Effiziente elektronische Wahlen mit Observer

Jörn Schweisgut

Justus-Liebig-Universität Gießen
Joern.Schweisgut@math.uni-giessen.de

Abstract:
Das größte Problem elektronischer Wahlsysteme ist das der Unüberprüfbarkeit (receipt-freeness). Sie wurde im System von Magkos, Burmester und Chrissikopoulos [MBC01] und kürzlich im System von Schweisgut [Sch05] mit Hilfe einer manipulationssicheren Hardware, eines Observers, realisiert.

In dieser Arbeit wird ein allgemeines Wahlsystem mit Unüberprüfbarkeit vorgestellt, das ebenfalls einen Observer zur Stimmabgabe verwendet, aber effizienter als die bekannten Systeme ist. Insbesondere wird der Wahlaufwand auf Seiten des Wählers so gering wie möglich gehalten.

Das System von Magkos et. al gewährleistet nicht die Unabhängigkeit der Stimmabgabe. Diese Lücke wurde bisher nicht aufgegriffen, so dass wir in dieser Arbeit das Problem aufzeigen und mit Hilfe des Einsatzes einer non-malleable Verschlüsselung lösen.

Key words: Elektronische Wahlen, Unüberprüfbarkeit, Observer.

1 Einleitung

Bei der eidgenössischen Volksabstimmung am 27.11.2005 konnten erstmals Stimmberechtigte des Kantons Zürich ihre Stimme elektronisch abgeben. Dies stellt nur ein Beispiel dar, das den immer breiter werdenden Trend zu elektronischen Wahlen verdeutlicht. Im Unterschied zu elektronischen Wahlmaschinen, wie sie unter anderen in den USA eingesetzt werden, geht es in dieser Arbeit darum, dem Wähler die Abstimmung über elektronische Netze, wie dem Internet, zu ermöglichen. Die Vorteile des Einsatzes elektronischer Medien liegen in der sicheren, robusteren und schnelleren Auszählung der Stimmen sowie im möglichen Anstieg der Wahlbeteiligung durch schnelleren, einfacheren und bequemeren Zugang zur Abstimmung.

Es gibt viele elektronische Wahlprotokolle, aber nur wenige erfüllen die komplexen Anforderungen. Die Anforderung, die sich bisher als am schwierigsten zu realisieren herausgestellt hat, ist die der Unüberprüfbarkeit. Ein Wahlsystem, in dem es nicht möglich ist, dass ein Wähler einen Beleg über die von ihm abgegebene Stimme erstellen kann, heißt unüberprüfbar. Die Möglichkeit, beweisen zu können, für welche Wahloption man sich entschieden hat, ist kein gewünschtes Feature - im Gegenteil. Kann ein Wähler einen solchen Beleg erstellen, so kann ein Erpresser oder Bestecher diesen auch von ihm verlangen.

1.1 Frühere Arbeiten

Der Begriff der Unüberprüfbarkeit wurde zuerst von Benaloh und Tuinstra in [BT94] verwendet. Ihr System, wie auch die meisten anderen Systeme, die versuchen, die Stimme allein mit probabilistischer homomorpher Verschlüsselung geheimzuhalten, gewährleistet jedoch keine Unüberprüfbarkeit. Der Wähler, der die Zufallszahl zur Verschlüsselung wählt, kann diese als Beleg für seine Stimme dem Angreifer zur Verfügung stellen. Andere Wahlsysteme, wie das von Hirt und Sako [HS00] sowie der effizientere Ansatz von Baudron et. al [BFP+01], erreichen Unüberprüfbarkeit, allerdings mit unrealistischen Annahmen, wie eines physikalisch sicheren Kanals von jeder Autorität des Wahlausschusses zu jedem Wähler. Die Unüberprüfbarkeit in diesen Systemen geht im Falle korrupter Autoritäten verloren.

Das erste System, das Unüberprüfbarkeit unter realistischeren Annahmen mit Hilfe des Einsatzes manipulationssicherer Hardware, sogenannter Observer (vgl. [CP92], [CP93]) erzielen sollte, ist das von Magkos et al. [MBC01]. Es hat sich jedoch herausgestellt, das ein in diesem System verwendeter Zero-Knowledge-Beweis nicht simulierbar und daher übertragbar ist und somit als Beleg für die Stimmentscheidung dienen kann. Im Anschluss an diesen Beweis muss der Wähler gegenüber dem Wahlausschuss beweisen, dass die von ihm und dem Observer erstellten Geheimtexte Verschlüsselungen gültiger Wahloptionen darstellen. Magkos et. al sprechen auch hier von *einem* Beweis, der bei genauerer Betrachtung aber für alle Wahloptionen durchgeführt wird. Darüber hinaus ist das vorgeschlagene Beweisprotokoll ebenfalls nicht effizient simulierbar, besitzt daher auch nicht die Zero-Knowledge-Eigenschaft. Das stellt keine Schwächung der Anonymität oder Unüberprüfbarkeit dar. Der beschriebene Beweis ist vielmehr ein interaktiver Witness-Indistinguishable Beweis (WI-Beweis) (siehe [FS90]). Die beschriebenen Lücken wurden in [Sch05] geschlossen, das System erweitert und effizienter gestaltet. Das System von Magkos et. al weist aber noch eine weitere Schwachstelle auf, die Unabhängigkeit der Stimmabgabe. In einer demokratischen Wahl darf es nicht möglich sein, dass Wähler Stimmen anderer Wähler als ihre eigenen ausgeben, bzw. Stimmen abgeben, die mit Stimmen anderer Wähler in einer bekannten Relation stehen.

1.2 Motivation, Zielsetzung und Aufbau dieser Arbeit

In Abschnitt 2 stellen wir zunächst ein allgemeines Wahlsystem vor, das allen bisher bekannten Anforderungen an demokratische elektronische Wahlen entspricht. Das Wahlsystem basiert auf dem Einsatz von Observern, ist aber effizienter als die o.g. Wahlsysteme mit Observer. Insbesondere ist der Wahlaufwand auf Seiten des Wählers minimal. Anschließend konstruieren wir darauf aufbauend in Abschnitt 3 ein konkretes, effizientes Wahlprotokoll mit Observer und analysieren es. Die Ergebnisse werden in Abschnitt 4 zusammengefasst.

1.3 Intuition hinter unserem Wahlsystem

In unserem Wahlsystem setzen wir eine non-malleable Verschlüsselung ein. Der Wähler muss zusammen mit dem Observer für jeden erstellten Geheimtext beweisen, dass er die zur Verschlüsselung verwendete Zufallszahl kennt. Ein Angreifer kann dann keinen von einem anderen Wähler abgegebenen Geheimtext als seine Stimme abgeben oder ihn so abzuwandeln, dass die beiden zugrundeliegenden Klartexte in einer dem Angreifer bekannten Relation stehen. Somit ist die Unabhängigkeit der Stimmabgabe gewährleistet.

Im Gegensatz zum System [Sch05] verwenden wir in unserem System keine Witness-Indistinguishable-Beweise, dass die von Wähler und Observer erstellten Geheimtexte wirklich Verschlüsselungen gültiger Wahloptionen sind. Das stellt auf Seiten des Wählers eine enorme Vereinfachung dar. Andererseits kann nun nicht mehr die Homomorphie der Verschlüsselungsfunktion verwendet werden um die Geheimtexte zusammenzufassen und dann das Auszählungsergebnis zu entschlüsseln. Die abgegebenen Stimmen müssen einzeln entschlüsselt werden. Dabei muss der Zusammenhang zwischen dem Wähler und der Stimme unkenntlich gemacht werden. Dies geschieht mittels eines verifizierbaren, robusten Entschlüsselungs-MIX-Netzwerkes, welches die abgegebenen Stimmen zufällig permutiert im Klartext ausgibt. Es kann nun leicht überprüft werden, ob die Klartextstimmen gültige Wahloptionen sind. Anschließend werden die gültigen Stimmen einfach ausgezählt.

Eine wesentliche Annahme für die Unüberprüfbarkeit in Systemen mit Observern ist die Manipulationssicherheit des Observers. Wenn er durch einen Angreifer vor der Ausgabe manipuliert werden kann, so dass er die gewählten und berechneten Werte nicht löscht und später dem Angreifer zugänglich macht oder die Zahlen nicht zufällig, sondern vom Angreifer festgelegt sind, kann der Angreifer vom Wähler einen Beleg fordern. Unter der Annahme der Manipulationssicherheit genügt es, dass nur die Stimme des Wählers und nicht alle Wahloptionen von Wähler und Observer verschlüsselt werden. Das erhöht die Effizienz auf Seiten des Wählers und verhindert den sogenannten Randomisations-Angriff (siehe Abschnitt 4).

2 Sichere Wahlsysteme mit Observer

Die Wahlsysteme [MBC01] und [Sch05] haben den Nachteil, dass jeder Wähler für alle Wahloptionen einen WI-Wiederverschlüsselungsbeweis durchführen muss. Darüber hinaus liegt der Aufwand bei einer Wahl mit n Wahlberechtigten und n_L Wahloptionen für die Auszählung bei $O(\sqrt{n^{n_L-1}})$, wenn man den Baby-Step-Giant-Step-Algorithmus verallgemeinert anwendet. In diesem Abschnitt wird ein Observer-basiertes Wahlsystem mit Unüberprüfbarkeit vorgestellt, das die Kommunikation zwischen Wahlausschuss und Wählern auf ein Minimum reduziert.

Damit nur gültige Stimmen in die Auszählung eingehen, müssen die Geheimtexte entschlüsselt und erst dann verrechnet werden. Sie durchlaufen ein robustes,

verifizierbares MIX-Netz (siehe z.B. [DK00]), um die Anonymität der Stimmen sicherzustellen. Wählt man als MIX-Netz ein System, das die Nachrichten beim Durchlauf entschlüsselt, so ist die Ausgabe des MIX-Netzes die Liste der gewählten Klartextstimmen. Nun kann überprüft werden, ob sie gültigen Wahloptionen entsprechen. Ungültige Stimmen werden ignoriert, gültige einfach ausgezählt.

2.1 Beteiligte Instanzen und Wahlablauf

Es gibt eine Registrierungsstelle, n Wahlberechtigte, n_L Wahloptionen, ein schwarzes Brett und ω Autoritäten im Wahlausschuss, deren Rolle durch die Server $A_1, \ldots, A_\omega$ eines verifizierbaren, robusten Entschlüsselungs-MIX-Netz übernommen werden. Sie berechnen einen gemeinsamen öffentlichen Schlüssel in einem (t, ω)-Schwellensystem ohne ihre geheimen Schlüsselanteile zu veröffentlichen (siehe z.B. [Ped91]). Durch das Schwellensystem können nur t oder mehr Autoritäten zusammen eine mit ihrem gemeinsamen öffentlichen Schlüssel verschlüsselte Stimme entschlüsseln. Die öffentlichen Parameter werden auf den Observern gespeichert.

Registrierung: Die Wähler $V_1, \ldots, V_n$ begeben sich in das Registrierungsbüro, authentifizieren sich und erhalten ihren Observer.

Sie wählen sich ein zufälliges Geheimnis und berechnen einen öffentlichen Anteil zu diesem Wert, der ebenfalls auf dem Observer gespeichert wird. Diese Werte werden zur Erstellung des Designated-Verifier-Beweises benötigt, mit denen der Observer dem Wähler bei der Stimmerzeugung nachweist, korrekt gearbeitet zu haben.

Auf dem Observer wird der geheime Signaturschlüssel des Wählers bzw. Observers und ein zugehöriges Pseudonym gespeichert, während der dazu gehörende öffentliche Schlüssel zusammen mit dem Pseudonym auf einer Liste der Wahlberechtigten geführt wird. Der Wähler kennt den geheimen, durch den Observer physikalisch geschützten Signaturschlüssel nicht. Der Schlüssel kann höchstens dann von einem Angreifer verwendet werden, wenn dieser in den Besitz des Observers kommt.

Wahl: Jeder Wähler verschlüsselt seine Stimme probabilistisch unter dem öffentlichen Schlüssel des Wahlausschusses und sendet den Geheimtext an den Observer. Außerdem schickt er die Werte an den Observer, die dieser zur Konstruktion seines Teils des Zero-Knowledge-Beweises der non-malleability benötigt. Der Observer verschlüsselt den Geheimtext ebenfalls probabilistisch unter dem öffentlichen Schlüssel des Wahlausschusses. Er berechnet die Werte, die der Wähler zur Erstellung des Beweises der non-malleability benötigt. Die Werte sendet er an den Wähler und beweist mittels eines Designated-Verifier Beweises, korrekt gearbeitet zu haben (siehe z.B. [JSI96]). Der Wähler lässt den Observer die verschlüsselte Wahloption und den Beweis der non-malleability signieren, prüft die Signatur und schickt alles an das schwarze Brett. Nach der Berechnung der Signatur ist das Protokoll für den Observer abgeschlossen und er löscht alle berechneten Werte. Selbst wenn der Observer nun einem Angreifer in die Hände fällt, der die physikalische Sicherheit des Observers überwindet, kann er keine Informationen daraus entnehmen.

Das schwarze Brett ist ein öffentlich zugänglicher Speicher, den jeder lesen und an den jeder Daten anhängen kann. Jedoch kann keiner gespeicherte Daten löschen oder verändern. Die Zero-Knowledge-Beweise und die Signaturen sind mit Hilfe der Liste der wahlberechtigten Pseudonyme global verifizierbar, d.h. jeder kann die Wahlberechtigungen und die Unabhängigkeit der Stimmabgaben überprüfen.

Auszählung: Nach Beendigung der Wahlphase werden die Signaturen überprüft. Stimmen mit ungültigen Signaturen und Stimmen ohne gültigen Zero-Knowledge-Beweis der Kenntnis der zur Verschlüsselung verwendeten Zufallszahlen werden ignoriert. Entsprechend einer Policy wird pro Wahlberechtigten nur eine Stimme, z.B. die erste abgegebene gültige, gewertet. Um die Reihenfolge der vom Wähler veröffentlichten Stimmen festzulegen, werden die auf dem schwarzen Brett eintreffenden Stimmen mit einem Zeitstempel versehen. Die nach diesen Überprüfungen verbliebenen Geheimtexte durchlaufen eine verifizierbare Entschlüsselungs-MIX-Kaskade (siehe z.B. [DK00]). Die vom MIX-Netz ausgegebenen Klartexte werden auf Gültigkeit überprüft und die gültigen Stimmen werden öffentlich ausgezählt.

2.2 Anforderungen

Dem Wahlsystem können verschiedene kryptografische Primitive zugrunde liegen. Dabei müssen sie folgende Grundanforderungen erfüllen:

- *Non-malleablility:* Das verwendete Kryptosystem muss non-malleable sein (vgl. [DDN00], [PS96]), damit es einem Angreifer nicht möglich ist, abgegebene Stimmen zu kopieren oder so modifiziert als seine eigene abzugeben, dass die Klartexte in einer dem Angreifer bekannten Relation stehen. Andernfalls wäre die Unabhängigkeit der Stimmabgabe nicht gewährleistet.

- *Probabilistische Wiederverschlüsselung:* Um die Unüberprüfbarkeit zu ermöglichen, benötigt man einen probabilistischen Wiederverschlüsselungsalgorithmus R, so dass die Wiederverschlüsselung über der Menge der möglichen Chiffretexte gleichverteilt ist.

- *Existenz eines Designated-Verifier-Wiederverschlüsselungsbeweises:* Es wird ein effizienter Designated-Verifier-Beweis benötigt (vgl. [JSI96]), der zeigt, dass ein Geheimtext eine Wiederverschlüsselung eines anderen darstellt.

- *Kenntnis des geheimen Schlüssels:* Jeder Wähler wählt einen öffentlichen Schlüssel, wobei sichergestellt werden muss, dass er seinen zugehörigen privaten kennt. Dies ist essentiell für die Designated-Verifier-Eigenschaft des Beweises und somit für die Unüberprüfbarkeit des Wahlsystems.

- *Observer:* Jeder Wähler besitzt eine manipulationssichere Hardware, einen Observer, der in der Lage ist, R, den Designated-Verifier-Beweis und mit dem Wähler zusammen die Zero-Knowledge-Beweise der non-malleability durchzuführen. Auf dem Observer muss dazu der Public-Key des Wahlausschusses,

der öffentliche Schlüssel des Wählers und der Signaturschlüssel „des Wählers" gespeichert sein. Der Wähler darf diesen Signaturschlüssel nicht kennen, da er sonst ohne den Observer Stimmen erzeugen könnte. Der Observer muss mit Hilfe des Signaturschlüssels qualifizierte digitale Signaturen erstellen können. Nach der Übermittlung der Signatur an den Wähler soll der Observer alle gewählten und berechneten Werte löschen (vgl. 2.3).

- *Existenz eines schwarzen Brettes:* Die Stimmen werden an ein schwarzes Brett geschickt, auf dem jeder Leserechte und das Recht besitzt, Daten anzuhängen, aber keiner über das Recht verfügt, Daten zu löschen oder zu ändern.

- *Sicherheit der Verschlüsselung:* Der Wahlausschuss besteht aus $\omega \geq t$ Personen. Für jede Gruppe von weniger als t Personen des Wahlausschusses muss es unmöglich sein, einen Chiffretext zu entschlüsseln.

- *Verifizierbares, robustes Entschlüsselungs-MIX-Netz:* In der Auszählungsphase wird ein MIX-Netz benötigt, das die Geheimtexte der Wahlberechtigten verifizierbar entschlüsselt und so permutiert, dass der Zusammenhang zwischen dem Wähler und der Stimme nicht mehr nachvollziehbar ist. Die MIX-Server besitzen jeweils einen Anteil am geheimen Schlüssel des MIX-Netzes. Es darf nicht möglich sein, dass ein Zusammenschluss von weniger als t MIX-Servern die Stimmen entschlüsselt. Die Ausgabe des MIX-Netzes sind die abgegebenen entschlüsselten Stimmen in zufälliger Reihenfolge. Das MIX-Netz sollte robust sein, damit es leicht möglich ist, bis zu $\omega - t$ korrupte MIX-Server zu erkennen und auszuschließen.

- *Stimmabgabe in virtueller Wahlkabine:* Die Kommunikation zwischen Observer und Wähler darf nicht durch Angreifer überwacht werden können. Wähler und Observer befinden sich sozusagen in einer virtuellen Wahlkabine.

2.3 Vertrauensmodell - Anforderungen an den Observer

Die Unüberprüfbarkeit wird in diesem System durch den Einsatz des Observers sichergestellt. Entsprechend den in [CP92] und [CP93] formulierten Anforderungen kommuniziert dieser während der Wahlphase nur mit bzw. über den Wähler. Der Wähler kontrolliert alle ausgehenden Nachrichten. Der Observer beweist dem Wähler in einem Designated-Verifier Beweis die korrekte Verschlüsselung. Während der Wahl kann der Wähler also alle Aktionen des Observers kontrollieren.

Der Observer könnte aber nach der Wahl in fremde Hände gelangen. Es muss vorausgesetzt werden, dass der Observer manipulationssicher ist, der Angreifer also nicht an die Informationen des Observers gelangen kann. Dies ist eine Annahme, die für die Unüberprüfbarkeit von Wahlsystemen mit Observern unabdingbar ist. Obgleich sie ein sehr großes Vertrauen in den Observer fordert, ist diese Forderung erheblich schwächer als die eines physikalisch sicheren Kanals von jeder Autorität zu jedem Wähler, wie es in [HS00] gefordert ist. Wir gehen in diesem Wahlsystem

davon aus, dass der Observer die zur Stimmerzeugung gewählten und berechneten Werte sofort nach dem Senden seiner signierten Nachricht an den Wähler löscht und der Angreifer nicht in der Lage ist, den Observer vor der Wahl so zu manipulieren, dass dieser die Zufallszahlen zur Verschlüsselung nicht zufällig wählt.

3 Eine effiziente, Observer-basierte Wahl mit Unüberprüfbarkeit

Im Folgenden wird ein konkretes Beispiel eines effizienten Observer-basierten Wahlsystems mit Unüberprüfbarkeit beschrieben und untersucht.

3.1 Wahlvorbereitungs- und Registrierungsphase

Die MIX-Server bestimmen zusammen eine multiplikative Gruppe G mit Primzahlordnung $|G| =: q$ und ein erzeugendes Element g von G. Dann erzeugen sie gemeinsam ein ElGamal-Schlüsselpaar (s, h) mit $h = g^s$ (vgl. [Ped91]), so dass jede Person des Wahlausschusses A_j einen Anteil s_j von s in einem $(t, n)-$Schwellensystem erhält und öffentlich darauf über $h_j = g^{s_j}$ festgelegt wird. h wird als öffentlicher Schlüssel des Wahlausschusses bekannt gegeben und auf den Observern gespeichert.

Jeder Wahlberechtigte V_i, $(i = 1, \ldots, n)$, wird vom Wahlausschuss benachrichtigt und begibt sich zum Registrierungsbüro, wo er nach einer geeigneten Authentifikation einen Observer ausgehändigt bekommt.

Der Wähler wählt sich ein zufälliges Geheimnis $z_V \in_R \mathbb{Z}_q$ und berechnet $h_V = g^{z_V}$ als öffentlichen Anteil des Wertes z_V. Dieser Wert h_V wird ebenfalls auf dem Observer gespeichert. Wichtig ist, dass der Observer z_V selbst nicht kennt.

Auf dem Observer ist neben dem öffentlichen Schlüssel des Wahlausschusses und dem Wert h_V noch das Pseudonym id_V des Wählers und der geheime Signaturschlüssel des Observers gespeichert. Der dazu gehörende öffentliche Schlüssel befindet sich auf einer Liste der wahlberechtigten Signaturen.

3.2 Wahlphase

Da die Stimmen durch das MIX-Netz entschlüsselt und am Ende einzeln im Klartext ausgegeben werden, kann eine Darstellung der Wahloptionen gewählt werden, die durch einfache Addition gültiger Klartextstimmen das Auszählungsergebnis ermittelt. Daher werden die Wahloptionen in einem Zahlensystem zur Basis n beschrieben. Da n die Anzahl der Wähler ist, kann es nur dann zu keiner Stellenüberschreitung kommen, wenn alle Wähler die gleiche Wahloption wählen. Sei also $\mathbf{L} = (m_1, \ldots, m_{n_L}) = (1, n, n^2, \ldots, n^{n_L-1})$ die Menge der Wahlmöglichkeiten, dann kann man leicht die Anzahl der Stimmen für jede Wahlmöglichkeit berech-

nen, wenn die Summe der Stimmen berechnet wurde. Da in diesem System Wähler und Observer nicht nachweisen müssen, dass sie gültige Wahloptionen verschlüsselt haben, benötigt man in diesem Wahlsystem im Unterschied zu [HS00], [MBC01] oder [Sch05] auch keine Standardverschlüsselung der Stimmen.

Jeder Wähler wählt sich Zufallszahlen $a, a' \in_R \mathbb{Z}_q$ und verschlüsselt seine Stimme m aus $\mathbf{L}$: $(x, y) = (g^a, h^a m)$. Des Weiteren berechnet er $g^{a'}$. Die Werte sendet der Wähler an den Observer.

Der Observer wählt Zufallszahlen $b, b' \in \mathbb{Z}_q$ und verschlüsselt den Geheimtext erneut: $(x', y') = (g^b g^a, h^b h^a m)$. Er berechnet $g^{a'+b'}$ und den für die non-malleability notwendigen Wert $b \cdot H(g, x', y', g^{a'+b'}, id_V) + b'$. Dabei liefert die kryptografische Hashfunktion H die Challenge für den nicht-interaktiven Zero-Knowledge Beweis der non-malleability.

Der Observer sendet $(x', y', g^{a'+b'}, b \cdot H(g, x', y', g^{a'+b'}, id_V) + b', id_V)$ an den Wähler. Hat er korrekt gearbeitet, kann der Wähler daraus (g^b, h^b) berechnen. Den Beweis der non-malleability bzw. Unabhängigkeit kann der Wähler nun fertigstellen: $(a+b)H(g, x', y', g^{a'+b'}, id_V) + (a'+b')$. Die non-malleable ElGamal-Nachricht ist dann $E(m) = (x', y', g^{a'+b'}, (a+b)H(g, x', y', g^{a'+b'}, id_V) + (a'+b'), id_V)$. Ohne Kenntnis der zur Verschlüsselung verwendeten Zufallszahlen a und b lässt sich diese Nachricht nicht erstellen (vgl. [TY98]).

Um das Maß des Vertrauens, dass der Wähler dem Observer entgegen bringen muss, möglichst gering zu halten, beweist der Observer mittels eines Designated-Verifier-Beweises (siehe z.B. [JSI96]), dass er korrekt verschlüsselt hat. Der Wähler lässt den Observer die verschlüsselte Wahloption und den Zero-Knowledge-Beweis der non-malleability signieren (siehe z.B. [Sch91]), prüft die Signatur und schickt dies alles an das schwarze Brett.

Das schwarze Brett ist öffentlich lesbar, d.h. die Signaturen sind mit Hilfe der Liste der öffentlichen Verifikationsschlüssel der Wahlberechtigten global verifizierbar. Ebenfalls sind die Zero-Knowledge-Beweise global verifizierbar, d.h. jeder kann die Wahlberechtigungen und die Unabhängigkeit der Stimmabgaben überprüfen.

3.3 Auszählungsphase

Nach Beendigung der Wahlphase werden die Signaturen überprüft. Stimmen mit ungültigen Signaturen und Stimmen ohne gültigen Zero-Knowledge-Beweis der Kenntnis der zur Verschlüsselung verwendeten Zufallszahlen werden ignoriert. Pro Wahlberechtigten wird nur eine Stimme, z.B. die erste gültige, gewertet. Die nach diesen Überprüfungen verbliebenen Geheimtexte durchlaufen eine verifizierbare Entschlüsselungs-MIX-Kaskade (vgl. [DK00]). Bei den von dem MIX-Netz ausgegebenen Klartexten wird überprüft, ob sie aus $\mathbf{L}$ stammen. Schließlich werden die gültigen Stimmen öffentlich ausgezählt, d.h. addiert.

3.4 Analyse des Wahlsystems

3.4.1 Wahlberechtigung, Fälschungssicherheit, Einmaligkeit

Die Überprüfung der Wahlberechtigung und die Fälschungssicherheit der Stimmen wird durch die digitale Signatur sichergestellt. In der Registrierungsphase werden die öffentlichen Signaturschlüssel der Wahlberechtigten auf einer Liste zertifiziert. Mit Hilfe der Zertifikate kann jeder feststellen, welche Nachrichten von Wahlberechtigten signiert wurden. Unberechtigt abgegebene Nachrichten werden nicht berücksichtigt. Die Fälschungssicherheit der Stimmen leitet sich direkt von der Fälschungssicherheit der digitalen Signatur ab.

Wenn nur die zuerst veröffentlichten Stimmen mit korrekter Signatur in das MIX-Netz eingehen und später veröffentlichte Stimmen der gleichen Wähler für ungültig erklärt und verworfen werden, wird durch die Verifizierbarkeit des MIX-Netzes sichergestellt, dass jeder Wähler nur einmal seine Stimme abgeben kann. Die Einmaligkeit basiert auf der Fälschungssicherheit des verwendeten Signaturschemas.

3.4.2 Verifizierbarkeit

Da das schwarze Brett öffentlich lesbar ist, kann jeder die Signaturen und Zero-Knowledge-Beweise überprüfen. Während der Auszählungsphase durchlaufen die Stimmen das MIX-Netzwerk. Anschließend liegen die abgegebenen Stimmen im Klartext vor und sind öffentlich auszählbar. Das bedeutet, dass sich die Verifizierbarkeit des Wahlverfahrens aus der Verifizierbarkeit des MIX-Netzes ergibt.

3.4.3 Korrektheit

Die Korrektheit der Auszählung ist garantiert, wenn alle Wähler die Stimme ihrer Wahl abgeben können, also jeweils die Korrektheit der Verschlüsselung durch den Observer nachvollziehen können. Dies wird durch die Designated-Verifier-Beweise, die Verifizierbarkeit des MIX-Netzes und die öffentliche Auszählbarkeit der Klartextstimmen gewährleistet.

3.4.4 Ehrlichkeit, Robustheit

Ein unehrlicher Wähler kann keine ungültige Stimme in die Auszählung einfließen lassen, da diese am Ende des MIX-Netzes im Klartext vorliegt und ignoriert wird.

Die Verifizierbarkeit der Aktionen der MIX-Server ermöglicht es, betrügerische Autoritäten zu identifizieren und auszuschließen. Solange höchstens $\omega - t$ Personen des MIX-Netzes unehrlich sind, kann die Wahl mit Ausschluss dieser MIX-Server durchgeführt werden. Daher ist das Wahlverfahren robust.

3.4.5 Wahlaufwand

Die Komplexität der Kommunikation hängt natürlich stark von den verwendeten Beweisen, also vom Designated-Verifier-Beweis und vom Zero-Knowledge-Beweis der Unabhängigkeit ab. Diese Beweise sind effizient durchführbar und der Kommunikationsaufwand ist sowohl unabhängig von der Anzahl der Autoritäten als auch von der Anzahl der Wahloptionen!

Da im Unterschied zu [MBC01] und [Sch05] kein Wiederverschlüsselungsbeweis für alle Wahloptionen durchgeführt werden muss, ist der Aufwand auf Seiten des Wählers entscheidend geringer. Darüber hinaus muss pro Wähler nur die Stimme und nicht jede Wahloption verarbeitet werden.

3.4.6 Wahlgeheimnis, Anonymität

Die Anonymität eines jeden Wählers ist garantiert, wenn die verschlüsselte Stimme nicht durch eine außenstehende Person oder Gruppe von weniger als t Personen des Wahlausschusses entschlüsselt werden kann. Dies trifft für dieses Wahlsystem zu.

Nur jemand, der das Pseudonym eines Wählers kennt, kann feststellen, ob er eine Stimme abgegeben hat. Erst eine Menge von mindestens t MIX-Servern kann die Entschlüsselung der Wahloptionen vornehmen, um festzustellen, wie ein einzelner Wähler gewählt hat. Solange nicht mehr als $t - 1$ Personen des Wahlausschusses kooperieren, ist die Anonymität durch die Sicherheit des Verschlüsselungsverfahrens gewährleistet.

3.4.7 Unabhängigkeit

Es ist nicht möglich, eine Stimme eines anderen Wählers zu kopieren, da man für die verschlüsselte Wahloption einen Zero-Knowledge-Beweis liefern muss, die zur Verschlüsselung verwendete Zufallszahl zu kennen. Durch diese Non-malleable-Eigenschaft ist es nicht möglich, Stimmen abzugeben, die in einer dem Angreifer bekannten Korrelation zu Stimmen anderer Wähler stehen.

3.4.8 Unüberprüfbarkeit

Das Wahlsystem ist unüberprüfbar, d.h. es ist nicht möglich, dass der Wähler einen Beleg erstellen kann, wie er gewählt hat. Die Unüberprüfbarkeit in diesem System basiert auf dem Einsatz des Observers, der einen Teil der zur Verschlüsselung verwendeten Zufallszahl generiert. Diese Zufallszahl ist dem Angreifer und sogar dem Wähler unbekannt und kann daher auch nicht als Beleg für die abgegebene Stimme gelten. Der Designated-Verifier-Beweis ist nicht übertragbar. Aufgrund der Annahme, dass der Observer manipulationssicher ist, hat ein Angreifer also keine Möglichkeit, an die Werte des Observers zu gelangen. Somit hat der Wähler keine Möglichkeit, andere beweisbar davon zu überzeugen, welche Wahloption in seinem Geheimtext verborgen ist.

4 Zusammenfassung und Fazit

Das Wahlsystem erfüllt alle angegebenen Anforderungen einschließlich der Unüberprüfbarkeit. Es verzichtet auf unrealistische Annahmen wie physikalisch sichere Kanäle von jedem Wähler zu jeder Person im Wahlausschuss. Die Annahme, dass es dem Angreifer nicht gelingt, den Observer vor der Wahl, d.h. auch vor der Ausgabe durch die Registrierungsstelle zu manipulieren, verlangt ein großes Maß an Vertrauen vom Wähler in den Observer. Der Aufwand für einen solchen Angriff liegt aber deutlich höher als wenn man dem Wähler direkt über die Schulter sähe. Diese Möglichkeit eines Angriffs gibt es bereits heute bei der Briefwahl.

Der Aufwand auf Seiten des Wählers sollte bei einer Wahl möglichst gering gehalten werden. Insbesondere da Observer naturgemäß Operationen nicht besonders performant ausführen, sollten nur notwendige Berechnungen auf Seiten des Wählers bzw. Observers durchgeführt werden. Das System reduziert den Wahlaufwand auf Seiten des Wählers im Vergleich zu [MBC01] und [Sch05] erheblich. Die WI-Beweise der korrekten Verschlüsselung gültiger Wahloptionen entfallen und der Wähler muss nur eine Wahloption als Stimme verarbeiten.

Im November 2005 veröffentlichten Juels, Catalano und Jakobsson [JCJ05] weitere Angriffsszenarien bzw. Sicherheitsanforderungen an Wahlsysteme, die sie unter dem Begriff der Erpressungsresistenz (coercion-freeness) zusammenfassten. Das hier vorgestellte System ist bereits sicher gegen einen der drei folgenden Angriffe, den Randomisations-Angriff. Es ist durch leichte Zusatzanforderungen an den Observer möglich, das System gegen den Impersonationsangriff abzusichern.

- Randomisation-Angriff: Der Angreifer kann den Wähler zwingen, einen bestimmten Geheimtext als Stimme zu wählen - ohne dass der Angreifer den zugrundeliegenden Klartext kennt. Das Wahlsystem in dieser Arbeit ist im Unterschied zu [HS00], [MBC01] und [Sch05] bereits gegen diesen Angriff abgesichert, da pro Wähler nur eine Wahloption verarbeitet wird.
- Der Angreifer kann den Wähler zwingen, sich der Wahl zu enthalten.
- Impersonationsangriff: Ein Wähler könnte dem Angreifer seinen Observer und geheimen Schlüssel geben, so dass dieser an Stelle des Wählers abstimmen kann. Das kann man verhindern, indem zur Benutzung des Observers biometrische Merkmale des Wählers geprüft werden. Es ist auch möglich, dass der Observer einen zweiten Wert h'_V und den zugehörigen geheimen Wert z'_V gespeichert hat. Der Wähler würde dem Angreifer dann den Wert z'_V, den Observer und eine PIN geben, die den Observer zum falschen Arbeiten und falschen Designated-Verifier-Beweis bezüglich z'_V bzw. h'_V veranlasst.

Zusammenfassend ist das Wahlverfahren effizient und sicher gegen alle bisher bekannten Angriffe, abgesehen vom Enthaltungsangriff. Letzterer ist auch in den bisher bekannten Systemen [HS00], [MBC01] und [Sch05] durchführbar und lässt sich durch den in [JCJ05] verwendeten Ansatz wählerbezogener Credentials statt digitaler Signaturen zur Überprüfung der Wahlberechtigung verhindern.