöcher in dem oberen Stimmzettel sichtbar sind. Die Stimmzettel werden für die Wahl übereinander gelegt und von dem Wähler so ausgefüllt, dass beide Stimmzettel markiert sind. Der Wähler sucht per Zufall einen der beiden Stimmzettel aus. Der ausgesuchte Stimmzettel wird in die Wahlurne gegeben und der Wähler erhält als Beleg eine Kopie von diesem. Der andere Stimmzettel wird vernichtet.

Wahlnachbereitung: Nach der Wahl werden alle Belege auf einem Bulletin Board veröffentlicht. Der Wähler kann seinen Stimmzettel anhand der Seriennummer identifizieren und überprüfen, ob sein Stimmzettel unverfälscht gespeichert wurde. Die Wahlentscheidung ist anhand des Belegs nicht ersichtlich. Für die Stimmauszählung muss der vernichtete Stimmzettel rekonstruiert werden. Anschließend wird die Integrität der Stimmauszählung mittels Mixnets [Cha81] und Partial Random Checking [MJ02] nachgewiesen.

2.3 Bingo Voting [JB07]

Wahlvorbereitungsphase: Für jeden Kandidaten P_i werden l Zufallszahlen $r_1^i, r_2^i, ..., r_l^i$ generiert. Die Anzahl l der pro Kandidat generierten Zufallszahlen entspricht der Anzahl der wahlberechtigten Personen. Anschließend werden Pedersen-Commitments [Ped91] auf alle Tupel (P_i, r_j^i) ausgeführt.

Wahl: Der Wähler wählt an einer Wahlmaschine den gewünschten Kandidaten. Anschließend wird jedem Kandidaten wie folgt eine Zufallszahl zugeordnet: Dem gewählten Kandidaten wird eine Zufallszahl zugeordnet, die während der Wahl von einem zuverlässigen Zufallszahlengenerator erzeugt wird. Den nicht-gewählten Kandidaten werden Zufallszahlen zugeordnet, die vor der Wahl generiert wurden. Der Wähler erhält als Beleg eine Liste aller Kandidaten mit den ihnen assoziierten Zufallszahlen. Die Wahlentscheidung ist anhand des Belegs nicht ableitbar, da nicht ersichtlich ist, welches „alte“ und welches „neue“ Zufallszahlen sind.

Wahlnachbereitung: Nach der Wahl werden alle Belege auf einem Bulletin Board veröffentlicht. Der Wähler kann anhand des Belegs überprüfen, ob sein Stimmzettel korrekt gespeichert wurde und in die Stimmauszählung eingeht. Zusätzlich werden die nicht gebrauchten Commitments sowie das Ergebnis der Stimmauszählung veröffentlicht. Anschließend wird die Korrektheit der Stimmauszählung mittels Zero-Knowledge-Beweis [UF88] nachgewiesen.

2.4 Prêt-à-Voter [Rya05]

Wahlvorbereitungsphase: Die Stimmzettel werden zusammen mit den notwendigen Informationen zur Entschlüsselung der Stimmzettel bei der Auszählung von der Wahlleitung generiert.

Wahl: Jeder Wähler sucht per Zufall einen Stimmzettel aus. Dieser ist zweigeteilt: Die linke Seite enthält die Liste aller Kandidaten in beliebiger Reihenfolge. Auf der rechten Seite markiert der Wähler den von ihm gewünschten Kandidaten. Zusätzlich enthält die rechte Seite des Stimmzettels eine Ballot Onion θ. Diese kodiert die Kandidatenreihenfolge in verschlüsselter Form. Nach getroffener Wahlentscheidung wird der Stimmzettel in der Mitte geteilt. Die linke Seite des Stimmzettels wird vernichtet, die rechte Seite des Stimmzettels wird in die Wahlurne gegeben. Der Wähler erhält als Beleg eine Kopie der rechten Seite des Stimmzettels.

Wahlnachbereitung: Nach der Wahl werden alle Belege auf einem Bulletin Board veröffentlicht. Der Wähler kann anhand des Belegs die korrekte Speicherung seines Stimmzettels überprüfen, ohne dass der Beleg seine Wahlentscheidung offen legt. Für die Auszählung muss die Ballot Onion entschlüsselt werden, um die Kandidatenreihenfolge des Stimmzettels zu rekonstruieren. Dies erfolgt mittels Mixnets, wobei die erfolgreiche Entschlüsselung der Ballot Onion an das Zusammenwirken von k Mixern gekoppelt ist (k-Threshold). Der Nachweis der Korrektheit der Entschlüsselung und Permutation der Stimmzettel sowie der Integrität der Stimmauszählung erfolgt anschließend mittels Mixnets und Partial Random Checking.

3 Systematische Betrachtung von E2E verifizierbaren Wahlverfahren

In diesem Abschnitt werden die in Kapitel 2 genannten E2E verifizierbaren Wahlverfahren bzgl. der Anforderungen betrachtet, die aus dem Grundsatz der Öffentlichkeit der Wahl als Konsequenz resultieren. Ziel ist es, diejenigen Verfahren zu identifizieren, welche den Anspruch erfüllen, der durch das Urteil des BVerfG in Hinblick auf die Nachvollziehbarkeit der Wahl durch den Bürger vorgegeben ist. Es sind folgende Fragestellungen zu beantworten:

- **Funktionale Gewährleistung & Verifikationsmethoden:** Inwiefern gewährleisten die genannten Wahlverfahren die Integrität der Stimmen sowie der Stimmauszählung und welche Verifikationsmethoden nutzen sie dafür?
- **Benutzerfreundlichkeit:** Wie ist die Benutzerfreundlichkeit der Wahlverfahren bzgl. der Verifikation zu bewerten? Wie einfach kann der Wähler die Richtigkeit der Ergebnisse und die Existenz des eigenes Votums überprüfen?
- **Schwachstellen:** Welche Schwachstellen bestehen und welche Bedrohung für die zu schützenden Werte stellen diese dar?

3.1 Funktionale Gewährleistung & Verifikationsmethoden

Integrität der Stimme:
- *ThreeBallot, Punchscan & Prêt-à-Voter:* Der Wähler kann seinen Stimmzettel anhand der Seriennummer auf dem Bulletin Board identifizieren und überprüfen, ob der Stimmzettel korrekt gespeichert wurde.
- *Bingo Voting:* Die Integrität der Stimme wird durch zwei Maßnahmen gewährleistet. Zum Einen überprüft der Wähler, ob die generierte Zufallszahl korrekt an die Wahlmaschine übermittelt und dem richtigen Kandidaten zugeordnet wird, indem er die von dem Zufallszahlengenerator angezeigte Zufallszahl mit der von der Wahlmaschine angezeigten Zufallszahl vergleicht. Zum Anderen werden nach der Wahl alle Belege auf dem Bulletin Board veröffentlicht, so dass der Wähler seinen Stimmzettel anhand der Seriennummer identifizieren und dessen korrekte Speicherung überprüfen kann.

Integrität der Stimmauszählung:
- *ThreeBallot:* Die Stimmzettel liegen in unverschlüsselter Form vor, daher unterliegt die Integrität der Stimmauszählung unmittelbar der öffentlichen Überprüfbarkeit.
- *Punchscan & Prêt-à-Voter:* Die Integrität der Stimmauszählung wird mittels Mixnets und Partial Random Checking gewährleistet.
- *Bingo Voting:* Der Nachweis der Korrektheit der Stimmauszählung erfolgt mittels Zero-Knowledge-Beweis.

3.2 Benutzerfreundlichkeit

Ein weiterer Ansatzpunkt, der den Grundsatz der Öffentlichkeit einer Wahl fördert, ist die Benutzerfreundlichkeit (Usability). Dies beinhaltet Aspekte der Ergonomie wie das einfache Ausfüllen eines Wahlzettels, die Überprüfung der Existenz der eigenen Stimme aber auch die Kontrollierbarkeit des Gesamtergebnisses hinsichtlich seiner Korrektheit.

Ausfüllen der Stimmzettel:
- *ThreeBallot:* Der Wähler muss den gewünschten Kandidaten mit zwei Kreuzen pro Zeile und alle anderen Kandidaten mit einem Kreuz pro Zeile markieren. Diese Regel kann unter Umständen zu Verständnisproblemen führen.
- *Punchscan:* Jeder Wähler erhält zwei Stimmzettel, die zur Stimmabgabe übereinander gelegt werden. Der Wähler muss zunächst auf dem oberen Stimmzettel dasjenige Symbol identifizieren, welches mit seinem Kandidaten assoziiert ist. Anschließend muss er dieses Symbol entsprechend durch eines der Sichtlöcher markieren, so dass anschließend beide Stimmzettel markiert sind.
- *Bingo Voting:* Der Wähler muss die korrekte Übermittlung der neu generierten Zufallszahl von dem zuverlässigen Zufallszahlengenerator an die Wahlmaschine sowie die korrekte Zuordnung dieser Zufallszahl zu dem tatsächlich gewählten Kandidaten überprüfen. Dies kann je nach Länge der verwendeten Zufallszahl Probleme bei der Verwendung von Bingo Voting in der Praxis verursachen.
- *Prêt-à-Voter:* Die Benutzerfreundlichkeit beim Ausfüllen des Stimmzettels ist ein großer Vorteil von Prêt-à-Voter. Die Stimmabgabe erfolgt analog zur Papierwahl durch einfaches Ankreuzen des gewünschten Kandidaten.

Überprüfung der Integrität der Stimmauszählung:
- *ThreeBallot:* Die Stimmzettel liegen in unverschlüsselter Form. Die Korrektheit der Stimmauszählung kann daher ohne besondere Sachkenntnisse nachvollzogen werden.
- *Punchscan & Prêt-à-Voter:* Der Nachweis der Integrität der Stimmauszählung basiert auf dem Einsatz von Mixnets und Partial Random Checking. Die Nachvollziehbarkeit des Beweises kann daher als kritisch betrachtet werden.
- *Bingo Voting:* Die Integrität der Stimmauszählung wird mittels Zero-Knowledge-Beweis nachgewiesen. Auch hier kann die Nachvollziehbarkeit des Beweises als kritisch angesehen werden.

3.3 Schwachstellen

In Hinblick auf das Urteil des BVerfG lassen sich die Integrität der Stimme und die Integrität der Stimmauszählung als zu schützende Werte einer Wahl identifizieren. Bei allen vorgestellten Verfahren wurden in der Vergangenheit Sicherheitsanalysen durchgeführt und Schwachstellen identifiziert oder auch Annahmen für eine korrekte Durchführung einer Wahl getroffen. An dieser Stelle möchten wir aufgrund des Umfangs der Papers das Bingo Voting bzgl. der Integrität und Verifizierbarkeit auf eventuelle Schwachstellen untersuchen. Eine Manipulation der Stimmauszählung wird mit Hilfe des Zero-Knowledge-

Beweis mit hinreichend hoher Wahrscheinlichkeit aufgedeckt und die Integrität der Stimmauszählung somit geschützt. Der Fokus der nachfolgenden Betrachtungen liegt daher auf der Integrität der Stimme als zu schützenden Wert. Die Integrität der Stimmen hängt beim Bingo Voting in hohem Maße von der Zuverlässigkeit des Zufallszahlengenerators ab. Dies wird daher wie folgt in [JB07] als wesentliche Voraussetzung für das Bingo Voting identifiziert: *„The key assumption to ensure correctness is a trusted random number generator attached to the voting machine“*. Im Folgenden wird eine Schwachstelle des Bingo Votings aufgezeigt, welche auf einer Manipulation des Zufallszahlengenerators basiert und auf die Integrität der Stimmen abzielt. Da diese trotz Zero-Knowledge-Beweis unentdeckt bleibt, stellt dies einen direkten Widerspruch zu dem Urteil der BVerfG dar.
Trifft der Wähler seine Wahlentscheidung so wird statt der vom Zufallszahlengenerator neu erzeugten Zufallszahl eine Zufallszahl angezeigt, die in der Wahlvorbereitungsphase für diesen Kandidaten generiert und festgeschrieben wurde. Diese wird dem gewählten Kandidaten zugeordnet. Demjenigen Kandidaten, zu dessen Gunsten die Wahl manipuliert werden soll, wird nun die tatsächlich neu erzeugte Zufallszahl zugeordnet. Da die Anzeige manipuliert ist, bleibt dieser Austausch von Zufallszahlen von dem Wähler unentdeckt.
Nach Beendigung der Wahl werden alle Belege zusammen mit den nicht gebrauchten und aufgedeckten Commitments auf dem Bulletin Board veröffentlicht. Anschließend erfolgt ein Zero-Knowledge-Beweis über die Integrität der Stimmauszählung. Dazu wird C_{left} auf dem Bulletin Board veröffentlicht. C_{left} beinhaltet die Liste aller Kandidaten sowie Commitments auf alle Zufallszahlen des Wahlbelegs. Eine (geheime und zufällige) Permutation der Reihenfolge garantiert dabei die Wahrung des Wahlgeheimnis. Anhand von C_{left} ist lediglich erkennbar, dass der Stimmzettel genau eine tatsächliche Stimme und ansonsten nur Füllstimmen enthält. Der Austausch der Zufallszahlen ist somit nicht erkennbar. Die Commitments von C_{left} werden anschließend zu neuen Commitments maskiert und in permutierter Reihenfolge auf dem Bulletin Board veröffentlicht ($= C_{middle}$). Der letzte Schritt wird wiederholt und ebenfalls auf dem Bulletin Board veröffentlicht ($= C_{right}$). C_{right} wird nun aufgedeckt. Jeder Kandidat sowie alle Zufallszahlen des Wahlbelegs müssen genau einmal, jedoch in permutierter Reihenfolge vorkommen. Dies ist trotz der Manipulation des Stimmzettels der Fall. Anschließend wird für jedes Commitment von C_{middle} per Zufall entschieden, ob das korrelierende Commitment von C_{left} oder von C_{right} aufgedeckt wird. Da das Wahlgeheimnis gewahrt bleiben muss und somit nie ganze Pfade aufgedeckt werden dürfen, bleibt die Manipulation des Stimmzettels weiterhin unentdeckt.
Ein solcher Angriff auf die Integrität der Stimmen kann jedoch mit einfachen Mitteln unterbunden werden:

1. Der Wähler kann einen eigenen Zufallszahlengenerator mitbringen. Dies birgt jedoch die Gefahr, dass dieser Zufallszahlengenerator ebenfalls manipuliert ist und somit Erpressung und Stimmenkauf ermöglicht.

2. Der Wähler addiert auf die vom Zufallszahlengenerator erzeugte Zufallszahl eine beliebige Zahl x auf. Im Falle der oben beschriebenen Manipulation hätte dies zur Konsequenz, dass pro Stimmzettel zwei Commitments nicht verwendet würden und dies bei dem Zero-Knowledge-Beweis und der Erstellung von C_{left} aufgedeckt würde. Erpressung und Stimmenkauf wären jedoch weiterhin möglich, da der

Wähler gezwungen werden könnte, für einen bestimmten Kandidaten per Addition eine vorher vereinbarte Zahl zu generieren.

3. Zur Vermeidung von Erpressung und Stimmenkauf kann der in 2. beschriebene Lösungsansatz dahingehend modifiziert werden, dass der Wähler eine beliebige Zahl x auf die neu erzeugte Zufallszahl addiert. Die Zahl x darf jedoch nur aus einem beschränkten Wertebereich stammen.

4 Fazit

In diesem Papier haben wir E2E verifizierbare Wahlprotokolle auf die Einhaltung des Wahlgrundsatzes der Öffentlichkeit untersucht. Alle Verfahren wurden bzgl. ihrer Methoden zur Gewährleistung der Integrität der Stimme und der Stimmauszählung betrachtet. Bezugnehmend auf das Urteil des BVerfG wurde besonderer Wert auf die Benutzerfreundlichkeit und Nachvollzierbarkeit dieser Methoden von Seiten des Wählers gelegt. Hier sind unsere Ergebnisse eindeutig: Auch wenn diese Systeme die geforderten Anforderungen (Wähler erhalten eine Quittung, Quittung ist kein Beweis für den Inhalt, Wähler können feststellen, dass ihre Stimmen berücksichtig wurden und die Auszählung korrekt ist) nach Expertenwissen erfüllen, sind diese für den Wähler ohne besondere Sachkenntnisse kaum überprüfbar und nachvollziehbar, da diese auf Verifikationsmethoden wie Mixnets, Partial Random Checking und Zero-Knowledge-Beweisen beruhen. Wir haben exemplarisch eine Schwachstelle des Bingo Voting, aber auch entsprechende Lösungen präsentiert, die diese Wissenslücke der Wähler nutzen, um das Wahlergebnis zu manipulieren. In weiteren Arbeiten sollen auch für die übrigen vorgestellten Verfahren ähnliche Schwachstellenanalysen vorgenommen werden.

Literatur

[AN06] B. Adida und C.A. Neff. Ballot Casting Assurance. *In EVT 06, Proceedings of the First Usenix/ACCURATE Electronic Voting Technology Workshop, Vancouver, Canada*, 2006.

[BuG] Bundesverfassungsgericht, 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1-163).

[Cha81] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communication of the ACM*, 24(2), 1981.

[JB07] S. Röhrich J.M. Bohli, J. Müller-Quade. Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator. In *VOTE-ID*, Seiten 111–124, 2007.

[MJ02] R. Rivest M. Jakobsson, A. Juels. Making mix nets robust for electronic voting by randomized partial checking. *In USENIX Security Symposium*, Seite 339353, 2002.

[Ped91] T.P. Pedersen. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *CRYPTO*, Seiten 129–140, 1991.

[RC97] B. Schoenmakers R. Cramer, R. Gennaro. A Secure and Optimally Efficient Multi-Authority Election Scheme. *Advances in Cryptology - Eurocrypt'97, LNCS 1233*, Seiten 103–118, 1997.

[Riv06] R.L. Rivest. The ThreeBallot Voting System, 2006.

[Rya05] P.Y.A. Ryan. Prêt-à-Voter: a System Perspective. Bericht, Technical Report CS-TR: 929, School of Computing Science, Newcastle University, 2005.

[SP06] B. Hosp S. Popoveniuc. An Introduction to Punchscan. *IAVoSS Workshop on Trustworthy Elections (WOTE), June 2006, Cambridge, UK und VSRW 06, Washington, DC*, 2006.

[UF88] A. Shamir U. Feige, A. Fiat. Zero Knowledge Proofs of Identity. *Journal of Cryptology*, 1(1):77–94, 1988.