Die Infrastruktur für die elektronische Stimmabgabe über das Internet

Alexander Prosser

Institut für Informationsverarbeitung und Informationswirtschaft,
Wirtschaftsuniversität Wien
Augasse 2–6, A-1090 Wien
alexander.prosser@wu-wien.ac.at

Schlagworte: elektronische Stimmabgabe, elektronische Demokratie, e-Voting

Abstract: Die Stimmabgabe über das Internet ist zu einer realen Möglichkeit geworden. Der Beitrag untersucht die verschiedenen Realisierungsvarianten und deren Anforderungen an die Infrastruktur des Wahlsystems unter Berücksichtigung der Einhaltung der Wahlrechtsgrundsätze.

1. Einleitung

Internetwahlen (e-Voting) sind zu einer realen Möglichkeit geworden, es müssen aber die Grundsätze der allgemeinen, gleichen, unmittelbaren, persönlichen, geheimen und freien Wahlen eingehalten werden [WaMe82, 93f]. Im Folgenden wird e-Voting immer als remote e-Voting über das Internet verstanden – Systeme zur Automation der Wahlzelle oder remote e-Voting über andere Medien (zB SMS) sind nicht Gegenstand der Überlegungen. Das Internet Policy Institute hat speziell im Hinblick auf e-Voting daraus folgende Forderungen abgeleitet [IPI01, 7ff]: (i) korrektes Zählen der Stimmen, (ii) unehrliche Wähler können die Wahl nicht stören, (iii) permanente Anonymität, (iv) jeder Wähler kann nur einmal, gleich in welcher Form, ob konventionell oder mit e-Voting, wählen, (v) nur authorisierte Wähler können wählen, (vi) Unabhängigkeit (keine unstatthafte Einwirkung auf den Wähler), (vii) Nachvollziehbarkeit, (viii) Quittungsfreiheit (um Stimmenkauf zu vermeiden).

Den Grundsatz der persönlichen Stimmabgabe kann in bestimmten Wahlordnungen noch hinzukommen.

Für das Design eines kryptographischen Algorithmus lassen sich daraus drei Hauptforderungen zusammenfassen:

- Eindeutige Identifizierung des Wahlberechtigten bei gleichzeitig vollkommen gesicherter Anonymität in der Stimmabgabe.

- Außerdem darf die Systemadministration der Wahlbetreiber keinerlei Möglichkeit haben (i) die Anonymität zu unterlaufen oder (ii) Stimmen zu manipulieren.

Hinzu kommt die Sicherung der vom Wählenden verwendeten Infrastruktur gegen Viren, Trojaner und andere Schadprogramme. In allen diesen Funktionalitäten spielen digitale Signaturkarten eine wesentliche Rolle. Bevor auf diese eingegangen wird, ein kurzer Abriss der Realisierungsvarianten von e-Voting-Systemen.

2. Realisierungsvarianten

2.1. Nichtkryptographische Verfahren

An nichtkryptographischen Verfahren kommen PIN- bzw TAN-basierte Verfahren zum Einsatz. Derartige Verfahren wurden bereits bei der Wahl zum Hohen Rat der Auslandsfranzosen 2003 [Con03] und bei einem Referendum in der Gemeinde Anières im Kanton Genf 2003 [Hen00] eingesetzt. Dabei wird ein PIN/TAN an die Wahlberechtigten per Post geschickt. Der Wahlberechtigte kann diesen Code dann für die Authentisierung im Wahlsystem und die Abgabe einer Stimme nutzen. Schwachstellen bei diesem Verfahren sind der Postversand der Codes und die rein organisatorische Sicherung gegen Unterlaufen der Anonymität durch die Administratoren bzw Betreiber des Wahlsystems; eine technische Garantie dagegen besteht nicht (vgl dazu die Diskussion in [PrMü02]). Vorteile sind die rasche Implementierbarkeit und die vergleichsweise geringen Anforderungen an die Infrastruktur beim Wählenden. Auch kann das Versenden konventioneller Briefwahlkarten und der PIN Codes miteinander verbunden werden, wie dies in Anières auch geschehen ist [CdE03].

2.2. Kryptographische Verfahren – einstufig

Der Wahlakt – auch bei papierbasierter Wahl – besteht aus einem Identifizierungsschritt, bei dem Identität und Wahlberechtigung geprüft werden, und der eigentlichen Stimmabgabe. Ein System zur elektronischen Stimmabgabe besteht aus eben diesen Schritten, wobei diese in einer Benutzersitzung (einstufig) oder in getrennten Sitzungen (mehrstufig) durchgeführt werden können (vgl *Nurmi* et al [NSS91]).

2.2.1. Anonymer Kanal

Diese e-Voting Prototypen gehen zurück auf den Vorschlag von *Chaum*'s MIX Netzen [Cha81], bei der die ursprüngliche Nachricht mit den öffent-

lichen Schlüsseln mehrerer Server verschlüsselt wird, dann von einem Server an den anderen überreicht und von jedem mittels dessen privaten Schlüssel dechiffriert wird. Anschließend wird die Nachricht an den jeweils nächsten Server in der Reihe mit einer anderen Reihenfolge (dies ist der entsprechende MIX Vorgang) weitergereicht. Dieser Ansatz – den Chaum für einen vollkommenen anderen Einsatzbereich vorgesehen hat – weist mehrere strukturelle Probleme in Zusammenhang mit e-Voting auf:

- Zumindestens einer der MIX-Server muss vertrauenswürdig sein; wenn die Zahl der Server laufend erhöht wird, wird das Protokoll langsamer und fehleranfälliger.
- Die Lösung stellt hohe Anforderungen an die Infrastruktur, die während der Wahltage benötigt wird.
- Um Mixer am Einschleusen von manipulierten Stimmen in den Mixer Prozess zu hindern, muss ein Mechanismus gefunden werden, um die Stimme zu authentisieren. Dies kann durch zwei Ansätze realisiert werden – entweder durch eine blinde Signatur nach [Cha87] von einen Dritten, dem vertraut wird, oder die Stimme wird durch den Wähler verschlüsselt und der Schlüssel wird zur Dechiffrierung später eingesendet.

Erweiterungen des ursprünglichen Protokolls wurden von *Park* et al [PIK94] und von *Sako* und *Kilian* [SaKi95] gefunden. Allerdings konnten beide Protokolle gebrochen werden [Pf89, HoMi96]. Spätere Versuche durch *Abe* [Abe98] und *Jakobsson* [Jak98, Jak99] trugen neben algorithmischen Verbesserungen vor allem zur Stabilität und zur Geschwindigkeit des Protokolls bei. Ebenso wurde der Verarbeitungsaufwand auf der Seite des Wählers (Client) drastisch reduziert (ein gemeinsamer Schlüssel anstelle von mehreren Schlüsseln); diese Verbesserungen müssen dennoch erst analysiert und in Prototypimplementierungen getestet werden, um zu sehen, ob die grundlegenden Schwierigkeiten in MIX Netzen komplett gelöst wurden.

2.2.2. Homomorphismus

Die Stimme wird bei diesem Verfahren in einer binären Ja/Nein-Darstellung der Stimme repräsentiert und in einem homomorphen Schema chiffriert. Dann wird die Stimme an mehrere Wahlurnen übermittelt. Aufgrund der Eigenschaft des Homomorphismus ist es möglich, die Ja/Nein-Stimmen zu summieren ohne die individuellen Stimmen zu kennen [CGS97]. Dieser Vorteil ist auch das Hauptproblem des Ansatzes, denn es können nur binäre Stimmen abgebildet werden. Es wäre natürlich denkbar, die Auswahl einer Partei mittels einer Serie von Ja/Nein-Entscheidungen abzubilden. Dies impliziert aber die Prüfung, dass nur ein Eintrag als Ja ausge-

wählt wird. Weiters bleibt es fragwürdig, ob ein solches Protokoll entsprechend skalierbar wäre.

2.2.3. Blinde Signatur

Der Blinde-Signatur-Mechanismus [Cha87] kann in Verbindung mit MIX Netzwerken verwendet werden, um die Authentisierung einer Stimme zu ermöglichen, nachdem sie einen MIX Kanal durchlaufen hat oder als Abbildung in einem eigenständigen Wahlprotokoll. Die blinde Unterschrift kann hier entweder auf den Stimmzettel oder eine blind unterschriebene Wahlkarte aufgebracht werden, mit der dann der Stimmzettel anonym abgegeben werden kann.

Der bekannteste Ansatz dazu ist sicherlich der von *Fujioka*, *Okamoto* und *Ohta* [FOO93], der auch mehrfach implementiert wurde. Publizierte Implementierungen können in [Riv99] und [CC97] gefunden werden. Dieses Protokoll hat, trotz seiner Popularität, einige fundamentale Probleme in Bezug auf die Anonymität des Wählers und das Einschleusen falscher Stimmen für Nichtwähler von Seiten der Administration. Für eine umfangreiche Kritik siehe [PrMü02]. Das Problem der Einschleusen falscher Stimmen wurde von [BPS94] mit der Einführung von Pseudonymen für die Wähler adressiert. Diese Pseudonyme werden durch einen anonymen Kanal an alle Registrierungsserver geschickt, mit denen dann die Stimme authentisiert werden kann. Dies fügt eine beträchtliche Komplexität zu dem Protokoll und der Artikel äußert sich auch nicht näher über den notwendigen anonymen Kanal; dieser wäre ein entsprechender Ansatz für weitere Forschungsvorhaben. In einer anderen Erweiterung durch *Okamoto* [Oka96] wird das Problem durch mehrere Blind Signature Server angegangen. Die Problematik der Anonymität wird durch die Verwendung eines MIX Netzwerks gelöst, was die oben erwähnten Einschränkungen aufwirft.

2.3. Kryptographische Verfahren – mehrstufig

2.3.1. All-or-nothing disclosure of secrets (ANDOS)

ANDOS-Protokolle bieten einen anonymen Senderkanal. Sie emulieren dabei den anonymen Kauf eines Bitstrings [BCR87]. Folglich kann dieses Protokoll für ein- und zwei-phasige Protokolle verwendet werden. *Nurmi* et al [NSS91] und *Salomaa* [Sal91] haben die Ausgabe von Wahlkarten mittels ANDOS vorgeschlagen, die dann für die anonyme Stimmabgabe benutzt werden können. Verbesserungen des Protokolls in Bezug auf die Effizienz und Komplexität wurden von *Niemi* [Nie94] sowie *Hassler* und *Posch* [HaPo95] vorgeschlagen. Die Hauptnachteile von ANDOS-Proto-

kollen sind ihre beschränkte Skalierbarkeit und die Möglichkeit des Stimmenkaufs, da der Wähler selbst nachweisen kann, wie er gewählt hat.

2.3.2. Protokoll von Prosser und Müller

Prosser und *Müller-Török* [PrMü01, 02] schlugen ebenfalls ein auf der blinden Signatur basierendes Protokoll vor, wo im Unterschied zu den oben erwähnten Protokollen eine Wahlkarte und nicht der Stimmzettel blind unterschrieben wird. Ähnlich zu [Oka96] wird ein zweiter Blinde-Signatur-Server verwendet, die Anonymität ist jedoch nicht von Mixern abhängig. Das Protokoll schützt die Wahl vor korrupten Wählern, die den Wahlablauf stören wollen, als auch vor einer korrupten Wahladministration, die Stimmen einschleusen will. Die Anonymität wird insbesondere durch die strikte Trennung zwischen der Registrierung und der eigentlichen Stimmabgabephase gesichert.

3. Kritische Elemente im System

3.1. Sicherung der Anonymität

Die Anonymität kann dann durchbrochen werden, wenn eine Beziehung zwischen den Identifikationsdaten und der Stimme des Wahlberechtigten hergestellt werden kann; dies kann über (i) die Reihenfolge, (ii) die Herkunft (zB die IP Adresse eines Rechners) oder (iii) andere Merkmale erfolgen. Einstufige Verfahren, wie sie in Abschnitt 2.2 geschildert wurden, mögen auf der kryptographischen Ebene durchaus die Anonymität sicherstellen, da jedoch Identifizierung und Stimmabgabe in einem Schritt erfolgen, kann hier eine Sicherung auf Betriebssystem- bzw Netzwerkebene nicht garantiert werden. Es scheint zweifelhaft, ob dieses Problem zufriedenstellend lösbar ist.

Zweistufige Verfahren hingegen trennen die identifizierten Funktionen im Wahlsystem von der anonymen Stimmabgabe und haben daher dieses Problem nicht. Sie werfen aber das Problem der Zwischenspeicherung einer Berechtigungsinformation („Token", „elektronische Briefwahlkarte" etc) auf. Diese Zwischenspeicherung muss nicht nur sicher erfolgen, sondern auch sicherstellen, dass über die Speicherung nicht wiederum identifizierende Informationen über den Benutzer ausgelesen werden können (siehe dazu die Diskussion in [KKPU03]).

3.2. Wahlkommission

Die wichtigsten Aufgaben der Wahlkommission im konventionellen Wahlsystem sind es, die Identifizierung der Wahlberechtigten zu überwachen,

die Urnen nach der Wahl zu öffnen und die Stimmen im jeweiligen Sprengel auszuzählen. Die Wahlkommission ist damit ein wesentliches Element des Vertrauens für die Wählenden.

Im elektronischen System kann die Wahlkommission durchaus analoge Aufgaben übernehmen. Im System von *Prosser* et al [PKKU03, 04b] generieren die Mitglieder der Wahlkommission asymmetrische Schlüsselpaare, wovon vor der Wahl der öffentliche Teil bekannt gegeben wird; der private Teil verbleibt beim jeweiligen Kommissionsmitglied bzw wird bei einer Stelle des Vertrauens hinterlegt. Die abgegebenen Stimmen werden beim Wähler mit diesen Schlüsseln codiert und sind somit für niemanden (auch nicht die Serveradministration des Wahlsystems oder einzelne Mitglieder der Wahlkommission) lesbar. Nach Ende der Wahl stellen die Mitglieder der Wahlkommission ihre geheimen Schlüsselteile zur Verfügung und erst dann sind die Stimmen decodier- und damit lesbar.

Nachteil dieses Systems ist, dass alle Kommissionsmitglieder ihre Schlüssel zur Verfügung stellen müssen, damit die Stimmen lesbar werden. Dies bringt Probleme bei Sabotageversuchen einer einzelnen politischen Gruppe (bzw dessen Vertreter in der Wahlkommission), bei Unfällen, Verlust des Speichermediums, aber auch bei der Abbildung von Mehrheitsentscheidungen, dort wo diese durch die Rechtsordnung vorgesehen sind, mit sich.

In einem Vorschlag von [PKU04] wird ein kryptographischer Mechanismus für die Abbildung von Mehrheitsentscheidungen vorgeschlagen. Damit sind beliebige Quoren (auch Minderheiten) definierbar, für die die Stimmzettel lesbar sind, auch wenn nicht alle Schlüssel zur Verfügung gestellt werden.

3.3. Schutz gegen böswillige Software

Es bedarf keiner Begründung, warum Viren, Trojaner und andere Schadprogramme ein Problem gerade für den Wahlprozess darstellen. So könnten Schadprogramme benutzt werden, die Anonymität zu unterlaufen, die Wahl zu sabotieren oder Stimmen zu manipulieren (vgl die Diskussion in [Rub04]). Eine Lösung ist das Auslagern der sensiblen Teile eines Wahlsystems in eine zertifizierte Signaturkarte, wobei der PC des Wählenden eine reine „Datensichtstation" wird und die entscheidenden Protokollteile in der Karte ablaufen.

3.4. Signaturkarten

Die Wahlordnungen der österreichischen Hochschülerschaft und der Wirtschaftskammer sehen bereits heute e-Voting vor (§74 WKG bzw §34 HSG); beide verlangen die Authentisierung durch eine Bürgerkarte [Pos03].

Signaturkarten haben jedoch auch zwei andere wesentliche Rollen in einem elektronischen Wahlsystem.

Wie in Abschnitt 3.1 dargelegt, sind zweistufige Verfahren der vermutlich am ehesten gangbare Weg, die Anonymität in der Stimmabgabe sicherzustellen. Dies erfordert jedoch die Zwischenspeicherung der anonym einsetzbaren Berechtigungsfunktion; hier bietet sich die Signaturkarte als sicheres Speichermedium an. Die Übernahme dieser Rolle setzt aber zwei wesentliche Eigenschaften der Signaturkarte voraus:

(i) Die Berechtigungsinformation muss PIN-geschützt auf der Karte speicherbar sein und (ii) eine Applikation, die die Berechtigungsinformation ausliest, darf keinen Zugriff auf die identifizierenden Teile der Karte (Zertifikat, Kartennummer etc) erhalten – beide Domänen müssen also strikt getrennt werden.

Wie in Abschnitt 3.3 dargestellt, ist eine Signaturkarte auch ein geeignetes Medium, die entscheidenden Teile des kryptographischen Wahlprotokolls zu rechnen, da sie eine sichere und unangreifbare Rechenumgebung darstellt. Dies bedingt aber, dass der Befehlssatz der Karte die Operationen, die das Protokoll benötigt, auch durchführen kann (vgl die Analyse des Befehlssatzes in [PKK04a]).

4. Akzeptanz

Elektronische Wahlen sind ein hochreglementierter und sensibler Prozess, dessen elektronische Abbildung höchste Anforderungen an Sicherheit, Reliabilität und Transparenz stellt. Ein System zur elektronischen Stimmabgabe wird nur dann Akzeptanz bei den Wählenden erringen, wenn es diese Anforderungen erfüllt.

Literaturverweise

[Abe98] *Abe M.*: Universally Verifiable Mix-Net with Verification Work Independent of the Number of Mix-Centers. In: Advances in Cryptology – EUROCRYPT '98, Springer-Verlag, Berlin 1998, S 437–447.

[BCR87] *Brassard G., Crepeau C., Robert J.-M.*: All-or-Nothing Disclosure of Secrets. In: Lecture Notes in Computer Science 263, Advances in Cryptology; Crypto 86, Berlin, Springer-Verlag, 1987, S 234–238.

[BPS94] *Baraani-Dastjerdi A., Pieprzyk J., Safavi-Naini R.*: A Practical Electronic Voting Protocol Using Threshold Schemes. In: Center f. Computer Security Research, Department of Computer Science, University of Wollongong, Australia 1994.

[CEG00] Chancellerie d'Etat de Genève: Cahier des charges e-voting. http://www.geneve.ch/chancellerie/e-government/cahier_charges.html (5. 3. 2003).

[Cha81] *Chaum D.*: Untraceable electronic mail return addresses and digital pseudonyms. In: Communications of the ACM, Vol 24(2), 1981, S 84–88.

[Cha87] *Chaum D.*: Blinding for Unanticipated Signatures. In: Chaum David; Price, Wyn (Eds.): Advances in Cryptology, EUROCRYPT '87, Springer-Verlag, Berlin 1987, S 227–233.

[CC97] *Cranor L. F., Cytron R. K.*: Sensus: A Security-Conscious Electronic Polling System for the Internet. In: Proceedings of the Hawai International Conference on System Sciences (HICSS-97). Hawaii 1997. http://lorrie.cranor.org/pubs/hicss/hicss.html (4. 2. 2001).

[CdE03] Chancellerie d'Etat de la République et du Canton de Genève; Résultats du vote du 19 janvier 2003 à Anières (GE); http://www.geneve.ch/chancellerie/E-government/doc/Rapport_Final9.pdf.

[CGS97] *Cramer R., Gennaro R., Schoenmakers B.*: A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Advances in Cryptology-EUROCRYPT'97, Lecture Notes in Computer Science 1233, Springer-Verlag, Berlin 1997, S 103–118.

[Con03] Conseil Supérieur des Français à l'Étranger; Elections 2003; http://www.csfe.org/elections/index.htm?http://www.csfe.org/elections/elections_300403.htm~pages (4. 5. 2004)

[FOO93] *Fujioka A., Okamoto T., Ohta K.*: A Practical Secret Voting Scheme for Large Scale Elections. In: Advances in Cryptology – AUSCRYPT92. Springer-Verlag, Berlin 1993, S 244 –251.

[HaPo95] *Hassler V., Posch R.*: A LAN voting protocol. In: IFIP/SEC '95, Capetown 1995, S 154–167.

[Hen00] *Hensler R.*: Cahier des charges d'un système du vote par Internet; http://www.geneve.ch/chancellerie/E-Government/cahier_charges.html (4. 5. 2004)

[HoMi96] *Horster P., Michels M.*: Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme. In: Asiacrypt'96, LNCS 163, Springer-Verlag, Berlin 1996, S 125–132.

[IPI01] Internet Policy Institute: Report on the National Workshop on Internet Voting, Issues and Research Agenda. The Internet Policy Institute, Washington (DC) 2001. http://www.internetpolicy.org/research/e_voting_report.pdf (20. 11. 2001).

[Jak98] *Jakobsson M.*: A Practical Mix. In: Advances in Cryptology – EUROCRYPT '98, Springer-Verlag, Berlin 1998, S 448–461.

[Jak99] *Jakobsson M.*: Flash Mixing. In: Information Sciences Research Center, Bell Labs, New Jersey, http://www.bell-labs.com/user/markusj (19. 11. 2002).

[KKPU03] *Kofler R., Krimmer R., Prosser A., Unger M.*: Two-Stage Internet Voting: Advantages and Difficulties. Proceedings of the e-Government Workshop in conjunction of the 16th International Conference on Legal Knowledge and Information Systems, Amsterdam 2003.

[Nie94] *Niemi V.*: Cryptographic protocols and voting. In: Results and Trends in Theoretical Computer Science, Springer LNCS, Springer-Verlag, Berlin 1994, S 307–316.

[NSS91] *Nurmi H., Salomaa A., Santean L.*: Secret ballot elections in computer networks. In: Computers and Security 36 (1991) 10, S 553–560.

[Oka96] *Okamoto T.*: An Electronic Voting Scheme: IFIP'96, Advanced IT Tools, Chapman and Hall, London 1996, S 21–30.

[Pf89] *Pfitzmann B., Pfitzmann* A.: How to Break the Direct RSA-Implementation of Mixes. In: Eurocrypt 89, Springer-Verlag, Berlin 1989, S 373–381.

[PIK94] *Park C., Itoh K., Kurosawa K.*: All/Nothing Election Scheme and Anonymous Channel. In: Lecture Notes in Computer Science 765, Advances in Cryptology Eurocrypt 93, Berlin, Springer-Verlag 1994, S 248–259.

[PKK03] *Prosser A., Kofler R., Krimmer R.*: Deploying Electronic Democracy for Public Corporations. In: DEXA/EGOV 2003, Prague 2003.

[PKKU03] *Prosser A., Kofler R., Krimmer R., Unger M.*: Die erste Internet-Wahl Österreichs / The first internet-election in Austria. Working Paper 04/2003 des Institut für Informationsverarbeitung und -wirtschaft der Wirtschaftsuniversität Wien 2003.

[PKKU04a] *Prosser A., Kofler R., Krimmer R., Unger M.*: The Role of Digital Signature Cards in Electronic Voting. Proceedings of 37th Annual Hawaii International Conference on System Sciences (CD/ROM), Computer Society Press, 2004.

[PKKU04b] *Prosser A., Kofler R., Krimmer R., Unger M.*: e-Voting Wahltest zur Bundespräsidentschaftswahl 2004, Arbeitsbericht zum Tätigkeitsfeld Informationsverarbeitung und Informationswirtschaft 01/2004, Wirtschaftsuniversität Wien 2004.

[PKU04] *Prosser A., Kofler R., Unger M.K.*: Quroum-based Decisions in an Election Committee; accepted for DEXA 2004.

[Pos03] *Posch R.*: Das Konzept der Bürgerkarte light. Chief Information Office, Wien 2003.

[PrMü01] *Prosser A., Müller-Török R.*: Electronic Voting via The Internet. In: 3rd International Conference on Enterprise Information Systems ICEIS-2001, Setubal 2001, S 1061–1066.

[PrMü02] *Prosser A., Müller-Török R.*: E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. In: Wirtschaftsinformatik 44 (2002) 6, S 545–556.

[Riv99] *Rivest R.*: Cryptography and Information Security Group Research Project: e-Voting. In: http://theory.lcs.mit.edu/~cis/voting/voting.html (19. 11. 2001).

[Rub04] *Kohno T., Stubblefield A., Rubin A., Wallach D.*: Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy, Oakland 2004.

[SaKi95] *Sako K., Kilian J.*: Receipt-Free, Mix-Type Voting Scheme. In: Lecture Notes in Computer Science 921, Advances in Cryptology Eurocrypt 95, Berlin, Springer-Verlag 1995, S 393–403.

[Sal91] *Salomaa A.*: Verifying and Recasting Secret Ballots in Computer Networks. In: Maurer, H.A. (Eds): New Results and New Trends in Computer Science, Springer-Verlag, Berlin 1991, S 283–289.

[WaME82] *Walter R., Mayer H.*: Grundriß des österreichischen Bundesverfassungsrechts; Manz Verlag, Wien 1982.