Berner Fachhochschule, Departement Technik und Informatik, CH-2501 Biel, Schweiz

Konzept und Implikationen eines verifizierbaren Vote Électronique Systems

Eric Dubuis, Rolf Haenni, Reto Koenig

in Zusammenarbeit mit

Stephan Fischli, Michael Schläpfer

21. Februar 2012

im Auftrag der Schweizerischen Bundeskanzlei

Version	Date	Authors	Changes
1.2	21.2.2012	E. Dubuis	Rückmeldungen Vernehmlassung.
1.1	11.10.2011	R. Haenni	Rückmeldungen BK.
1.0	5.8.2011	E. Dubuis, R. Haenni, R. Koenig	Initiale Version.

Zusammenfassung

Dieser Bericht beschreibt ein technisches Konzept eines verifizierbaren Internet-Wahlsystems für politische Wahlen und Abstimmungen in der Schweiz. Als Grundlage dieses Konzepts dienen der aktuelle Stand der wissenschaftlichen Forschung sowie die Erfahrungen mit den existierenden Systemen. Im Zentrum des Konzepts steht ein kryptographisches Wahlprotokoll, dass darauf ausgelegt ist, möglichst viele Sicherheitsanforderungen zu erfüllen und gleichzeitig die Verifizierung des Wahlergebnisses zu ermöglichen. Für die Verifizierung werden sämtliche im Wahl- und Auszählungsprozess anfallenden Daten veröffentlicht. Die einzelnen Schritte können somit von einer beliebigen Person nachvollzogen und überprüft werden. Das Protokoll ist eng mit der Forderung an ein vertrauenswürdiges Wahlgerät verknüpft, mit dem die eigentliche Wahlhandlung durchgeführt wird. Dadurch können sichere Wahlen und Abstimmungen garantiert werden, auch wenn die persönlichen Geräte (PCs, Smartphones, Tablet-Computer, etc.) der Wählerinnen und Wähler mit Schadprogrammen befallen sind. Das vorgestellte Konzept bietet somit eine Lösung für zwei grosse Kritikpunkte an den heute existierenden Systemen: die fehlende Verifizierbarkeit und das sogenannte Problem der sicheren Plattform.

Die in diesem Text geäusserten Meinungen und Positionen sind diejenigen der Autoren und stimmen somit nicht unbedingt mit denjenigen der Schweizerischen Bundeskanzlei überein.

Diese Seite ist absichtlich leer.

Inhaltsverzeichnis

Vorwort

Computer übertragen heute über das Internet sekundenschnell Millionen von Bits rund um den Erdball. Ein Bit ist die kleinstmögliche Informationseinheit, welche zwischen zwei möglichen Optionen unterscheidet, zum Beispiel zwischen *Ja* und *Nein*. Um genau solche Bits geht es also, wenn die Schweizer Stimmbürgerinnen und Stimmbürger in einer Volksabstimmung ihren politischen Willen zu konkreten Sachfragen ausdrücken können. In Anbetracht der enormen Möglichkeiten der heutigen Informations- und Kommunikations-Technologien müsste es für die Stimmbürgerinnen und Stimmbürger somit nicht besonders schwierig sein, solche „Abstimmungs-Bits“ über einen elektronischen Kanal zu übertragen. Bei genauerer Betrachtung erweist sich diese Aufgabe aber als äusserst schwierig. Nicht die Übertragung selbst ist das Problem, sondern das Verhindern von möglichen Fehlern oder Manipulationen beim eigentlichen Abstimmungsakt oder bei der anschliessenden Auszählung. Gleichzeitig muss unter allen Umständen das Stimmgeheimnis bewahrt werden, das heisst, es darf nicht möglich sein zu erfahren, wie eine bestimmte Person gestimmt hat. Da die inneren Abläufe eines Computers einem äusseren Betrachter grundsätzlich verborgen bleiben, sind diese Anforderungen nur schwer zu erfüllen.

Die Schweiz gehört weltweit zu den Ländern, die mit elektronischen Abstimmungen am meisten Erfahrung hat. Vor mehr als 10 Jahren hat der Bund ein Pilotprojekt *Vote Électronique* gestartet, und seit 2003 sind in den Kantonen Genf, Neuenburg und Zürich unter der Aufsicht des Bundes entsprechende Systeme im Einsatz. Besonders für die Auslandschweizerinnen und Auslandschweizer dieser Kantone ist die Möglichkeit des elektronischen Abstimmens eine grosse Erleichterung. Durch Beherbergung auf den bestehenden Systemen sind andere Kantone zurzeit daran, diesen Dienst auch für ihre eigenen Auslandschweizerinnen und Auslandschweizer bereitzustellen. Mit all diesen Projekten nimmt die Schweiz im internationalen Vergleich eine Pionierrolle ein, durch welche sie in Anbetracht der oben erwähnten Schwierigkeiten viel Mut zum technischen Fortschritt bewiesen hat.

Trotz den mehrheitlich positiven Erfahrungen mit den existierenden Schweizer Systemen gibt es viele Stimmen, die der elektronischen Stimmabgabe skeptisch gegenüberstehen. Während konservative Kreise dabei die in der direkten Demokratie verwurzelten Traditionen in Frage gestellt sehen, sind vor allem aus wissenschaftlichen Kreisen Bedenken bezüglich der Sicherheit dieser Systeme geäussert worden [38]. Einige der weltweit namhaftesten Experten im Bereich der IT-Sicherheit haben eine Empfehlung veröffentlicht, in der sie vom Einsatz von elektronischen Wahlsystemen abraten, solange die technischen Schwierigkeiten nicht vollumfänglich gelöst sind [43]. Diese Empfehlung basiert auf mehr als 20 Jahren wissenschaftlicher Forschung auf diesem Gebiet. Dabei ist eine Vielzahl von elektronischen Wahlprotokollen vorgeschlagen und analysiert worden,

welche bezüglich der gebotenen Sicherheit unterschiedliche Eigenschaften besitzen. Da noch kein System sämtliche wünschenswerte Eigenschaften vollumfänglich erfüllt, gibt es zurzeit noch keinen Konsens darüber, welches dieser Systeme als das Beste bezeichnet werden soll.

Eine der wichtigsten gemeinsamen Eigenschaften der in der wissenschaftlichen Literatur vorgeschlagenen Systeme ist die *Verifizierbarkeit*. Es geht dabei darum, dass die Korrektheit des Abstimmungs- oder Wahlresultats von unabhängigen Personen überprüft werden kann. Im Extremfall könnte diese Überprüfung sogar von den Stimmbürgerinnen und Stimmbürgern selbst durchgeführt werden, sofern sie mit genügend technischen Hilfsmitteln ausgestattet sind. Moderne kryptographische Verfahren garantieren dabei mit mathematischer Präzision, dass aufgrund einer erfolgreichen Verifikation auf die Korrektheit des Resultates geschlossen werden kann. Diese Verfahren sind jedoch heute in der Praxis noch kaum bekannt. Auch die existierenden Schweizer Systeme sind nicht verifizierbar.

Die vorliegende Arbeit ist dadurch zustande gekommen, dass die Schweizerische Bundeskanzlei mit dem Auftrag an die Autoren herangetreten ist, ein Konzept eines transparenten und verifizierbaren elektronischen Abstimmungs- und Wahlsystems für die Schweiz zu erarbeiten. Der Stand der wissenschaftlichen Forschung soll dabei ebenso berücksichtigt werden, wie auch die Besonderheiten der direkt-demokratischen Abstimmungs- und Wahlprozesse in der Schweiz und die Erfahrungen der existierenden, nicht-verifizierbaren Systeme. Es geht also darum, erste Schritte in Richtung eines Abstimmungs- und Wahlsystems der *zweiten Generation* vorzubereiten, bei welchem der Weg einer abgegebenen elektronischen Stimme und die Berücksichtigung der Stimme bei der Auszählung für jeden einzelnen nachvollziehbar ist. Ein hohes Mass an Transparenz und Verifizierbarkeit wird mittel- oder langfristig wichtig sein, um als vertrauensfördernde Massnahme die Akzeptanz des elektronischen Abstimmens bei der Bevölkerung aufrechtzuerhalten. Obwohl im Schweizer Recht nicht explizit gefordert, ist die transparente Auszählung ein allgemein akzeptierter Wahlrechtsgrundsatz, der bei elektronischen Systemen besonders zu berücksichtigen ist [13, 14]. Neben der vollständigen Offenlegung des Verfahrens, der Dokumente und Evaluationen sowie der eingesetzten Software scheint Verifizierbarkeit diesbezüglich eines der geeignetsten Mittel zu sein.

Mit dieser Zielsetzung und dem erteilten Auftrag für diese Arbeit beweist die Schweizerische Bundeskanzlei erneut grossen Mut, den Weg des technologischen Fortschritts fortzusetzen und die Pionierrolle der Schweiz beim *Vote Électronique* weiterzuführen. Ein ähnliches Projekt gibt es zurzeit nur in Norwegen, wo in Kürze ein hoch transparentes System eingeführt wird. Die Autoren fühlen sich geehrt, im Rahmen ihrer Kompetenzen in der Schweiz an diesem Prozess mitwirken zu können. Durch diese Zusammenarbeit erhält ein ursprünglich rein wissenschaftliches Interesse an diesem Thema eine unerwartete gesellschaftspolitische Relevanz. Entsprechend gross werden die Bemühungen der Autoren sein, sich für das Erreichen der gestellten Zielsetzungen einzusetzen und so das Projekt in die richtige Richtung zu leiten.

1. Einleitung

Die vorliegende Arbeit ist im Frühjahr 2011 durch die Schweizerische Bundeskanzlei initiiert und von den Autoren in den Monaten Mai bis August 2011 geschrieben worden. Der Auftrag der Bundeskanzlei sah vor, ein Konzept für ein verifizierbares elektronisches Abstimmungs- und Wahlsystem zu erstellen, das als technische Grundlage für zukünftige *Vote Électronique* Projekte dienen könnte. Als rechtliche Grundlage für diesen Auftrag diente der Vertrag zwischen der Schweizerischen Bundeskanzlei und der Berner Fachhochschule vom 25. Mai 2011. Bei der Ausarbeitung des Konzepts und dem Schreiben dieser Arbeit haben die Autoren ihre Erfahrungen aus einer mehrjährigen Forschungs-, Publikations- und Lehrtätigkeit auf dem Gebiet der elektronischen Abstimmungen eingebracht. Das vorgestellte Resultat soll dabei nicht als endgültiger Lösungsvorschlag verstanden werden, sondern als Diskussionsgrundlage für eine weiterreichende Ausarbeitung.

In diesem ersten Kapitel wird zunächst die Ausgangslage genauer beschrieben, die durch den oben erwähnten Vertrag zwischen den Autoren und der Bundeskanzlei vorgegeben war. Daraus werden verschiedene Zielsetzungen abgeleitet, an denen sich diese Arbeit orientiert. Anschliessend wird das methodische Vorgehen zum Erreichen dieser Zielsetzungen beschrieben.

1.1. Ausgangslage

Im Kern der von der Schweizerischen Bundeskanzlei in Auftrag gegebenen Konzeption eines elektronischen Abstimmungs- und Wahlsystems steht die *Verifizierbarkeit*. Diese soll der Wählerschaft die Möglichkeit geben, die Korrektheit des Abstimmungs- oder Wahlergebnisses nachzuvollziehen. Es geht also einerseits darum, die Stimmbürgerinnen und Stimmbürger zu überzeugen, dass die eigene Stimme im Sinne ihrer Abgabe im Ergebnis enthalten ist. Andererseits soll die Wählerschaft nachvollziehen können, dass das Ergebnis alle abgegebenen aber nur legitime Stimmen berücksichtigt. Die Forderung nach Verifizierbarkeit ist im Bericht über die Schweizer Pilotprojekte zum *Vote Électronique* vom 31. Mai 2006 wie folgt begründet:

> „Die Risiken, die in einer fehlenden Nachvollziehbarkeit und Beweisbarkeit begründet sind, müssen als hoch eingestuft werden.“ [16, Abschnitt 5.2.2.6]

Neben der angestrebten Verifizierbarkeit wurde auch festgehalten, dass das System sich sowohl für Wahlen wie auch für Abstimmungen eignen muss, dass es die klassischen Kanäle (Urnenwahl, Briefwahl) komplementieren soll, dass die Sicherheit auch auf Seite

der Clients (d.h. auf den Computern der Stimmbürgerinnen und Stimmbürger) angemessen berücksichtigt werden soll und dass die Benutzerfreundlichkeit in etwa dem Stand der existierenden Schweizer Systeme entsprechen sollte.

Das in Auftrag gegebene Arbeitspaket umfasst gemäss Beschreibung im Vertrag drei Punkte, wobei der erste unter dem Stichwort *Konzept* und die beiden letzteren unter dem Stichwort *Implikationen* zusammengefasst werden können.

Konzept. Zunächst soll das vorgeschlagene verifizierbare *Vote Électronique* System spezifiziert werden. Dazu gehören eine Auflistung der verwendeten Systemkomponenten sowie eine Beschreibung der notwendigen Initialisierung dieser Komponenten auf Seiten des Betreibers (einmalig und vor jeder Abstimmung oder Wahl wiederkehrend). Weiter soll die Integration des elektronischen Systems mit den klassischen Kanälen geklärt werden, indem die Aufbereitung des Wahl- und Abstimmungsmaterials sowie die Wahlprozedur im Wahllokal (zur Streichung von elektronisch abgegebenen Stimmen) beschrieben wird. Und nicht zuletzt soll die Kernkomponente des Konzepts, die eigentliche elektronische Wahl- und Abstimmungsprozedur, im Detail spezifiziert und diskutiert werden. Der Abstraktionsgrad soll jenem von technisch-wissenschaftlichen Publikationen entsprechen. Dieser erste Teil des ersten Arbeitspakets ist in Kapitel 3 dargelegt. Einige der zum Verständnis notwendigen kryptographischen Grundlagen werden in Anhang A eingeführt.

Implikationen. Der zweite und dritte Punkt im ersten Arbeitspaket betreffen die möglichen Implikationen des vorgestellten Konzepts. Im Vordergrund steht dabei eine Diskussion der erreichten und im Vergleich zu den bestehenden Systemen gewonnenen Sicherheit. Auf potentielle Einsparungen bei der Zertifizierung soll ebenso hingewiesen werden wie auch auf die Implikationen auf den Wahl- und Abstimmungsprozess. Unter Mitwirkung der Schweizerischen Bundeskanzlei sollen zudem die nötigen Änderungen bei der Umsetzung des Beschwerderechts sowie an den technischen Schnittstellen (u.a. zu den Wählerregistern) aufgezeigt werden. Weiter sollen mögliche Auswirkungen auf die Benutzerfreundlichkeit des Systems diskutiert werden. Die Resultate dieses zweiten Teils des ersten Arbeitspakets werden in Kapitel 4 vorgestellt.

1.2. Zielsetzungen

Aus der zuvor beschriebenen Ausgangslage lassen sich verschiedene Zielsetzungen ableiten, welche die Eigenschaften des zu konzipierenden *Vote Électronique* Systems weiter konkretisieren. Diese Zielsetzungen orientieren sich an den Eigenschaften der bestehenden Schweizer Systeme und sollen den gewonnenen Mehrwert aufzeigen. Die folgende Auflistung enthält die 12 wichtigsten dieser Zielsetzungen (die gewählte Reihenfolge steht in keinem Zusammenhang mit der relativen Wichtigkeit der einzelnen Punkte).

1. Die Möglichkeit, die korrekte Stimmabgabe bzw. das Abstimmungs- oder Wahlergebnis zu verifizieren (im oben beschriebenen Sinne, siehe Abschnitt 1.1), wird von keinem der bestehenden Schweizer Systeme geboten [16, Abschnitt 5.2.2.6]. Das Konzept soll Verifizierbarkeit als zentrale Systemeigenschaft vorsehen und aufzeigen, wie diese zu realisieren ist.

2. Bei den bestehenden Schweizer Systemen können Manipulationen durch Schadprogramme auf den (möglicherweise infizierten) Computern der Stimmbürgerinnen und Stimmbürger nicht vollständig ausgeschlossen werden [16, Abschnitt 5.2.2.4]. Das Konzept soll diesem Umstand Rechnung tragen und mögliche Lösungswege vorschlagen.

3. Das Problem des Stimmenkaufs oder des Erzwingens einer bestimmten Wahlhandlung (z.B. durch Bedrohung oder Nötigung) ist im elektronischen Kontext besonders ausgeprägt. Die bestehenden Schweizer Systeme sehen hierfür keine besonderen Gegenmassnahmen vor. Entsprechend soll das Konzept Massnahmen präsentieren, um dieses Problem zu lösen oder zumindest zu entkräften.

4. Obwohl dem Stimmgeheimnis auch bei den bestehenden Schweizer Systemen grosses Gewicht eingeräumt wird, ist es zum Teil unklar (u.a. wegen fehlenden öffentlichen Dokumentationen [38]), ob dieses unter akzeptablen Annahmen tatsächlich immer gewährleistet werden kann. Im Konzept sollen Vorschläge unterbreitet werden, die das Stimmgeheimnis unter möglichst allen denkbaren Angriffsszenarien garantieren können.

5. Bei der Realisierung der bestehenden Schweizer Systeme wurde die vorhandene wissenschaftliche Fachliteratur nicht oder nur ansatzweise berücksichtigt. Demzufolge müssen sich die Schweizer Systeme heute den Vorwurf gefallen lassen, nicht dem Stand der wissenschaftlichen Forschung zu entsprechen. Das Konzept hingegen soll die vorhandene Fachliteratur als Ausgangsbasis betrachten, um darauf aufbauend ein für die Schweiz geeignetes System vorzuschlagen.

6. Da elektronische Abstimmungen vor allem auch für Auslandschweizerinnen und Auslandschweizer wünschenswert sind, wäre es sinnvoll, wenn auch das Verschicken des Stimmmaterials über den Postweg entfallen könnte. Dies ist bei den bestehenden Schweizer Systemen nicht gegeben. Das Konzept soll deshalb Möglichkeiten prüfen, durch welche die Stimmbürgerinnen und Stimmbürger durch eine einmalige Registrierung Zugang zum System und somit zu mehreren zukünftigen Wahlen oder Abstimmungen erhalten. Wohnsitzänderungen oder Änderungen bezüglich des Stimmrechts müssen leicht vollzogen werden können.

7. Da nicht beabsichtigt ist, die traditionellen Abstimmungskanäle (Urne, Briefpost) in absehbarer Zukunft einzustellen, muss der zusätzliche elektronische Kanal komplementär dazu sein. So muss zum Beispiel gewährleistet sein, dass niemand mehr als eine gültige Stimme über die verschiedenen Kanäle abgeben kann. Es soll jedoch nicht möglich sein, dass jemand eine elektronisch abgegebene Stimme mittels

einer brieflichen Stimmabgabe oder an der Urne überstimmt.[1] Ebenso soll es nicht möglich sein, eine elektronische Stimme durch eine zweite elektronische Stimme zu ersetzen.

8. Bezüglich Benutzerfreundlichkeit befinden sich die bestehenden Schweizer Systeme auf einem relativ hohen Niveau. Das Konzept muss von einer vergleichbaren Benutzerfreundlichkeit ausgehen. Dies bedeutet insbesondere, dass die Möglichkeit der Verifizierung der eigenen Stimme oder des gesamten Ergebnisses die Handhabung der Abstimmungs-Software nicht viel komplizierter machen darf.

9. Die Sicherheit, Verfügbarkeit und Funktionstüchtigkeit eines elektronischen Abstimmungssystems sollte nicht von einzelnen Komponenten oder einzelnen Personen abhängen. Solche sogenannte *Single-Points-of-Failure* sind bei den bestehenden Schweizer Systemen zum Teil zu erkennen. Um diesem Problem entgegenzuwirken, sollte das Konzept darauf ausgerichtet sein, dass alle kritischen Komponenten und alle beteiligten Personen redundant ausgelegt sind.

10. Wie in allen bestehenden Schweizer Systemen soll das Konzept die Besonderheiten der schweizerischen Abstimmungs- und Wahlprozeduren berücksichtigen und auf die entsprechenden Bedürfnisse zugeschnitten sein. Dazu gehört zum Beispiel die Tatsache, dass Vorlagen aus allen föderativen Stufen (Bund, Kantone, Gemeinden) gemeinsam zur Abstimmung gelangen können. Zudem gibt es zahlreiche kantonale Unterschiede bezüglich Wahlprozeduren, Wählerregister, Stimmmaterial, Behandlung von Beschwerden, etc. Und nicht zuletzt soll die Kapazität des Systems für die Grösse der Schweizer Wählerschaft ausgelegt sein.

11. Ein oft genannter Kritikpunkt an den bestehenden Schweizer Systemen ist die mangelnde Transparenz bezüglich Dokumentation des realisierten Verfahrens, der verwendeten Technologien und Algorithmen sowie der durchgeführten Tests und Evaluationen [38]. Auch der Quellcode der eingesetzten Software ist aus unterschiedlichen Gründen schwierig einzusehen. Um diese Art von Kritik zu vermeiden und gleichzeitig das Vertrauen der Wählerschaft ins System zu stärken, soll das Konzept von einem maximal möglichen Grad an Transparenz ausgehen. Die Sicherheit des Systems soll also nicht auf dem Zurückhalten von Informationen beruhen, sondern auf deren Offenlegung [19].

12. Die Realisierbarkeit eines solchen Projekts hängt immer stark von den zu erwartenden Kosten für die Entwicklung, die Einführung, den Betrieb und den Unterhalt des konzipierten Systems ab. Die Abschätzung dieser Kosten ist zwar noch nicht Teil des vorliegenden Arbeitspakets, doch sollte das Konzept in dieser Hinsicht keine unrealistischen Annahmen treffen.

In den folgenden Kapiteln, insbesondere in den Abschnitten 2.1, 2.4 und 4.1 werden die oben genannten Zielsetzungen weiter präzisiert. Gegen Schluss dieser Arbeit, in Abschnitt 5.1, wird das vorgeschlagene System diesen Zielsetzungen gegenübergestellt.

[1] Dieser Punkt ist in der Beschreibung des erteilten Auftrags missverständlich formuliert, wurde jedoch nachträglich in einer mündlichen Vereinbarung in diesem Sinne festgehalten.

1.3. Vorgehen und Überblick

Als Entscheidungsgrundlage wird im folgenden Kapitel zunächst auf die Sicherheitsanforderungen für ein elektronisches Abstimmungs- und Wahlsystem eingegangen, wie sie in der Fachliteratur üblicherweise angegeben sind. Diese Anforderungen orientieren sich an einem idealen System und dienen somit als Referenzpunkte für die Ausarbeitung des Konzepts in Kapitel 3. Im Anschluss daran wird der Stand der wissenschaftlichen Forschung zusammengefasst, indem die verschiedenen existierenden Ansätze kurz vorgestellt und deren Vor- und Nachteile diskutiert werden, insbesondere auch in Bezug auf eine mögliche Anwendung in der Schweiz. Auf dieser Diskussion beruht dann die Entscheidung für den Ansatz, der dem Konzept zugrunde liegen soll. Aus dem wissenschaftlich geprägten Blickwinkel dieser Betrachtungen werden anschliessend die bestehenden Schweizer Systeme kurz vorgestellt und deren Verbesserungspotential aufgezeigt. Zum Schluss werden in einem separaten Abschnitt vertrauensbildende Massnahmen zur Sprache gebracht, welche für die Akzeptanz von elektronischen Abstimmungen und Wahlen bei der Wählerschaft von erheblicher Bedeutung sind. Unter dem Stichwort *Transparenz* werden in diesem Zusammenhang verschiedene Punkte genauer erläutert, die bei der Ausarbeitung des Konzepts allenfalls zu beachten sind [19, 42].

In Kapitel 3, dem eigentlichen Hauptteil dieser Arbeit, wird das erarbeitete Konzept eingeführt. Das vorgeschlagene System beruht auf einem kryptographischen Protokoll, welches sich in Bezug auf die gestellten Sicherheitsanforderungen und im Vergleich zu anderen Protokollen am geeignetsten erwiesen hat. Das Protokoll alleine kann nicht sämtliche Sicherheitsprobleme lösen, bildet aber ein stabiles Fundament, das durch entsprechende nicht-kryptographische Komponenten oder Prozeduren komplettiert werden kann. Sämtliche benötigte Komponenten und die einzelnen Schritte der daraus hervorgehenden Abstimmungs- oder Wahlprozeduren werden in Kapitel 3 im Detail beschrieben und diskutiert. Teile des Konzepts sind modular aufgebaut, das heisst, dass einzelne Komponenten (mit entsprechenden Auswirkungen auf gewisse Sicherheitseigenschaften) auch weggelassen werden können, sofern sich deren Realisierung als zu aufwendig herausstellen sollte. Viele technische Fragen bezüglich einer möglichen konkreten Realisierung bleiben in diesem Konzept jedoch noch unbeantwortet.

Neben den mehrheitlich technischen Fragestellungen in Kapitel 3 werden in Kapitel 4 die verschiedenartigen Implikationen einer allfälligen Realisierung des Konzepts auf den Status Quo erläutert. Dabei kommen Verbesserungen an den Sicherheitseigenschaften ebenso zur Sprache wie auch Änderungen in Bezug auf die Abstimmungs- und Wahlprozesse. Diskutiert werden ebenfalls Implikationen zu rechtlichen oder organisatorischen Aspekten, zum Beispiel in Bezug auf das Beschwerderecht oder hinsichtlich der existierenden Schnittstellen zu den Wählerregistern. Auf die Beschreibung der Implikationen auf die Benutzerfreundlichkeit, bei der insbesondere die Verifizierungsprozedur aus Benutzersicht zur Sprache kommt, folgt zum Schluss des Kapitels die Erörterung der Konsequenzen einer Homologation, falls das System realisiert würde.

Die Schlussfolgerungen aus dieser Arbeit werden in Kapitel 5 zusammengefasst und Möglichkeiten für das weitere Vorgehen erörtert.

2. Grundlagen

Die Sicherheit von elektronischen Abstimmungen und Wahlen ist seit mehr als 30 Jahren Gegenstand der wissenschaftlichen Forschung. Mit dem Ziel, bestimmte Sicherheitsanforderungen zu erfüllen, sind dabei verschiedenste Systemvorschläge entstanden. Die meisten dieser Systeme basieren auf einem kryptographischen Protokoll, welches den Ablauf einer elektronischen Wahl oder Abstimmung regelt. Dabei werden viele technische Details, die für die konkrete Realisierung eines solches Protokolls geklärt werden müssen, offen gelassen. Weil einige Sicherheitsprobleme nicht von Anfang an als solche erkannt wurden, ist im Laufe der Jahre die Liste der Sicherheitsanforderungen ständig erweitert worden. Entsprechend sind auch die Protokolle und die daraus resultierenden Systeme immer ausgeklügelter und zum Teil komplexer geworden. In den folgenden Abschnitten werden diese Anforderungen eingeführt und die verschiedenen Protokollansätze vorgestellt. Darauf folgen eine kurze Beschreibung der drei existierenden Schweizer Systeme sowie einige allgemeine Bemerkungen zur Transparenz und anderen vertrauensbildenden Massnahmen.

2.1. Anforderungen

Die Liste der Anforderungen an ein elektronisches Abstimmungs- und Wahlsystem orientiert sich primär an Wahlrechtsgrundsätzen wie der *Freiheit der Wahl*, der *Öffentlichkeit der Wahl* oder dem *Geheimnis der Wahl*. Diese sind in gewissen Ländern in der Verfassung oder im Wahlgesetz explizit aufgeführt, jedoch nicht in der Schweiz. Vergehen gegen diese Grundsätze werden aber auch in der Schweiz strafrechtlich verfolgt (StGB, Art 279ff). In den traditionellen Abstimmungs- und Wahlprozeduren (Wahlurne, Briefpost) wurden entsprechende Massnahmen zum Schutz dieser Grundsätze installiert. Diese können Verletzungen an den Grundsätzen nicht in allen erdenklichen Szenarien verhindern (brieflich abgegebene Stimmen können zum Beispiel verlorengehen oder gestohlen werden), bieten aber insgesamt einen relativ guten Schutz. Wichtig dabei ist, dass die möglichen Sicherheitslücken nicht beliebig skalierbar sind und somit nur eine geringe Auswirkung auf das Ergebnis der Abstimmung oder Wahl haben können. Diese Eigenschaft bringt das Medium des gedruckten Papiers mit sich. Zudem hinterlassen papierbasierte Manipulationsversuche oft Spuren oder fallen andersartig auf.

Bei einer elektronischen Abstimmung oder Wahl sind die zuletzt genannten Punkte grundsätzlich anders. Da sich elektronische Dokumente ohne grossen Aufwand beliebig oft kopieren lassen und zudem die Kopien nicht vom Original zu unterscheiden sind, sind die Gefahr und die mögliche Auswirkung einer unentdeckten (oder nicht-entdeckbaren)

Manipulation grundsätzlich wesentlich höher. Hinzu kommt, dass das Internet als naheliegender elektronischer Übertragungskanal als äusserst unsicher einzustufen ist, weil der Datenverkehr über eine Reihe von unsicheren Netzwerkknoten und Verbindungen geleitet wird, die grundsätzlich abgehört oder manipuliert werden können. Und nicht zuletzt liegt in den privaten Computern der Wählerinnen und Wähler ein grosses Gefahrenpotential, weil diese durch Schadprogramme oder andere Attacken relativ leicht zu manipulieren sind.

Sichere elektronische Abstimmungen und Wahlen sind deshalb um ein Vielfaches schwieriger zu realisieren als traditionelle Abstimmungen und Wahlen auf Papier. Eine kleine Sicherheitslücke könnte durch eine gezielte Attacke zu einem grossen Problem werden, welches unter Umständen gar nicht erkannt werden kann. Als Orientierungshilfe bei der Konzipierung eines elektronischen Systems ist deshalb die folgende Zusammenstellung der wichtigsten Anforderungen von grosser Bedeutung. Diese beschreiben den Idealfall eines absolut sicheren Systems, das in der Praxis so gut wie möglich angenähert werden sollte. Im Folgenden wird aus Gründen der Einfachheit nur noch von Wahlen die Rede sein, gemeint ist aber immer die Doppelbedeutung einer Wahl oder Abstimmung.

Korrektheit des Ergebnisses. Eine grundlegende Eigenschaft eines Wahlsystems ist die korrekte Ermittlung des Ergebnisses. Die Herausforderung bei elektronischen Wahlsystemen liegt in der Garantie, dass niemand unbemerkt das Wahlergebnis manipulieren kann. Dies bedeutet, dass

- die Wahlberechtigung eindeutig nachgewiesen werden muss,
- jede wahlberechtigte Person höchstens einmal wählen darf,
- alle abgegebenen gültigen Stimmen gezählt werden,
- abgegebene Stimmen nicht verändert oder ersetzt werden können,
- niemand die Ergebnisermittlung manipulieren kann.

Diese Punkte müssen den unterschiedlichsten technischen Angriffsszenarien standhalten. Selbst Manipulationen durch die Wahlbehörden oder die Entwickler und Betreiber der einzelnen Systemkomponenten sollen grundsätzlich ausgeschlossen sein. Auch der technische Ausfall von Teilkomponenten darf das Ergebnis nicht verändern können. Letztendlich geht es also darum, dass das Wahlergebnis unter allen Umständen exakt dem ermittelten kollektiven Willen der Wählerschaft entspricht.

Geheimnis der Wahl. Diesem Grundsatz zufolge darf niemand feststellen können, ob und wie jemand gewählt hat. Indem die Wahlentscheidung geheim gehalten wird, ist garantiert, dass Wählerinnen und Wähler ihre Stimme unbeeinflusst abgeben können. Bei einer strikten Auslegung dieses Grundsatzes bedeutet dies, dass

- die abgegebenen Stimmen nicht mit den Wählerinnen und Wählern verknüpft werden können,
- niemand erkennen kann, wer an der Wahl teilgenommen hat und wer nicht,

- niemand beweisen kann, ob und wie sie oder er gewählt hat,
- keine Teilresultate ermittelt werden können (während oder nach der Wahl).

Der zuletzt genannte Punkt wird oft als Grundsatz für eine *gerechte Wahl* angegeben, da das Bekanntgeben von Zwischenresultaten die Wahl beeinflussen könnte. Zusammenfassend kann also gesagt werden, dass bei einer geheimen Wahl ausser dem Wahlergebnis keinerlei Information über das Verhalten der Wählerschaft ermittelt werden kann. Wiederum muss diese Anforderung allen möglichen Angriffsszenarien standhalten, zum Beispiel auch gegenüber Angriffen, die von den Wahlbehörden oder den Betreibern einzelner Systemkomponenten ausgehen.

Freiheit der Wahl. Dieser Grundsatz besagt, dass die Wählerinnen und Wähler ihre Stimmen ohne Zwang oder Druck und ohne sonstige unzulässigen Beeinflussungen von aussen abgeben können. Damit wird die Entscheidungsfreiheit der Wählerinnen und Wähler weiter geschützt, also auch in Fällen, die durch das Wahlgeheimnis alleine nicht abgedeckt sind. Konkret bedeutet dies, dass niemand gezwungen werden kann, weder durch Nötigung noch durch Bestechung, eine bestimmte Wahlhandlung durchzuführen, wie zum Beispiel

- eine bestimmte gültige Stimme abzugeben,
- eine ungültige Stimme abzugeben,
- eine bereits abgegebene Stimme zu kopieren,
- eine zufällige Stimme abzugeben,
- eine beliebige Stimme abzugeben (überhaupt an der Wahl teilzunehmen),
- keine Stimme abzugeben,
- das Wahlrecht an jemand anders abzutreten [27].

Es geht hier also darum, dass ein sicheres Wahlsystem resistent gegenüber diesen verschiedensten Formen der Nötigung und des Stimmenkaufs sein soll. Eine Voraussetzung dazu ist die im Wahlgeheimnis verankerte Anforderung, dass es für die Wählerinnen und Wähler nicht möglich ist, einen Beweis über die durchgeführte Wahlhandlung zu erbringen. Das Nichtvorhandensein einer solchen *Quittung* reicht aber nicht aus, um alle oben genannten Möglichkeiten einer nicht-freien Wahlhandlung auszuschliessen.

Öffentlichkeit der Wahl. Um die Wählerinnen und Wähler davon zu überzeugen, dass der Wahlvorgang korrekt abgelaufen ist, fordert dieser Grundsatz, dass der Weg der abgegebenen Stimmen von der Abgabe über die Auszählung bis zur Ermittlung des Ergebnisses vollständig nachvollziehbar ist. Letztendlich geht es also darum, dass Mechanismen oder Prozeduren zur Verfügung gestellt werden müssen, mit welchen die Korrektheit des Ergebnisses (gemäss obiger Definition) verifiziert werden kann. Diese Anforderung der Verifizierbarkeit besitzt zwei Teilaspekte.

- Unter *individueller* Verifizierbarkeit versteht man die Möglichkeit, die Berücksichtigung der eigenen Stimme im Endergebnis zu überprüfen. Dies geschieht oft in drei Teilschritten, welche in der Literatur als *cast-as-intended*, *recorded-as-cast* und *counted-as-recorded* bekannt sind.
- Bei der *universellen* Verifizierbarkeit geht es darum, den Wählerinnen und Wählern die Möglichkeit zu geben, auf der Basis sämtlicher abgegebener Stimmen die Ergebnisermittlung nachzuvollziehen und somit das Endresultat zu überprüfen. Dies impliziert, dass auch die Gültigkeit der einzelnen Stimmen überprüfbar ist, also zum Beispiel, ob jede Stimme von einer wahlberechtigten Person stammt (jedoch ohne dabei das Wahlgeheimnis zu verletzen).

Um universelle Verifizierbarkeit zu realisieren, müssen die abgegebenen Stimmen der Öffentlichkeit zugänglich gemacht werden. Diese Offenlegung der bei einer Wahl anfallenden Daten ist ein Teilaspekt einer übergeordneten Anforderung der *Transparenz* (siehe Abschnitt 2.4). Anstelle der vollen universellen Verifizierbarkeit gibt es die Variante der *delegierten* Verifizierbarkeit, bei welcher die Verifizierung an eine Gruppe von unabhängigen und vertrauenswürdigen Wahlauditoren delegiert wird. In diesem Fall kann die Offenlegung der Daten auf diese Personengruppe beschränkt werden.

Weitere technische Anforderungen. Neben den oben beschriebenen Anforderungen, die sowohl für traditionelle wie elektronische Wahlsysteme gelten, gibt es eine Reihe von weiteren technischen Anforderungen, die im speziellen Fall von elektronischen Wahlsystemen zu beachten sind. Die folgende Liste fasst die wichtigsten dieser technischen Anforderungen für den Fall eines Internet-Wahlsystems zusammen.

- Neben der Korrektheit des Ergebnisses muss ein elektronisches Wahlsystem auch garantieren, dass es während der Durchführung der Wahl ständig verfügbar ist. Es geht also darum, dass die Wählerinnen und Wähler nicht darin eingeschränkt werden dürfen, wann sie ihre Stimmen abgeben können. Es ist klar, dass bei einem gleichzeitigen Ausfall aller Systemkomponenten die korrekte Durchführung einer Wahl nicht mehr gewährleistet werden kann. Um dieses Risiko zu minimieren, soll der Ausfall von einzelnen Systemkomponenten tolerierbar sein und die korrekte Funktionsweise des Gesamtsystems nicht beeinträchtigen. Diese Anforderung, die sogenannte *Robustheit*, muss für sämtliche Systemkomponenten erfüllt sein, damit es im System keinen *Single-Point-of-Failure* gibt. Technisch gesehen wird hierfür ein Schwellwert definiert, der die minimale Anzahl von korrekt funktionierenden Komponenten bestimmt, welche für die korrekte Funktionsweise des Gesamtsystems erforderlich ist. So könnte zum Beispiel eine Teilfunktion des Systems durch 10 unabhängige Komponenten getragen werden, von denen mindestens 3 (Schwellwert) korrekt funktionieren müssen. In dieser Weise wird die Wahrscheinlichkeit eines Ausfalls dieser Teilfunktion massiv verkleinert. Wichtig dabei ist die vollständige Unabhängigkeit dieser Komponenten. So dürfen sie zum Beispiel nicht von den gleichen Personen betrieben werden.
- Bei Internet-Wahlen werden die Stimmen auf den persönlichen Geräten der Wählerinnen oder Wähler abgegeben, deren Sicherheit nicht vorausgesetzt werden kann.

Man spricht dabei vom *Problem der sicheren Plattform* [32]. Die daraus abgeleitete Anforderung an ein Wahlsystem besteht darin, dass die oben erwähnten Sicherheitsanforderungen auch dann gewährleistet sein müssen, wenn die Wählerinnen und Wähler ihre Stimmen auf unsicheren Geräten abgeben. Konkret können diese Geräte durch Schadprogramme wie Viren, Würmer, trojanische Pferde, Spyware oder Scareware infiziert sein, welche auf einen gezielten Angriff auf die bevorstehende Wahlhandlung ausgerichtet sind. Dass Attacken dieser Art heute ohne allzu grossen Aufwand zu realisieren sind, haben verschiedenste Beispiele aus anderen Anwendungsbereichen deutlich gezeigt.

- Für die Vorbereitung, Durchführung und Auszählung einer Wahl steht jeweils eine bestimmte Zeit zur Verfügung. Zum Beispiel müssen die Wählerinnen und Wähler ihre Wahlhandlung – insbesondere das eigentliche Abschicken der Stimme – innerhalb einer vernünftigen Zeit (wenige Minuten oder Sekunden) durchführen können. Nach Abschluss der Wahl muss das Ergebnis innert einer nützlichen Frist (wenige Stunden) ermittelt und bekannt gegeben werden können. Dies impliziert, dass ein elektronisches Wahlsystem so konzipiert sein muss, dass diese Anforderung mit realistischen Annahmen bezüglich der zur Verfügung stehenden Rechenleistung bei den Wahlbehörden sowie den Wählerinnen und Wählern zu erfüllen ist. Dies scheint mit den heute verfügbaren Geräten relativ leicht möglich zu sein. Da aber viele kryptographische Methoden einen sehr grossen Rechenaufwand erfordern, und komplexe kryptographische Wahlprotokolle deshalb sehr zeitintensiv sein können, muss diesem Punkt grosse Beachtung geschenkt werden.

- Ein elektronisches Wahlsystem sollte von niemandem zu einem anderen Zweck verwendet werden können. Es darf zum Beispiel nicht möglich sein, Nachrichten über das Wahlsystem zu verbreiten. Das heisst, dass die abgegebenen Stimmen keine solchen Nachrichten enthalten dürfen oder dass solche Stimmen erkannt werden können. Das System muss also geeignete Mechanismen bereitstellen, um solche Missbräuche zu verhindern. Es geht dabei vor allem darum, das System vor einer gezielten Diskreditierung zu schützen.

- Damit ein elektronisches Wahlsystem in der Praxis eingesetzt werden kann, muss der Zugang zum System sowie der eigentliche Wahlvorgang aus Sicht des Benutzers mit möglichst wenigen und einfachen Schritten zu bewerkstelligen sein. Man kann verlangen, dass die Benutzer einige einfach zu kommunizierende Instruktionen befolgen können, es dürfen aber keine komplizierten Installationen oder technisch schwer verständliche Benutzerinteraktionen vorausgesetzt werden. Neben der eigentlichen Benutzerfreundlichkeit geht es hierbei darum, das System den verschiedensten Personengruppen in gleicher Weise zugänglich zu machen, also auch technisch weniger versierten Personen. Hinter dieser Anforderung steht ein weiterer Wahlrechtsgrundsatz, die sogenannte *Allgemeinheit der Wahl*, welche den gleichen Zugang zum Wahlsystem für die gesamte Wählerschaft postuliert. Neben Personen mit eingeschränkten technischen Fähigkeiten und Mitteln bezieht sich dieser Grundsatz vor allem auch auf Personen mit körperlichen Behinderungen. Konkret bedeutet das zum Beispiel, dass ein elektronisches Wahlsystem auch von sehbehinderten Personen benutzt werden kann.

2.2. Stand der Forschung

Die Forschung im Bereich der elektronischen Wahlen unterscheidet grundsätzlich zwischen zwei Kategorien von Systemen. Zum einen geht es um elektronische Geräte, welche im Abstimmungslokal zum Zuge kommen und die präzise und schnelle Auszählung zum Ziel hat. Entsprechend sind die dabei erzielten Resultate für diese Arbeit von untergeordneter Bedeutung. Unser Augenmerk liegt vielmehr bei der zweiten Kategorie von Systemen, welche die elektronische Stimmabgabe von zuhause aus über das Internet zum Ziel hat. In der englischsprachigen Fachliteratur spricht man dabei von *Remote Electronic Voting Systems*, im Folgenden wird jedoch einfach von *Internet-Wahlsystemen* die Rede sein. Da die Geräte, auf denen die Stimmen abgegeben werden, nicht unter der Kontrolle der Wahlbehörden stehen, sind sichere Internet-Wahlsysteme grundsätzlich schwieriger zu realisieren als entsprechende Systeme für Wahllokale. Entsprechend befasst sich der grösste Teil der publizierten wissenschaftlichen Arbeiten elektronischer Wahlsysteme mit den Internet-Wahlen.

Ein wichtiges Unterscheidungsmerkmal bei den vorgestellten Verfahren ist die Art und Weise, wie die Anonymisierung der Stimmen durchgeführt wird, um das Wahlgeheimnis zu gewährleisten. Grob lassen sich die Verfahren in fünf *Protokollfamilien* einteilen, welche in den folgenden Unterabschnitten vorgestellt werden. In Bezug auf die im vorherigen Abschnitt eingeführten Anforderungen hat jeder dieser Ansätze bestimmte Vor- und Nachteile. Eine kurze Diskussion dieser Vor- und Nachteile wird zu Beginn von Kapitel 3 als Entscheidungsgrundlage für die Auswahl des dem Konzept zugrundeliegenden kryptographischen Protokolls dienen. Einige der zum Verständnis der folgenden Ausführungen notwendigen kryptographischen Grundlagen werden in Anhang A eingeführt (z.B. der Begriff des *kryptographischen Protokolls*).

Eine Gemeinsamkeit von fast allen bekannten elektronischen Wahlprotokollen ist die Realisierung der elektronischen Urne als *öffentliches Anschlagbrett* (engl. *Public Bulletin Board*), auf welchem die abgegebenen Stimmen veröffentlicht werden. Vereinfacht kann man sich ein solches Anschlagbrett als eine Webseite vorstellen, auf der alle abgegebenen Stimmen aufgelistet werden. Die Veröffentlichung der Stimmen ist eine zentrale Voraussetzung für die universelle Verifizierbarkeit. Die Realisierung eines solchen Anschlagbretts ist ein schwieriges Problem für sich, welches in dieser Arbeit nicht weiter beschrieben wird [8, 24, 34].

Blinde Signaturen. Blinde Signaturen wurden in den frühen 1980er Jahren erstmals beschrieben [9]. Wie gewöhnliche digitale Signaturen erlauben sie das Signieren von Dokumenten, wobei in diesem Fall das Dokument vom Urheber im Vorfeld für den Signierenden unlesbar (blind) gemacht wird. Nach der Signatur kann der Urheber die Lesbarkeit des Dokuments wieder herstellen und ist somit im Besitz eines gültig signierten Dokuments. Allgemein dienen blinde Signaturen also dazu, Dokumente von jemandem für einen bestimmten Zweck beglaubigen oder autorisieren zu lassen, ohne den Inhalt des Dokuments aufdecken zu müssen.

Genau diese Eigenschaft hat man sich in einem der ältesten Protokolle für Internet-Wahlen zu Nutze gemacht [21]. Dabei wird die verschlüsselte Stimme verblindet der Wahlbehörde zur Signatur vorgelegt. Diese prüft die Wahlberechtigung des Antragstellers und stellt sicher, dass zuvor noch keine Stimme vom Antragsteller abgegeben wurde. Demzufolge erhält die verschlüsselte Stimme durch die blinde Signatur den Status einer gültigen Stimme, welche in die elektronische Urne gelegt werden darf (über einen anonymen Kanal, siehe Anhang A). Wenn die elektronische Urne öffentlich zugänglich ist, kann jeder die Gültigkeit der abgegebenen Stimmen überprüfen, ohne dabei Rückschlüsse auf die Urheber der Stimmen machen zu können. Auch die Wahlbehörde kann das Wahlgeheimnis nicht brechen, da diese nur die verblindeten Stimmen gesehen hat. Am Schluss werden die Stimmen mit einem Schwellwert-Verfahren entschlüsselt und gezählt, was ebenfalls öffentlich verifiziert werden kann.

Weil der Ansatz der blinden Signaturen den traditionellen Prozess im Wahllokal relativ genau nachbildet (der Stempel auf dem Wahlumschlag entspricht der blinden Signatur), wurden bis vor kurzem grosse Anstrengungen unternommen, diese Protokollfamilie als mögliche Lösung zu etablieren. Es gibt zum Beispiel Varianten des ursprünglichen Protokolls, welche das Ausstellen der blinden Signaturen nicht an eine einzelne Wahlbehörde knüpft (*Single-Point-of-Failure*), sondern an eine Gruppe von unabhängigen Wahlbehörden. Dabei ist die Korrektheit des Ergebnisses gegeben, wenn eine Mehrheit der Wahlbehörden korrekt arbeitet (mittels einer blinden Gruppensignatur mit Schwellwert). Heute jedoch werden diese Ansätze in der Forschung kaum mehr weiterverfolgt, da die Nachteile gegenüber anderen Ansätzen überwiegen. Zum Beispiel ist es äusserst schwierig, das Problem des Stimmenkaufs oder der Nötigung zu lösen, ohne gleichzeitig andere Anforderungen zu tangieren.

Homomorphe Auszählung. Eine andere Möglichkeit, das Wahlgeheimnis sicherzustellen, besteht darin, die einzelnen Stimmen gar nie zu entschlüsseln. Man benutzt dabei eine mathematische Eigenschaft gewisser asymmetrischer Verschlüsselungsverfahren, die es erlaubt, mit verschlüsselten Daten zu rechnen. Diese Eigenschaft wird *Homomorphismus* genannt. Statt der Entschlüsselung und anschliessenden Zählung der einzelnen Stimmen, können die verschlüsselten Stimmen aufsummiert werden, ohne sie einzeln zu entschlüsseln. Daraus entsteht eine Verschlüsselung des Ergebnisses, welches dann mit Hilfe eines Schwellwert-Verfahrens entschlüsselt wird (siehe Anhang A). Da der private Schlüssel dabei von verschiedenen Personen geteilt wird, kann niemand alleine das Wahlgeheimnis brechen. Um sicherzustellen, dass nur gültige Stimmen aufsummiert werden, müssen den verschlüsselten Stimmen sogenannte *Zero-Knowledge Beweise* (siehe Anhang A) mitgegeben werden, die deren Gültigkeit bezeugen.

Das erste kryptographische Protokoll, welches diese Idee im Detail beschreibt, wurde 1997 vorgestellt [15]. Seither sind viele Varianten dieses Verfahrens vorgeschlagen worden. Da die einzelnen Stimmen gar nie im Klartext ersichtlich sind, ist es legitim, jeweils die Namen der Wählerinnen und Wähler direkt mit den zugehörigen verschlüsselten Stimmen zu veröffentlichen. Dies vereinfacht den Prozess der Authentifizierung und erlaubt es, auch im Nachhinein öffentlich zu überprüfen, dass jede abgegebene Stimme von einer wahlberechtigten Person stammt. Dies ist aber gleichzeitig ein Nachteil, weil damit

schon während der Wahl ersichtlich ist, wer bereits eine Stimme abgegeben hat und wer nicht. Bei einer strikten Auslegung des Wahlgeheimnisses ist dieses damit gebrochen.

Eine praktische Umsetzung dieser Protokollfamilie existiert unter dem Namen HELIOS. In grösseren Hochschulwahlen wird diese Umsetzung seit einigen Jahren erprobt [2]. Leider sind aber die Anforderungen an die Rechenleistung derart hoch (vor allem für die aufwendigen Zero-Knowledge Beweise), dass nur Wahlen mit wenigen Kandidierenden oder einfache Ja/Nein-Abstimmungen homomorph ausgezählt werden können. Ein anderes Problem ist die Möglichkeit des Stimmenkaufs und der Nötigung, für welches es keine zufriedenstellende Lösung gibt.

Verifizierbare Mix-Netzwerke. Eine weitere Art, die abgegebenen Stimmen zu anonymisieren, besteht darin, verifizierbare Mix-Netzwerke (siehe Anhang A) zu verwenden. Damit kann eine Liste von verschlüsselten Stimmen derart gemischt (permutiert) und verändert werden, dass am Schluss keine Verbindung mehr zu den ursprünglichen Stimmen hergestellt werden kann. Anschliessend können die Stimmen, wie bei den Ansätzen mit der blinden Signatur, durch ein Schwellwert-Verfahren entschlüsselt und zusammengezählt werden [6, 37]. Wenn die Stimmen und die Beweise des Mix-Netzwerks auf einem öffentlichen Anschlagbrett publiziert sind, kann die Korrektheit des Ergebnisses überprüft werden. Ähnlich wie bei der homomorphen Auszählung ist bei diesem Verfahren schon während der Wahl ersichtlich, wer bereits eine Stimme abgegeben hat und wer nicht.

Eine frühere Version von HELIOS – und bei komplexen Wahlen auch die aktuelle Version – sind auf dieses Verfahren ausgerichtet [1]. Auch das System der spanischen Firma SCYTL, welches im Kanton Neuenburg eingesetzt wird (siehe Abschnitt 2.3), setzt ein Mix-Netzwerk für das Mischen der Stimmen ein, bietet für diesen Schritt aber keine universelle Verifizierbarkeit [11].

Anonymisierte öffentliche Schlüssel. Statt die Stimmen in einem verifizierbaren Mix-Netzwerk zu anonymisieren, können durch ein ähnliches Verfahren auch die öffentlichen Schlüssel der Wählerinnen und Wähler anonymisiert werden. Wenn dann die abgegebenen Stimmen mit den privaten Schlüsseln der Wählerinnen und Wähler signiert sind, können diese mit den entsprechenden anonymisierten öffentlichen Schlüsseln verifiziert werden. Dabei wird überprüft, ob die Signaturen von wahlberechtigten Personen erstellt wurden, jedoch ohne aufzudecken von wem. Mit anderen Worten findet bei diesem Verfahren eine *anonyme Authentifizierung* der Wählerinnen und Wähler statt. Die Stimmen können anschliessend mit einem Schwellwert-Verfahren entschlüsselt und zusammengezählt werden. Im Unterschied zu den Verfahren mit der blinden Signatur oder den anonymisierten Stimmen kann hier nicht festgestellt werden, wer eine Stimme abgegeben hat und wer nicht.

Diese Art von Protokoll wurde 2004 zum ersten Mal erwähnt [30]. Später wurde der Ansatz von den Autoren dieser Arbeit weiterentwickelt [39, 23]. Ein grosser Vorteil des Ansatzes besteht darin, dass der grösste Teil der benötigten Rechenleistung im Vorfeld

des eigentlichen Wahlprozesses erbracht werden kann, in dem normalerweise am meisten Zeit zur Verfügung steht. Auch können Wahlen mit vielen Kandidierenden effizient durchgeführt werden. Unter dem Namen *Selectio Helvetica* wird dieses Protokoll bereits praxisnah eingesetzt [18] und zwar im Rahmen der Abstimmungsplattform *baloti.ch*, welche für Immigranten in der Schweiz bestimmt ist. Zwar deckt die aktuelle Umsetzung noch nicht alle Eigenschaften des Protokolls ab, zeigt aber bereits, dass die praktische Realisierung möglich ist.

Erpressungsfreie Systeme. Eine weitere Protokollfamilie wird unter dem Prädikat *erpressungsfrei* geführt. Vereinfacht gesagt, handelt es sich dabei um eine Kombination der beiden zuvor beschriebenen Protokollfamilien. Es werden also sowohl die Stimmen in einem verifizierbaren Mix-Netzwerk gemischt, wie auch die öffentlichen Schlüssel der Wählerinnen und Wähler. Basierend auf dieser Idee wurde 2005 ein viel zitierter Artikel publiziert [27]. Das darin beschriebene Protokoll ermöglicht im Fall einer Erpressung oder Bestechung die Abgabe einer falschen Stimme, die während des gesamten Abstimmungsprozesses nicht von einer gültigen Stimme zu unterscheiden ist. Die Wählerinnen und Wähler können somit immer eine Stimmabgabe vortäuschen und dadurch einer Erpressung oder Bestechung entgehen. Zu einem späteren Zeitpunkt kann dann die echte Stimme abgegeben werden, ohne dass dies vom Erpresser oder Stimmenkäufer bemerkt werden kann. Dies ist eine aussergewöhnliche Eigenschaft, die bei keinem anderen Protokoll auch nur ansatzweise vorliegt. Gleichzeitig erfüllt es alle anderen Sicherheitsanforderungen.

Leider besitzt das ursprüngliche Protokoll eine relativ grosse Komplexität. Diese impliziert eine derart hohe Rechenleistung, dass sie für Wahlen von einer realistischen Grösse nicht erbracht werden kann. Es gab zwar Versuche, solche Systeme konkret zu bauen, bisher jedoch nur in einem akademischen Kontext [12]. Neuerdings gibt es einige Vorschläge für effizientere Varianten dieses Protokolls [4, 10, 28, 41], doch steht deren Praxistauglichkeit noch aus.

Code Voting. Eine andere Gruppe von Protokollen stellt nicht die Anonymisierung der Stimmen oder die Erpressungsfreiheit in den Vordergrund, sondern das Problem der sicheren Plattform bei den Wählerinnen und Wählern. Das Ziel dabei ist die sichere Stimmabgabe auf einem (möglicherweise) unsicheren Computer. Um nicht das Wahlgeheimnis zu gefährden, darf der Computer die Klartext-Stimme nicht erfahren, weil diese sonst unbemerkt weitergegeben oder veröffentlicht werden könnte [5]. Zudem darf der Computer nicht selber wählen können, also den Benutzer glauben lassen, korrekt abgestimmt zu haben, während in Tat und Wahrheit eine andere Stimme abgeschickt wurde. Die Möglichkeit der Durchführung solcher Attacken mit Hilfe unbemerkt installierter Schadprogramme, wurde in anderen Anwendungsbereichen schon deutlich unter Beweis gestellt.

Der Ansatz, der von diesen Protokollen verfolgt wird, ist unter dem Begriff *Code Voting* bekannt [26, 31, 33]. Die Idee dabei besteht darin, die Wählerinnen und Wähler mit

individualisierten Codes für die verschiedenen Kandidierenden auszustatten. Statt deren Namen elektronisch zu erfassen, wird nun der entsprechende Code eingegeben. Der möglicherweise mit Schadprogrammen infizierte Computer kann aufgrund dieser Codes nicht auf die eigentliche Wahl schliessen, wodurch das Wahlgeheimnis gewährleistet ist. Auch kann ein Schadprogramm keine Codes von anderen Kandidierenden abschicken, da diese dem Programm nicht bekannt sind. Dies setzt aber voraus, dass diese Codes über einen unabhängigen Kanal an die Wählerschaft verteilt werden, üblicherweise als gedrucktes *Code Sheet* über den Postkanal. Zurzeit ist dieses Thema auch Gegenstand eines von der Schweizerischen Bundeskanzlei initiierten Forschungsprojekts an der ETH Zürich.

Eines der fortschrittlichsten Protokolle dieser Art ist *Pretty Good Democracy* [25]. Die Autoren selbst raten aber davon ab, das Protokoll in der Praxis einzusetzen, weil nicht alle Probleme zufriedenstellend gelöst sind. Allein die Erstellung der individualisierten Codes pro Abstimmung ist ein sehr komplexes und fehleranfälliges Unterfangen, wenn es darum geht, das Wahlgeheimnis unter allen Umständen zu wahren. Zudem scheint der Postweg für den Versand der geheimen Codes in vielen Fällen nicht akzeptabel zu sein. Ein weiteres Problem ist die limitierte Benutzerfreundlichkeit bei der Eingabe der Codes.

2.3. Bestehende Systeme in der Schweiz

Die bestehenden Systeme in der Schweiz unterscheiden sich in vielen Punkten ganz wesentlich von den in der wissenschaftlichen Literatur vorgeschlagenen Protokollen für verifizierbare Internet-Wahlprotokolle. Zum Beispiel ist keines der Systeme individuell oder universell verifizierbar, da die Stimmen nicht auf ein öffentliches Anschlagbrett geschrieben werden. Zwar wird in allen drei Systemen eine sogenannte *Testurne* zur Verfügung gestellt [16, ergänzende Dokumentation 6], bei der die Mitglieder des Abstimmungsausschusses zur Überprüfung des Systems beliebige Teststimmen abgeben können. Diese werden in der Testurne gesammelt und unabhängig von den gültigen Stimmen zusammengezählt, um Plausibilitätsüberprüfungen zu ermöglichen. Erfolgreiche Tests dieser Art lassen aber nur bedingt Rückschlüsse auf die absolute Korrektheit des Ergebnisses zu, denn sie können zum Beispiel das unerlaubte Einfügen von Stimmen im Namen von Personen, die nicht abgestimmt haben, nicht erkennen. Eine raffinierte Attacke könnte zudem gezielt die gültigen Stimmen verändern, während die Teststimmen unverändert gelassen werden. Aus einem wissenschaftlichen Blickwinkel stellt deshalb die Testurne kein zufriedenstellendes Instrument zur Verifizierung des Ergebnisses dar.

Die drei Schweizer Systeme erlauben es den Wählenden nicht, die korrekte Verarbeitung der Daten selber zu überprüfen. Die fehlende Verifizierbarkeit kommt daher, dass keines der drei Systeme auf der Basis eines der etablierten kryptographischen Protokolle für verifizierbare Internet Wahlsysteme entwickelt wurde. Generell kann man sagen, dass die zur Verfügung stehenden kryptographischen Möglichkeiten nicht vollumfänglich genutzt werden. Zum Beispiel werden zum Verteilen von Kompetenzen keine Methoden

des *Secret Sharing* und keine echten Schwellwert-Kryptoverfahren eingesetzt (siehe Anhang A), und es werden keine Zero-Knowledge Beweise eingesetzt, um die Korrektheit der ausgetauschten Nachrichten abzusichern. Diese Elemente können letztendlich auch dazu dienen, stärkere Garantien bezüglich der Wahrung des Stimmgeheimnisses zu geben. Auch zur Sicherung der Benutzerplattform bietet die wissenschaftliche Literatur Potential zu Versbesserungen. Dabei muss aber auch erwähnt werden, dass ausser einem Versuch in Norwegen noch nie ein verifizierbares Internet-Wahlsystem für politische Wahlen in Betrieb war; es handelt sich um relativ neue Technologie.

Ein weiteres Problem aller drei Schweizer Systeme ist die mangelnde Transparenz. Besonders in den Kantonen Neuenburg und Zürich ist die öffentlich zugängliche Dokumentation des Systems und deren Komponenten äusserst spärlich. Zudem ist in keinem der drei Kantone der Quellcode der eingesetzten Software öffentlich zugänglich (in Genf erhalten Staatsbürgerinnen und -bürger oder Personen, die ein Mandat von der Wahlkommission erhalten haben, auf Anfrage Einsicht in den Quellcode). Dieser Mangel an Transparenz erfordert von den Wählerinnen und Wählern ein Höchstmass an Vertrauen, dass die eigene Stimme tatsächlich so ins Endergebnis einfliesst, wie sie abgegeben wurde, oder allgemein, dass die Korrektheit des Ergebnisses unter allen Umständen gegeben ist. Auch wenn die durchgeführten Pilotversuche gezeigt haben, dass die Wählerschaft in der Schweiz durchaus gewillt ist, dieses Vertrauen aufzubringen, ist ein höheres Mass an Transparenz anzustreben, um letztendlich die Akzeptanz der Systeme bei der Wählerschaft über einen längeren Zeitraum zu sichern. Dies entspräche zudem einer aktuellen Forderung des Europarats [14].

In den folgenden Abschnitten werden die drei Schweizer Systeme kurz eingeführt und deren Eigenschaften diskutiert. Dies wird in Kapitel 4 die Grundlage sein, um die Vorteile des vorgestellten Konzepts gegenüber dem Status Quo aufzeigen zu können.

2.3.1. Kanton Genf

Die charakteristischen Merkmale des Genfer Wahlsystems sind ein zentrales Stimmregister, ein Stimmrechtsausweis mit Rubbelfeld für die stimmberechtigten Personen und eine Browser-basierte Java-Anwendung, welche beim Abstimmungsvorgang vom Abstimmungsserver automatisch geladen wird, um die Kommunikation mit demselben zu bewerkstelligen [16, Seite 5475].

Die Abstimmung über das Internet geschieht in vier Schritten:

1. Die stimmberechtigte Person startet einen Java-fähigen Browser. Der Zugang zum Abstimmungsserver erfolgt durch die Eingabe der 16-stelligen Nummer, welche sich auf dem Stimmrechtsausweis befindet.[1] Nach einer positiver Prüfung der Nummer schickt der Abstimmungsserver den Abstimmungszettel an den Computer der stimmberechtigten Person.

[1] Aus Sicherheitsgründen wird der Hashcode der 16-stelligen Nummer zum Server geschickt. Mit Hilfe einer vorgefertigten Tabelle kann der Server daraus die 16-stellige Nummer rekonstruieren.

2. Die stimmberechtigte Person stimmt ab. Der ausgefüllte Stimmzettel wird dem Abstimmungsserver geschickt.
3. Der Abstimmungsserver prüft die Integrität des ausgefüllten Stimmzettels und schickt ihn der stimmberechtigten Person zur Kontrolle zurück, zusammen mit dem Kontrollcode, welcher sich auch auf dem Stimmrechtsausweis befindet. Die stimmberechtigte Person bestätigt ihren Stimmwillen durch die Angabe des Geburtsdatums, der Heimatgemeinde und des freigerubbelten Geheimcodes.
4. Sind die Angaben korrekt, so markiert der Abstimmungsserver die 16-stellige Nummer im elektronischen Stimmregister, verschlüsselt die Stimme mit dem öffentlichen Schlüssel der Urne, schickt sie der elektronischen Urne und schickt einen Bestätigungstext an die abstimmende Person zurück.

Sicherheit. Die Aufbereitung der Daten für die Stimmrechtsausweise erfolgt nach einem wohldefinierten und überwachten Prozess. Die Daten für die Stimmrechtsausweise werden mittels eines gesicherten Verfahrens an die Druckerei übergeben. Das elektronische Stimmregister erhält nur eine Teilmenge dieser Daten, insbesondere keine Namen und Adressen. Die stimmberechtigte Person kann die Authentizität des Abstimmungsservers anhand des Fingerprints des Server-Zertifikats überprüfen. Der Fingerprint befindet sich auch auf dem Stimmrechtsausweis. Die stimmberechtigte Person authentisiert sich, indem sie im ersten Schritt die 16-stellige Nummer angibt. Das Problem der Schadsoftware im Eingabegerät der stimmberechtigten Person wird entschärft, indem in einem weiteren Schritt ein neuer SSL-Kanal mit gegenseitiger Authentifizierung erstellt wird. Dazu wird Server-seitig ein temporäres Client-Zertifikat erstellt. Das Client-Zertifikat und der dazugehörige private Schlüssel werden mit einem symmetrischen Schlüssel, der aus der 16-stelligen Nummer auf eindeutige Art erzeugt wird, verschlüsselt und der Java-Anwendung im Browser zurückgeschickt. Nach erfolgter Entschlüsselung des Client-Zertifikats wird die erste SSL-Verbindung abgebaut und eine zweite SSL-Verbindung, diesmal mit gegenseitiger Authentifizierung, erstellt. Zusätzlich wird der Datenverkehr unter Verwendung des abgeleiteten Schlüssels aus der 16-stelligen Nummer symmetrisch verschlüsselt. Auch wird der Datenverkehr zum Server unter der Verwendung des privaten Schlüssels, der zum Zertifikat passt, signiert, so dass der Server immer sicher ist, dass die Daten vom Browser der abstimmenden Person stammen. Nach Erhalt der Stimme prüft der Server diese auf ihre Integrität und schickt sie zur Bestätigung an die Java-Anwendung im Browser zurück, zusammen mit dem Rückantwortcode. Die stimmberechtigte Person prüft die Stimme und vergleicht den Rückantwortcode mit demjenigen auf dem Stimmrechtsausweis. Wenn alles richtig ist, bestätigt die stimmberechtigte Person die Stimme mit ihrem Geburtsdatum, der Angabe des Heimatorts und dem freigerubbelten Geheimcode.

Die Stimme wird auf dem Server mit dem öffentlichen Schlüssel der elektronischen Urne verschlüsselt und in die Urne gelegt. Zudem wird die erfolgreiche Abgabe der Stimme im elektronischen Stimmregister vermerkt, wodurch die elektronische Mehrfachstimmabgabe verhindert wird. Die nachträgliche postalische Stimmabgabe oder der nachträgliche Urnengang ist wegen des freigerubbelten Geheimcodes auf dem Stimmrechtsausweis

nicht möglich. Zur Auszählung der Stimmen werden nach Schliessung der elektronischen Urne die Stimmen zuerst gemischt[2] und danach entschlüsselt. Dazu müssen die sogenannten *Kontrolleure* zwei Passwörter eingeben, die sie bei der Eröffnung des Abstimmungsvorgangs selbst kreiert haben [16, Seite 5475 unten]. Technisch gesehen wird damit ein privater Schlüssel für die Entschlüsselung freigeschaltet.[3]

Integraler Bestandteil der Sicherheit des Genfer Systems sind begleitende Prozesse, welche zur Wahrung der Sicherheitskriterien definiert sind. Diese sehen dementsprechend auch eine klare Trennung von Aufgaben vor, und Zugriffsrechte werden entsprechend auf verschiede Akteure verteilt. Bei der Schlüsselgenerierung und bei der Entschlüsselung sind Mitglieder der Wahlkommission beteiligt. Die wichtigsten Prozesse werden dadurch überwacht.

Analyse. Eine abgegebene Stimme ist beim Abstimmungsserver mit der 16-stelligen Nummer der stimmberechtigten Person gekoppelt. Die Kopplung derselben Nummer mit dem Namen und der Adresse der stimmberechtigten Person ist im Prozessschritt „Vorbereitung der Daten“ für die Bereitstellung der Stimmrechtsausweise zwingend notwendig.[4] Die stimmberechtigte Person erhält bei erfolgreicher elektronischer Stimmabgabe einen Bestätigungstext. Dieser Text erlaubt aber nicht zu prüfen, ob die Stimme korrekt in die elektronische Urne gelegt und ob die Stimme bei der Auszählung richtig gezählt wurde. Die Angabe von Geburtsdatum und Heimatort erschwert systematische Attacken von aussen. Interne Attacken werden durch technische Hilfsmittel (Logging, unabhängige Konsistenzchecks) in Kombination mit definierten Prozessen stark erschwert. Insbesondere sind im Online-System nicht alle Informationen vorhanden, die es Internen erlauben würden, eine Stimme abzugeben. Die Verwendung einer zweiten SSL-Verbindung mit symmetrischer Authentifizierung und zusätzlicher symmetrischer Verschlüsselung erschwert zwar die *Man-in-the-Middle*-Attacken, kann sie aber nicht mit absoluter Sicherheit verhindern. Gegen eine *Man-in-the-Browser*-Attacke bietet diese Massnahme allerdings keine grosse Abwehr.

2.3.2. Kanton Neuenburg

Die abstimmenden Personen des Kantons Neuenburg verwenden das *Portal Guichet Unique* (GU), um verschiedene staatsrelevante Aktivitäten elektronisch abzuwickeln. Auf Wunsch können die Stimmbürgerinnen und Stimmbürger auch elektronisch abstimmen. Im Hintergrund läuft zu diesem Zweck ein System der spanischen Firma Scytl. Aus den kommunalen Stimmregistern wird für das elektronische Abstimmen am Stichtag ein zentrales elektronisches Stimmregister erstellt [16, Seite 5481].

[2] Das Mischen verunmöglicht den Rückschluss der Stimmen auf die Abstimmenden, auch wenn man die zeitliche Reihenfolge des Stimmabgabe kennt. Beim Mischen wird ein Zufallszahlengenerator verwendet, der auf dem Quantenzufall basiert.

[3] Gemäss Angabe von Michel Warinsky anlässlich eines Treffens vom 29. Mai 2009 in Genf.

[4] Das Befolgen interner Prozesse garantiert, dass die Nummer bzw. die Stimme im Nachhinein nicht mit der stimmberechtigten Person verknüpft wird.

Die Abstimmung übers Internet erfolgt gemäss den folgenden Schritten:

1. Unter der Aufsicht des Abstimmungsausschusses werden der öffentliche und der private Schlüssel für die Verschlüsselung und Entschlüsselung der Stimmen generiert. Der private Schlüssel wird in zwei Schlüsselteile geteilt und auf mehrere Chipkarten gespeichert, die an eine feste Anzahl von Mitgliedern des Abstimmungsausschusses verteilt werden. Die Chipkarten werden mittels PIN geschützt und in versiegelten Umschlägen abgelegt.

2. Die stimmberechtigten Personen erhalten den Stimmrechtsausweis. Dieser enthält einen Validierungs- und einen Bestätigungscode, welche vertraulich und speziell für die elektronische Stimmabgabe bestimmt sind.

3. Eine Person meldet sich mit Hilfe ihres Computers in ihrem GU-Konto an (Benutzercode, PIN und Nummer, welche sich auf einer Strichliste befindet). Sie erhält je nach Stimmrecht Zugang zur Abstimmung. Der Computer zeigt einen leeren elektronischen Stimmzettel. Die stimmberechtigte Person füllt den Stimmzettel mit Hilfe des Computers aus.

4. Die stimmberechtigte Person bestätigt ihren Stimmwillen mit ihrem Validierungscode. Der Computer verschlüsselt die Stimme mit dem öffentlichen Schlüssel und schickt diese an den Abstimmungsserver (der Abstimmungsserver ist eine Komponente innerhalb des GU-Systems).

5. Der Abstimmungsserver bestätigt den Erhalt der Stimme mit dem Bestätigungscode, welcher auch auf dem Stimmrechtsausweis vermerkt ist. In [16, Seite 5481] wird leider nicht gesagt, wie der Bestätigungscode bestimmt wird, nur dass dieser später, nach der Abstimmung in einer Liste publiziert wird und so die stimmberechtigte Person sicher sein kann, dass die Stimme in der Auszählung mitberücksichtigt wurde.

Sicherheit. Der Zugang zum GU bedingt die Einrichtung eines Kontos. Dazu müssen sich die Neuenburger Stimmberechtigten einschreiben. Sie erhalten darauf per Post einen Benutzercode und eine PIN und später ihre Nummernkarte. Stimmberechtigte Personen erhalten für jede Abstimmung per Post ihren Stimmrechtsausweis. Die prozeduralen Sicherheitsmassnahmen zur Herstellung der Stimmrechtsausweise sind in [16] leider nicht beschrieben. Der Stimmrechtsausweis enthält den Validierungs- und Bestätigungscode. Die Verwendung des Validierungscodes verhindert, dass die stimmberechtigte Person mehrfach abstimmt. Mit dem Einlesen des Barcodes lässt sich nämlich bei der nachfolgenden postalischen Stimmabgabe oder Abgabe an der Urne feststellen, ob die stimmberechtigte Person schon elektronisch abgestimmt hat. Das Stimmgeheimnis wird gewahrt, indem die Stimme im Endgerät der stimmberechtigten Person verschlüsselt wird. Danach wird nur die verschlüsselte Stimme in die elektronische Urne gelegt. Stimmzettel, welche die Integrität verletzen, werden nach dem Entschlüsseln, aber vor dem Auszählen aussortiert. Die verschlüsselten Stimmen werden nach der Schliessung der elektronischen Urne mit den privaten, durch einen PIN geschützten Schlüsseln der Mitglieder des Abstimmungsausschusses entschlüsselt.

Analyse. Die verschlüsselte Stimme der stimmberechtigten Person ist beim Abstimmungsserver mit dem Validierungscode gekoppelt. Eine Entkopplung kann nur durch strikte prozedurale und technische Massnahmen garantiert werden. Die Mehrfachstimmabgabe wird dank dem Validierungscode verhindert. Der individualisierte Bestätigungscode garantiert, dass die Stimme den Abstimmungsserver erreicht hat. Er kann aber nicht garantieren, dass die Stimme mit dem richtigen öffentlichen Schlüssel verschlüsselt wurde und demnach nicht durch eine *Man-in-the-Middle*-Attacke auf dem Weg in die elektronische Urne verändert wurde. Der Bestätigungscode kann auch nicht garantieren, dass die Stimme beim Auszählen richtig gezählt wurde. Nicht benutzte Codes könnten missbraucht werden, um zusätzliche Stimmen in die Urne einzulegen. Durch die ungenaue Beschreibung des Bestätigungscodes kann nicht abschliessend beurteilt werden, ob dieser eingelegte Stimmen in der elektronischen Urne vor Manipulation schützt.

2.3.3. Kanton Zürich

Das Abstimmungssystem des Kantons Zürich basiert auf der dezentralen Führung der Stimmregister der 171 Zürcher Gemeinden. Das Abstimmungssystem stützt sich auf eine flexible, modulare Lösung, welche den Gemeinden eine gewisse Autonomie (z.B. die Öffnungszeiten der elektronischen Urne) bietet und gleichzeitig eine Vielzahl von Vorlagen sowohl für Abstimmungen wie auch für Wahlen zulässt. Eine Webanwendung führt die stimmberechtigte Person durch den Abstimmungsvorgang.[5]

Wie im Kanton Genf erhalten die stimmberechtigten Personen ihren Stimmrechtsausweis mit den persönlichen und allgemeinen Angaben. Die Abstimmung übers Internet erfolgt gemäss folgenden Schritten (basierend auf [16, Seite 5481], mit einigen Ergänzungen):

1. Die an der elektronischen Abstimmung beteiligten Gemeinden exportieren den Inhalt der Gemeindestimmregister ins virtuelle Stimmregister. Daraus werden die Stimmrechtsausweise generiert und verschickt. Diese beinhalten nebst den Personalien und Adressen den Zugangscode, den geheimen PIN-Code und ein persönliches Sicherheitssymbol. Danach werden im virtuellen Stimmregister sämtliche personenbezogenen Daten gelöscht.
2. Die stimmberechtigte Person startet die webbasierte Abstimmungsanwendung und meldet sich unter Verwendung des Zugangscodes an. Der Abstimmungsserver schickt den Abstimmungszettel in Abhängigkeit der Stimmrechte an den Computer der Person.
3. Die stimmberechtigte Person füllt den Abstimmungszettel mit Hilfe des Computers aus. Der Computer sendet den ausgefüllten Stimmzettel an den Abstimmungsserver zurück.
4. Der Abstimmungsserver prüft die Integrität des ausgefüllten Stimmzettels. Aus diesem wird ein Bild erzeugt, welches auch das Sicherheitssymbol beinhaltet. Das so entstandene Bild wird an das Endgerät des Benutzers zurückgeschickt und der

[5] Die SMS-Variante des Zürcher Systems wurde in der Zwischenzeit eingestellt.

stimmberechtigten Person angezeigt. Die stimmberechtigte Person vergleicht das Sicherheitssymbol mit demjenigen auf dem Stimmrechtsausweis und bestätigt die Korrektheit des Stimmzettels durch Angabe des Geburtsdatums und des geheimen PIN-Codes, welcher im Stimmrechtsausweis mittels eines HYDALAM-Siegels[6] geschützt ist.

5. Sind die Angaben korrekt, so verschlüsselt der Abstimmungsserver die Stimme mit dem Schlüssel der betreffenden Gemeinde und legt die verschlüsselte Stimme in die elektronische Urne (aus den Erläuterungen in [16, Seiten 5487ff.] geht nicht hervor, ob die verschlüsselten Stimmen in separaten Urnen abgelegt werden oder ob sie erst vor dem Auszählen aus einer gemeinsamen Urne entnommen und danach separiert und entschlüsselt werden). Die entschlüsselten Stimmen werden dem Ausmittlungssystem WABSTI übergeben, wo sie zu den konventionell eingegangenen Stimmen hinzugefügt werden.

Sicherheit. Die Aufbereitung der Daten für die Stimmrechtsausweise erfolgt wie in Genf zentral. Diese Daten werden an verschiedene vertrauenswürdige Druckereien übergeben. Die Trennung der personenbezogenen Daten von den Zugangscodes und dem Sicherheitssymbol erfolgt durch explizites Löschen der entsprechenden Daten im virtuellen Register. Die stimmberechtigte Person authentisiert sich, ähnlich wie beim Genfer System, mit dem Zugangscode, dem geheimen PIN-Code und dem Geburtsdatum (in Genf noch dem Heimatort). Das persönliche Sicherheitssymbol macht allfällige Schadsoftware, die sich auf dem Eingabesystem befindet und die Stimme zu manipulieren versucht, sichtbar. Zugangsdaten und der Stimmzettel werden über einen gesicherten Kanal (HTTPS) an den Abstimmungsserver übermittelt. Der Abstimmungsserver prüft die Zugangsdaten und die Integrität der Stimme. Die stimmberechtigte Person kann die Authentizität des Abstimmungsservers anhand des Fingerprints des Server-Zertifikats überprüfen. Der Fingerprint befindet sich auf dem Stimmrechtsausweis. Die verschlüsselten Stimmen werden erst nach Schliessung aller Urnen durch die Vertreter der beteiligten Gemeinden entschlüsselt. Ein vorzeitiges Entschlüsseln würde vermutlich dank der Aufzeichnungen entdeckt, falls diese nicht manipuliert wurden.

Analyse. Wie beim Genfer System ist die Unverknüpfbarkeit nur durch das Einhalten prozeduraler Massnahmen gewährleistet. Würde man im virtuellen Stimmregister keine Daten löschen, so wäre die Verknüpfung der Stimme mit Zugangscode und den Personalien der stimmberechtigten Person möglich. Eine routinemässige Datensicherung des virtuellen Stimmregisters vor dem Löschen der personenbezogenen Daten verschärft dieses Problem. Die stimmberechtigte Person hat keine Möglichkeit zu prüfen, ob ihre Stimme unverfälscht in die elektronische Urne gelangt ist und ob sie korrekt gezählt wurde. Nicht verwendete Zugangscodes könnten von Personen, welche entsprechenden Zugriff haben, missbraucht werden, um weitere Stimmen in die elektronische Urne zu legen. Auch könnten gültige Stimmen aus der elektronischen Urne entfernt werden, wenn

[6] HYDALAM ist ein Produkt der Firma KOOPMANN DRUCK, mit dessen Hilfe vertrauliche Informationen mit konventionellen Laserdruckern auf Papier gebracht werden können, um diese sicher zum Empfänger zu übermitteln.

die entsprechende Markierung im virtuellen Stimmregister rückgängig gemacht wird. Die zur Auszählung der verschlüsselten Stimmen benötigten Passwörter werden vorab den Verantwortlichen der beteiligten Gemeinden per Post zugeschickt. Der genaue Entschlüsselungsvorgang ist in [16] nicht beschrieben. Unklar ist auch, welche Garantien die Verantwortlichen in den Gemeinden haben, um sicher zu sein, dass alle gemeindespezifischen Stimmen korrekt entschlüsselt und zusammengezählt wurden.

2.4. Transparenz

Eine der grössten Stärken des Wahlverfahrens an der Urne ist die hohe Transparenz bei der Stimmabgabe und bei der Auszählung. So können die Wählerinnen und Wähler den Prozess verfolgen und ihn verstehen, ohne dass das Wahlgeheimnis verletzt wird. Diese Möglichkeit des Beobachtens und Überprüfens erzeugt bei der Wählerschaft das Vertrauen, das für die Akzeptanz des Wahlergebnisses nötig ist. Bei vielen elektronischen Wahlverfahren kehrt sich dieses Vertrauen aber oft ins Gegenteil. Denn meist bleibt selbst technisch versierten Wählerinnen und Wählern das Verständnis wegen intransparenter Vorgehensweisen verwehrt. Gepaart mit organisatorischen Massnahmen, welche ein hohes Mass an Vertrauen der Wählerschaft erfordern, kann sich eine Skepsis gegenüber dem konkreten Wahlhergang und ein Misstrauen in das Wahlergebnis ergeben. Auf Dauer ist deshalb diese Intransparenz für die Akzeptanz des Systems bei der Wählerschaft nicht förderlich.

Obwohl Transparenz, wie sie beim Urnengang gegeben ist, bei der elektronischen Stimmabgabe naturgemäss nie zu erreichen ist, sollten dennoch möglichst nachvollziehbare Prozesse zum Einsatz gelangen, welche jederzeit und ohne organisatorischen Aufwand eine Nachprüfung zulassen. Es ist dabei nicht zwingend notwendig, den mathematischen und technischen Hintergrund des elektronischen Wahlprozesses vollständig zu verstehen, um ihn überprüfen zu können. Viel wichtiger ist es, dass die konkreten Auswirkungen der einzelnen Teilprozesse transparent und somit überprüfbar sind. Ebenso verhilft das Offenlegen einzelner Programmteile eines elektronischen Wahlsystems versierten Personen zwar zu mehr Verständnis, echte Transparenz entsteht aber erst aus der Möglichkeit zur steten und vollständigen Überprüfung.

Dies führt zum Schluss, dass ein Maximum an Vertrauen für die elektronische Stimmabgabe erst dann gewonnen werden kann, wenn sämtliche Einzelheiten des Wahlprozesses offengelegt sind und die zu deren Realisierung eingesetzten Komponenten ihre Arbeit jederzeit lückenlos belegen können. Auf diese Weise kann der konkrete elektronische Wahlhergang dem beschriebenen Prozess gegenübergestellt werden. Als Beispiel ist Norwegen zu erwähnen, das zurzeit an der Einführung eines weitgehend transparenten Systems arbeitet. Eine ausführliche Dokumentation des norwegischen Systems und den zugehörigen Quellode findet man auf entsprechenden Webseiten.[7]

Transparenz, also die Offenlegung von Prozessen, Funktionen und kryptographischen Verfahren, ist ein wesentliches Element aus einer Reihe von *vertrauensbildenden Mass-*

[7] Siehe bit.ly/iMjivu für Dokumente und source.evalg.stat.no/websvn für den Quellcode.

nahmen [19, 42]. Verifizierbarkeit ist eine spezielle Form der Transparenz, welche zusätzlich das Offenlegen der anfallenden Daten fordert (siehe Abschnitt 2.1). Dadurch können die Wählerinnen und Wähler prüfen, ob ihre abgegebenen Stimmen korrekt erfasst wurden und ob am Schluss die Stimmen richtig zusammengezählt und dabei nur legitime Stimmen berücksichtigt wurden. Das Offenlegen der Daten muss durch geeignete kryptographische Massnahmen begleitet werden, um das Wahlgeheimnis unter allen Umständen zu wahren. Transparenz bezüglich Daten wird auch im Massnahmenkatalog des Europarats gefordert [14, Richtlinie 13].

Neben der Transparenz und der Verifizierbarkeit werden in der Literatur weitere Massnahmen für die Vertrauensbildung bei Internet-Wahlen gefordert. Dazu gehören die Aufgabentrennung bei allen sicherheitsrelevanten Systemkomponenten auf mehrere unabhängige Instanzen, das Bereitstellen von unabhängiger Software als Alternative zu den offiziell zur Verfügung gestellten Programmen (z.B. für die universelle Verifizierung) sowie die Sicherheitsevaluation durch verschiedene unabhängige Personen oder Institutionen [19, 42]. Solche oder ähnliche Massnahmen sollten aus Sicht der Autoren ein zukünftiges *Vote Électronique* Projekt begleiten.

3. Konzept

In diesem Kapitel erfolgt die Beschreibung des erarbeiteten Konzepts für ein verifizierbares elektronisches Wahl- und Abstimmungssystem für die Schweiz. Das Konzept versucht, sämtliche Zielsetzungen aus Abschnitt 1.2 sowie sämtliche Anforderungen aus Abschnitt 2.1 angemessen zu berücksichtigen. Wiederum wird dabei aus Gründen der Einfachheit immer nur von einem elektronischen Wahlsystem die Rede sein, obwohl jeweils die Doppelbedeutung als Wahl- und Abstimmungssystem gemeint ist. Der Abstraktionsgrad der technischen Beschreibung ist so gewählt, dass sie auch für Personen ohne besonderes technisches Fachwissen verständlich ist. Die dem Konzept zugrunde liegenden kryptographischen Methoden werden in Anhang A kurz eingeführt.

Das erarbeitete Konzept wird in zwei Stufen eingeführt. In Abschnitt 3.1 wird eine geeignete Kombination von zwei existierenden kryptographischen Protokollen als Grundlage für das Konzept vorgeschlagen. Das daraus hervorgehende Protokoll regelt die kryptographischen Berechnungen und die ausgetauschten Nachrichten zwischen den involvierten Personengruppen. Auf der Basis dieses Protokolls wird anschliessend das konzipierte System vorgestellt und dessen Systemkomponenten einzeln beschrieben. Mit der Forderung eines vertrauenswürdigen Wahlgeräts werden dabei zwei grosse Sicherheitsprobleme beseitigt, die durch das Protokoll alleine nicht gelöst werden können. Zum Schluss dieses Kapitels werden in Abschnitt 3.3 die verschiedenen Stufen der Verifizierungsprozedur zusammengefasst.

3.1. Kryptographisches Protokoll

In Abschnitt 2.2 wurden die verschiedenen Ansätze der existierenden kryptographischen Wahlprotokolle vorgestellt und diskutiert. Leider gibt es noch kein Protokoll, welches sämtliche in Abschnitt 2.1 aufgeführten Anforderungen vorbehaltlos erfüllt. Die Wahl des Protokolls für das Konzept erfordert deshalb das Abwägen der entsprechenden Vor- und Nachteile. Als Entscheidungsgrundlage und in Ergänzung zu den Ausführungen in Abschnitt 2.2 liefert Tabelle 3.1 eine übersichtliche Zusammenstellung der wichtigsten Vor- und Nachteile.

Ansatz	**Vorteile**	**Nachteile**
Blinde Signaturen	– Intuitives Konzept (einer Urnenwahl ähnlich) – Leicht umzusetzen – Effiziente Auszählung – Umsetzung erprobt	– Stimmabgabe erfordert synchrone bidirektionale Kommunikation – Universelles Verifizieren der Wahlberechtigung nicht möglich – Benötigt anonymen Kanal – Stimmenkauf und Erpressung möglich – Gilt als veraltet
Homomorphe Auszählung	– Elegantes Konzept – Effiziente Auszählung bei Abstimmungen – Gut erforscht (viele Publikationen) – In der Praxis erprobt (Helios) – In existierende PKIs integrierbar	– Sehr ineffizient bei komplexen Wahlen – Keine Anonymität bez. Teilnahme an der Wahl – Stimmenkauf und Erpressung möglich
Mix-Netzwerke	– Einfaches Konzept – Effiziente Stimmabgabe – In der Praxis erprobt (Scytl, Helios) – Erfahrung in der CH (Neuenburg) – In existierende PKIs integrierbar	– Keine Anonymität bez. Teilnahme an der Wahl – Stimmenkauf und Erpressung möglich
Anonymisierte öffentliche Schlüssel	– Einfaches Konzept – Anonymität bezügl. Teilnahme an der Wahl – Effiziente Stimmabgabe – Effiziente Auszählung – In der Praxis erprobt (Baloti) – Erfahrung in der CH (BFH) – In existierende PKIs integrierbar	– Nicht so gut erforscht – Aufwendige Wahlvorbereitung – Benötigt anonymen Kanal – Stimmenkauf und Erpressung möglich
Erpressungsfreie Systeme	– Verhindert Stimmenkauf und Erpressung – Gut erforscht (viele Publikationen) – State-of-the-Art in der Forschung	– Kompliziertes Konzept – Sehr ineffiziente Stimmabgabe bei komplexen Wahlen – Extrem ineffiziente Auszählung – Ermöglicht das Überfluten des öffentlichen Anschlagbretts – Praktische Erfahrung nur im akademischem Kontext (Civitas) – Nicht mit existierenden PKIs kompatibel
Code-Voting	– Löst das Problem der sicheren Plattform (mit gewissen Einschränkungen)	– Eingeschränkte Benutzerfreundlichkeit – Zusätzlicher sicherer Kanal (Post) erforderlich – Single-Point-of-Failure beim Drucken der Code-Sheets – Wenig Praxiserfahrung

Tabelle 3.1.: Vor- und Nachteile der verschiedenen Kategorien kryptographischer Wahlprotokolle.

3.1.1. Wahl des Protokolls

Die erpressungsfreien Protokolle kommen nicht in Frage, weil diese aus Gründen der Effizienz für den Einsatz bei grösseren Wahlen nicht geeignet sind. Der Ansatz der blinden Signaturen hat gegenüber den anderen Ansätzen mehrere gewichtige Nachteile und entspricht nicht mehr dem aktuellen Stand der Forschung. Code-Voting fällt ebenfalls aus dem Rennen, weil dabei weiterhin ein sicherer Kanal zum Verschicken des Wahlmaterials vorausgesetzt wird, die Benutzerfreundlichkeit stark beeinträchtigt ist und zusätzliche Probleme geschaffen werden. Der Ansatz des homomorphen Auszählens wäre für reine Abstimmungen eine gute und elegante Lösung, ist aber aus Gründen der Effizienz für komplexe Wahlen nicht geeignet.

Somit reduziert sich die Protokoll-Auswahl auf den Ansatz der Mix-Netzwerke oder der anonymisierten öffentlichen Schlüssel. Aufgrund der nachfolgend dargelegten Überlegungen sieht das vorliegende Konzept eine *Kombination* dieser beiden vergleichbaren Ansätze vor. Beide führen eine Anonymisierung der Stimme durch, entweder durch ein Mischen (der öffentlichen Schlüssel) *vor* der Stimmabgabe [23, 30, 39] oder durch ein Mischen (der verschlüsselten Stimmen) *nach* der Stimmabgabe [6, 37]. Das Ziel des Zusammenführens dieser beiden Varianten besteht darin, die entsprechenden Vorteile miteinander zu vereinen.

Das Konzept schlägt also vor, dass doppelt gemischt wird. Aus technischer Sicht gibt es dafür zwei konkrete Gründe. Erstens wird beim Ansatz der anonymisierten öffentlichen Schlüssel vorausgesetzt, dass die Stimmen über einen anonymen Kanal abgegeben werden. Da ein perfekt anonymer Kanal in der Praxis schwierig zu realisieren ist (siehe Abschnitt 3.2.3), muss damit gerechnet werden, dass diese Voraussetzung nicht immer bei allen Wählerinnen und Wählern erfüllt ist. Um zu verhindern, dass in einem solchen Fall das Wahlgeheimnis verletzt wird, werden die verschlüsselten Stimmen zusätzlich gemischt. Konkret könnte man zwar durch Abhören des nicht-anonymen Kanals noch in Erfahrung bringen, *dass* jemand abgestimmt hat, aber nicht mehr *wie*.

Zweitens verhindert ein zusätzliches Mischen der verschlüsselten Stimmen, dass diese unmittelbar vor der Entschlüsselung genau gleich aussehen wie beim Abschicken. Andernfalls wäre die abgeschickte Stimme eine direkte Quittung, mit der die verschlüsselte Stimme (und nach der Entschlüsselung auch deren Inhalt) auf dem öffentlichen Anschlagbrett identifiziert werden kann. Eine solche Quittung ist die Voraussetzung für den Verkauf der Stimme. Das zusätzliche Mischen erschwert dies, weil nicht mehr die verschlüsselte Stimme selbst als Quittung dient, sondern nur noch die für die ursprüngliche Verschlüsselung verwendete Randomisierung (siehe Anhang A). Wird den Wählerinnen und Wählern ein vertrauenswürdiges Wahlgerät zur Verfügung gestellt (siehe Abschnitt 3.2.2), mit dessen Hilfe die Verschlüsselung berechnet wird, könnte man verhindern, dass die Randomisierung das Gerät verlässt und als Quittung beim Stimmenkauf missbraucht wird. Unter dieser Annahme ist das vorgestellte System somit quittungsfrei.

Um einen weiteren Schutz gegen den Kauf oder die Erpressung einer Stimme zu bieten, könnte das vorgeschlagene Protokoll mit der in [40] vorgestellten Methode erweitert werden. Dabei geht es darum, ein verifizierbares elektronisches Wahlsystem mit einem

traditionellen System sinnvoll zu kombinieren. Indem an der Urne oder per Briefwahl eine elektronisch abgegebene Stimme *revoziert* und durch eine Papierstimme ersetzt werden kann, wird der Stimmenkauf oder die Erpressung automatisch weniger attraktiv. Denn der Käufer oder Erpresser müsste immer damit rechnen, dass die Stimme später revoziert wird und somit für ihn letztendlich keinen Wert mehr besitzt. Damit wird das System als Ganzes nicht in dem Masse erpressungsfrei wie die Protokolle, die auf diese Anforderung ausgerichtet sind. Der Käufer oder Erpresser könnte zum Beispiel verlangen, dass die Stimme nicht an der Urne revoziert wird, indem er dies am Wahltag durch das Beobachten des Wahllokals überprüft. Anders als in einem rein elektronischen Kontext wäre ein solches Vorgehen aber nicht mehr beliebig skalierbar. Grundsätzlich widerspricht dieser Ansatz jedoch einer Zielsetzung dieser Arbeit (siehe Abschnitt 1.2, Punkt 7), welche das Überstimmen der elektronischen Stimme an der Urne oder brieflich explizit ausschliesst.

3.1.2. Beschreibung des Protokolls

Nachfolgend werden die einzelnen Schritte des vorgeschlagenen Protokolls genauer beschrieben, wobei nicht alle kryptographischen Elemente im Detail erklärt werden (siehe hierzu [23]). Insgesamt können die Schritte in sechs Phasen aufgeteilt werden. Hinzu kommen zwei optionale Phasen für die Verifizierung (individuell und universell) und das Revozieren der Stimme an der Urne oder per Briefwahl. Die Beschreibung dieser Phasen geht von einer einzelnen Wahl auf einer der drei politischen Ebenen (Bund, Kanton, Gemeinde) aus. Würden gleichzeitig mehrere Wahlen stattfinden oder allgemein über mehrere Vorlagen abgestimmt, so müssten in den entsprechenden Phasen gewisse Schritte mehrfach durchgeführt werden. Sollten Instanzen auf mehreren politischen Ebenen involviert sein, so könnte die Durchführung der Wahl entweder von allen Instanzen unabhängig voneinander organisiert werden oder an eine der involvierten Instanzen (z.B. an den Kanton) delegiert werden. Es ist auch denkbar, dass gewisse Aufgaben an eine Instanz delegiert werden, während andere Aufgaben von allen Instanzen einzeln wahrgenommen werden.

In der folgenden abstrakten Beschreibung des Protokolls kommen insgesamt vier verschiedene Personengruppen vor:

- Die *Wahlbehörde* ist zuständig für die Durchführung der Wahl. Sie definiert die Vorlage, die Liste der Kandidierendem (oder allgemein die *Wahloptionen*) sowie das Wählerregister. Sie bestimmt auch den offiziellen Anfang und das Ende des Wahlprozesses. Nach Abschluss der Wahl ermittelt und publiziert sie das Endergebnis.
- Die *Treuhänder* (engl. *Trustees*) übernehmen diejenigen Aufgaben, die auf mehrere Personen verteilt sind (Mischen, Entschlüsseln, Signieren, etc.), um die Robustheit des Systems zu garantieren. Sie erhalten hierzu Teilschlüssel von entsprechenden kryptographischen Schwellwert-Verfahren und müssen möglichst unabhängig sein.
- Die *Wählerschaft* ist die Menge der stimmberechtigten Personen, die an der Wahl teilnehmen können.

- Die *Zertifizierungsstelle* überprüft einmalig die Identitäten der Personen, die an einer elektronischen Wahl teilnehmen wollen. Sie stellt dabei Zertifikate für die vorgelegten öffentlichen Schlüssel aus.

Des Weiteren gibt es eine Gruppe von Personen, die für den zuverlässigen Betrieb des öffentlichen Anschlagbretts verantwortlich sind.

Phase 1: Setup. Die Wahlbehörde und die Zertifizierungsstelle generieren jede für sich ein ElGamal-Schlüsselpaar und publizieren die entsprechenden öffentlichen Schlüssel mit Hilfe von Zertifikaten. Die Treuhänder generieren einen gemeinsamen öffentlichen Schlüssel und einen geteilten privaten Schlüssel. Auch dieser öffentliche Schlüssel wird mittels Zertifikat veröffentlicht. Zuvor müssen entsprechende ElGamal-Parameter (zwei grosse Primzahlen p und q und ein sogenannter Generator g) vereinbart werden. Bei der Wahl dieser Parameter sind die allgemein akzeptierten Richtlinien und Empfehlungen zu beachten. Die Setup-Phase ist ein einmaliger Akt.

Phase 2: Registrierung. Um an einer elektronischen Wahl teilnehmen zu können, generiert die entsprechende Person im Rahmen einer einmaligen Registrierung ein Signatur-Schlüsselpaar. Der öffentliche Schlüssel wird der Zertifizierungsstelle vorgelegt. Nach erfolgreicher Identifikation stellt die Zertifizierungsstelle der Person ein Zertifikat des öffentlichen Schlüssels aus und publiziert dieses in einem öffentlichen Verzeichnis. Die Registrierung ist für jede Person im Prinzip ein einmaliger Akt, der jedoch beim Verlust des privaten Schlüssels wiederholt werden kann. Es ist möglich, dass sich auch nicht-wahlberechtigte Personen registrieren lassen.

Phase 3: Wahlvorbereitung. Die Wahlbehörde stellt aufgrund eines existierenden Wählerregisters oder eines anderen dafür vorgesehenen Quellregisters ein aktuelles Wählerverzeichnis für die elektronische Stimmabgabe zusammen, welches von der Wahlbehörde signiert und auf dem öffentlichen Anschlagbrett publiziert wird. Die Korrektheit dieses Verzeichnisses kann somit öffentlich verifiziert werden. Anschliessend werden die in den Zertifikaten enthaltenen öffentlichen Schlüssel von den Treuhändern gemäss dem in [23] definierten Verfahren anonymisiert. Dies ist ein mehrstufiges Verfahren, bei dem die Treuhänder nacheinander die Liste der öffentlichen Schlüssel mischen. Anschliessend müssen sie beweisen, dass sie das Mischen korrekt durchgeführt haben. Entsprechende Zero-Knowledge Beweise müssen zusammen mit den gemischten Listen auf dem öffentlichen Anschlagbrett publiziert werden. Bei diesem Prozess entsteht zudem ein neuer Generator $\hat{g}$, der dann von den Wählerinnen und Wählern für die anstehende Wahl zum Signieren der Stimmen benutzt werden muss. Bei einer neuen Wahl entsteht jeweils ein neuer solcher Wert.

Im Weiteren definiert die Wahlbehörde eine offizielle Bezeichnung der Vorlage sowie die Liste der Wahloptionen. Im einfachsten Fall beinhaltet diese Liste einzelne Kandidierende (bzw. die Optionen *Ja* und *Nein* bei einer Abstimmung), aus welcher eine Option ausgewählt werden kann. Bei Listenwahlen werden die offiziellen Listen mit den Kandidierenden zusammengestellt. Sollte die Wahl von beliebigen Personen möglich sein

(sogenannte *Write-ins*), also auch von Personen, die nicht auf einer offiziellen Liste aufgeführt sind, dann müssen sich diese vorgängig bei der Wahlbehörde als Kandidierende anmelden (die Liste der offiziellen Kandidierenden kann so beliebig gross werden, muss aber zu Beginn der Wahl fixiert sein). Zudem definiert die Wahlbehörde den offiziellen Beginn und das Ende der Wahl. All diese Informationen werden digital signiert und publiziert. Die gesamte Wahlvorbereitung muss bei jeder Wahl wiederholt werden.

Phase 4: Stimmabgabe. Für die Stimmabgabe verschlüsselt die Wählerin oder der Wähler eine der zur Verfügung stehenden Optionen (die *Stimme*) mit dem öffentlichen Schlüssel der Treuhänder, zum Beispiel mit Hilfe des in Abschnitt 3.2.2 vorgestellten Wahlgeräts. Danach wird ein Zero-Knowledge Beweis erstellt, um zu zeigen, dass die Wählerin oder der Wähler die Randomisierung der Verschlüsselung kennt. Damit wird verhindert, dass bereits abgegebene Stimmen kopiert werden können. Zum Schluss wird die verschlüsselte Stimme mit dem eigenen privaten Schlüssel signiert, wobei hierzu der aktuelle Generator $\hat{g}$ zu verwenden ist. Zusammen mit dem privaten Schlüssel kann daraus der anonymisierte öffentliche Schlüssel berechnet werden. Diese vier Elemente, die verschlüsselte Stimme, der Zero-Knowledge Beweis, die digitale Signatur und der anonymisierte öffentliche Schlüssel, bilden zusammen den elektronischen Stimmzettel, der über einen anonymen Kanal (siehe Abschnitt 3.2.3) auf das öffentliche Anschlagbrett geschickt wird. Hierzu muss dieses zu Beginn der offiziellen Wahlperiode freigeschaltet werden (siehe Abschnitt 3.2.4).

Phase 5: Wahlnachbereitung. Nachdem die Wahl abgeschlossen ist, werden die abgegebenen Stimmzettel überprüft und ungültige Stimmen aussortiert, indem sie auf dem öffentlichen Anschlagbrett entsprechende markiert werden. Hierzu sind fünf Kriterien ausschlaggebend (einige dieser Kriterien können bereits während der Wahl angewandt werden):

- Der anonymisierte öffentliche Schlüssel ist nicht im anonymisieren Wählerverzeichnis enthalten.
- Die digitale Signatur ist ungültig.
- Der Zero-Knowledge Beweis ist ungültig.
- Die Verschlüsselung enthält keine gültige Stimme (dies kann mit dem in [23] vorgestellten Verfahren von den Treuhändern ermittelt werden, ohne die Stimme zu entschlüsseln).
- Unter dem gleichen anonymisierten öffentlichen Schlüssel wurden mehrere Stimmen abgegeben (in diesem Fall werden alle ausser der letzten oder der ersten Stimme gelöscht, je nachdem ob das Überschreiben einer Stimme erlaubt ist oder nicht).

Sämtliche Stimmen, welche dieser Überprüfung standhalten, sind gültig. Aus den oben erwähnten Gründen werden die gültigen Stimmen vor der Entschlüsselung von den Treuhändern in einem verifizierbaren Mix-Netzwerk gemischt, was einer zusätzlichen Anonymisierung gleichkommt. Ähnlich wie beim Mischen der öffentlichen Schlüssel handelt es sich dabei um ein mehrstufiges Verfahren, bei dem die Treuhänder für die einzelnen Schritte entsprechende Zero-Knowledge Beweise vorlegen müssen. Zum Schluss entschlüsseln die Treuhänder gemeinsam die Stimmen und schreiben die Klartext-Stimmen auf das öffentliche Anschlagbrett.

Phase 6: Auszählung. Nach der Wahlnachbereitung kann die Wahlbehörde das Wahlergebnis aufgrund der veröffentlichten Klartext-Stimmen ermitteln und publizieren.

Phase 7: Verifizierung (optional). Für die individuelle Verifizierung kann die Wählerin oder der Wähler auf dem öffentlichen Anschlagbrett überprüfen, ob die abgeschickte Stimme angekommen ist und nicht verändert wurde. Im Fall eines bidirektionalen anonymen Kanals könnte das öffentliche Anschlagbrett auch direkt eine digital signierte Bestätigung der erhaltenen Stimme zurückschicken. Mit Hilfe der bei der Verschlüsselung verwendeten Randomisierung wäre es sogar möglich, die Stimme zu entschlüsseln und somit deren Inhalt nachträglich zu überprüfen.

Für die universelle Verifizierung können sämtliche auf dem öffentlichen Anschlagbrett dokumentierten Schritte nachgerechnet und alle Zero-Knowledge Beweise überprüft werden. Die Korrektheit des Endergebnisses folgt dann als logische Konsequenz.

Phase 8: Revozieren (optional). Zum Revozieren einer Stimme gemäss [40] muss diese von der Wählerin oder vom Wähler wiederverschlüsselt werden. Durch zwei Zero-Knowledge Beweise zeigt man, dass erstens die Stimme einem tatsächlich gehört (hierzu beweist man die Kenntnis des privaten Schlüssels) und zweitens die Wiederverschlüsselung korrekt durchgeführt wurde. Die Treuhänder überprüfen diese Beweise und erlauben danach den Zugang zum traditionellen System (Urnen- oder Briefwahl). Zu diesem Zeitpunkt muss die elektronische Wahl abgeschlossen sein. Die Wiederverschlüsselung wird zudem von den Treuhändern digital unterschrieben und in eine separate elektronische Urne gelegt. Diese kann durch das gleiche öffentliche Anschlagbrett realisiert werden wie die normale elektronische Urne. Am Schluss werden die Stimmen in dieser Urne entschlüsselt und vom Gesamtergebnis abgezogen.

3.2. Komponenten

Das zuvor beschriebene kryptographische Protokoll definiert den Ablauf einer Wahl auf der Ebene der kryptographischen Berechnungen und der ausgetauschten Nachrichten. Das daraus resultierende System ist durch das Protokoll alleine allerdings noch unterspezifiziert. Wichtige offene Fragen betreffen die Wahl der benötigen Systemkomponenten und die damit zusammenhängende Systemarchitektur. Im Folgenden werden die

wichtigsten dieser Komponenten vorgestellt und deren Funktionsweise grob spezifiziert. Zentral dabei ist das in Abschnitt 3.2.2 vorgestellte Wahlgerät, auf dem die wesentlichen Schritte der Stimmabgabe durchgeführt werden. Die Autoren erachten die Existenz eines solchen Geräts zurzeit als den einzigen zulässigen Lösungsansatz für das Problem der sicheren Plattform. Entsprechend müssen die anderen Komponenten auf die zentrale Position des Wahlgeräts ausgerichtet sein. Die folgende Abbildung zeigt vereinfacht den Aufbau des Systems mit den fünf wichtigsten Komponenten. Dabei ist die zentrale Position des Wahlgeräts gut ersichtlich.

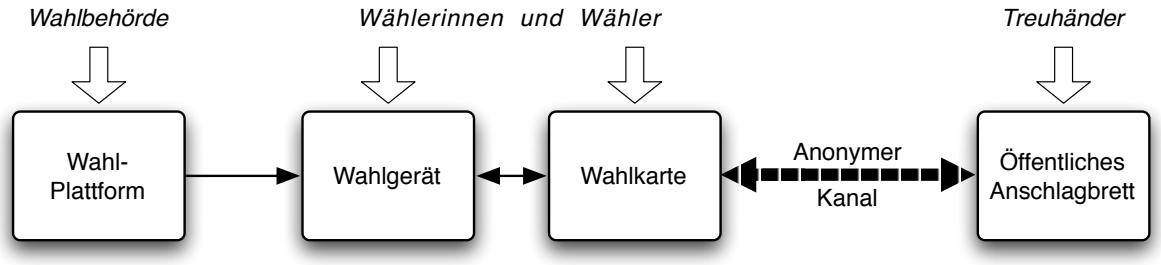

Abbildung 3.1.: Schematischer Aufbau des Wahlsystems mit den fünf wichtigsten Komponenten.

3.2.1. Wahlkarte

Das vorgestellte Protokoll verlangt eine sogenannte *Public-Key Infrastruktur* (PKI) über die gesamte Wählerschaft. Dies bedeutet, dass alle Wählerinnen und Wähler je mit einem Schlüsselpaar ausgestattet werden müssen. Während Zertifikate der öffentlichen Schlüssel in einem Zertifikatsverzeichnis abgelegt sein müssen, werden die privaten Schlüssel von den Wählerinnen und Wählern zum Signieren der Stimmen benötigt. Das Problem dabei ist, dass die privaten Schlüssel so abgespeichert werden müssen, dass sie den Wählerinnen und Wählern immer zur Verfügung stehen. Gleichzeitig dürfen die privaten Schlüssel nicht in fremde Hände geraten, da sie sonst als unerlaubter Zugang zum Wahlsystem missbraucht werden könnten. Um diese Sicherheit zu garantieren, müssen die privaten Schlüssel auf einer speziellen Hardware-Komponente abgespeichert sein, die eindeutig einer bestimmten Wählerin oder einem bestimmten Wähler zugeordnet werden kann. Diese Hardware-Komponente wird im Folgenden *Wahlkarte* genannt, welche den Wählerinnen und Wählern bei der Registrierung abgegeben wird. Bei einer Wahl ermöglicht die Wahlkarte die Abgabe von genau einer Stimme.

Eigenschaften. Die Anforderungen an die Wahlkarte sind vielfältig. Da sie letztendlich dazu dient, einen privaten Schlüssel an eine Person zu binden, müssen neben dem Schlüssel weitere Identifikationsmerkmale dieser Person abgespeichert sein. Neben einer eindeutigen, öffentlich bekannten Bezeichnung der Person (Name, Vorname, Geburtsdatum, ID-Nummer, etc.) ist auch eine bestimmte Form eines Geheimnisses erforderlich, welches für die Freischaltung des privaten Schlüssels und somit für die Benutzung der Wahlkarte offengelegt werden muss. Üblicherweise ist dieses Geheimnis eine PIN, man

könnte sich aber auch verschiedene Formen von biometrischen Daten (Fingerabdruck, Iris, etc.) vorstellen. Da die Wahlkarte nur in grossen zeitlichen Abständen benutzt würde, wäre bei einer rein PIN-basierten Authentisierung die Gefahr gross, dass viele Wählerinnen und Wähler ihre PIN nicht mehr wissen. Somit wäre eine biometrische Form des Geheimnisses wohl die sinnvollere Lösung.

All diese Informationen müssen in einem geschützten Speicher der Wahlkarte abgelegt sein, der bei der Initialisierung des Geräts einmalig beschrieben werden kann. Danach darf es nicht mehr möglich sein, von aussen den Inhalt dieses Speichers zu lesen oder zu verändern. Es geht dabei also darum, einerseits die Benutzung des privaten Schlüssels an den Besitz des Geräts und andererseits die Benutzung des Geräts an die Kenntnis oder den Besitz des Geheimnisses zu binden. Im Fachjargon spricht man dabei von *Tamper-Proof Hardware*, die es in verschiedensten Formen und mit verschiedensten Eigenschaften gibt. Die am weitesten verbreitete Form ist die sogenannte *Smartcard*, die zum Beispiel als Kredit- oder Bankkarte verwendet wird.

Neben dem gesicherten Speicher benötigt die Wahlkarte auch einen grösseren, nicht geschützten Speicherbereich. Dieser dient dazu, die elektronische Stimme nach deren Erstellung auf dem Wahlgerät (siehe folgender Abschnitt) abzuspeichern und zum Abschicken bereitzuhalten. Hierfür bietet sich die Technologie der Flash-EEPROM (Flash-Speicher) an, die sehr zuverlässig sind und heute äusserst preiswert hergestellt werden können. Um von aussen einfach auf diesen Speicher zugreifen zu können, braucht es zudem eine Schnittstelle, die möglichst weit verbreitet ist. Dieses Kriterium trifft heute vor allem für den USB-Standard zu, wobei in absehbarer Zukunft auch eine drahtlose Übertragung denkbar wäre, zum Beispiel mittels *Near Field Communication* (NFC), *Bluetooth* oder andere. Eventuell müsste hierzu den Wählerinnen und Wählern ein entsprechendes Kartenlesegerät zur Verfügung gestellt werden (diese Funktion könnte auch das im nachfolgenden Abschnitt eingeführte Wahlgerät erfüllen).

Nicht zuletzt benötigt die Wahlkarte auch einen Rechenprozessor, um mit Hilfe des privaten Schlüssels die Signatur der Stimme berechnen zu können. Dieser muss also eine genügend hohe Leistung besitzen, um diese Aufgabe in nützlicher Frist erledigen zu können. Wichtig dabei ist, dass die Signatur tatsächlich durch diesen Prozessor selbst berechnet wird, weil sonst der private Schlüssel das Gerät verlassen müsste. Der Prozessor muss so konstruiert sein, dass ein laufender Prozess von aussen nicht beobachtet werden kann. Die in den Smartcards integrierten Prozessoren bieten diese Eigenschaft.

Äusseres Aussehen und Benutzung. Durch die praktische Grösse und das kleine Gewicht bieten sich Smartcards als mögliche Technologie für die Wahlkarte an. Sie besitzen eine hohe Portabilität, sind in der Praxis sehr beliebt, und können in grossen Stückzahlen preisgünstig hergestellt werden. Um verlorene Karten an die Besitzer zurückgeben zu können, könnten diese zudem mit dem Namen des Besitzers beschriftet sein. Als Alternative zu einer Smartcard wäre auch die Form eines Sticks mit integriertem USB-Anschluss denkbar, ähnlich zu den heute weit verbreiteten Flash-Speichern.

Bei der Registrierung wird die Wahlkarte der entsprechenden Person ausgehändigt. Dabei erfolgt die Initialisierung, bei welcher das Schlüsselpaar generiert wird. Der private

Schlüssel wird zusammen mit der PIN oder mit den ermittelten biometrischen Daten im sicheren Speicherbereich abgelegt, während der öffentliche Schlüssel für die Zertifizierung der Zertifizierungsstelle übergeben wird (über den nicht-geschützten Speicherbereich und mit Hilfe der zur Verfügung stehenden Schnittstellen).

Zur Benutzung der Wahlkarte muss diese in einen Kartenleser geschoben werden. Diese Funktion könnte vom nachfolgend beschriebenen vertrauenswürdigen Wahlgerät übernommen werden, ebenso wie die benötigte Stromversorgung. Danach erfolgt die Authentisierung, für die neben dem blossen Besitz der Wahlkarte (*something-you-have*) mindestens ein weiteres Identifikationsmerkmal der Kategorien *something-you-know* (PIN) oder *something-you-are* (Biometrie) erforderlich ist. Für das Eingeben oder Einscannen dieser Daten könnte wiederum das nachfolgend vorgeschlagene Wahlgerät verwendet werden, wobei dieses mit entsprechenden Komponenten und Funktionen versehen werden müsste. Damit ist klar, dass die Wahlkarte und das Wahlgerät bestens aufeinander abgestimmt sein müssen. Bei einer Variante ohne Wahlgerät müsste im Fall einer Smartcard dem Benutzer ein Kartenleser bereitgestellt werden.

3.2.2. Wahlgerät

Das Problem der sicheren Plattform ist eines der am schwierigsten zu lösenden Probleme. Da die gleiche Problematik auch bei anderen kritischen Anwendungen auftritt, gibt es Lösungsansätze, die zum Teil bereits in der Praxis erprobt sind. Grundsätzlich gibt es zwei Kategorien von Ansätzen, je nachdem ob die Applikation ausschliesslich mit den (potentiell unsicheren) persönlichen Geräten der Benutzer auskommen muss, oder ob den Benutzern zusätzliche *vertrauenswürdige Geräte* (im Kontext dieser Arbeit also vertrauenswürdige *Wahlgeräte*) verteilt werden.

- Ohne die Abgabe von Wahlgeräten müsste die Klasse der erlaubten persönlichen Geräte der Benutzer stark eingeschränkt werden, um eine einheitliche Lösung realisieren zu können. Aus Gründen der Verfügbarkeit und Benutzerfreundlichkeit würde die Wahl heute wohl auf die persönlichen PCs und Notebooks zuhause oder am Arbeitsplatz fallen, wobei sich dies beim gegenwärtigen Trend in Richtung mobile Geräte (Smartphones, Tablet-Computer, etc.) verlagern könnte. Um bei den privaten PCs oder Notebooks eine sichere Plattform zu realisieren, gibt es auf dem Markt verschiedene Lösungen, zum Beispiel das Booten ab CD/DVD oder USB-Stick in ein sicheres Mini-Betriebssystem (z.B. ECOS Secure Boot Stick, etc.). Dabei garantieren die Hersteller, dass das Mini-Betriebssystem frei von Schadprogrammen ist und somit Angriffe dieser Art nicht möglich sind. Bei der aktuellen Version von Mac OS X (Lion) wurde ein ähnliches Prinzip implementiert, um den Benutzern das Booten in eine sichere Browser-Umgebung zur Verfügung zu stellen (die tatsächliche Sicherheit dieses Verfahrens kann heute noch nicht abschliessend beurteilt werden).

  Ein grosser Nachteil dieses Ansatzes ist das Problem, dass die existierenden Lösungen nicht auf allen Plattformen in gleicher Weise funktionieren. Zudem gibt es vor allem im geschäftlichen Umfeld viele Geräte, bei denen das Booten ab einem

fremden Datenträger durch bestimmte BIOS-Einträge bewusst unterbunden wird, um keine Schlupflöcher ins Firmennetzwerk zu ermöglichen. Auch ist es durch die Vielzahl der vorhandenen Hardware-Komponenten schwierig, die vollständige Unterstützung durch entsprechende Treiber und Konfigurationen zu garantieren. Obwohl dieser Ansatz grundsätzlich sehr billig zu realisieren wäre, würde er im praktischen Einsatz wohl zu sehr vielen, kaum lösbaren technischen Problemen und entsprechenden Kosten führen.

- Die Abgabe von vertrauenswürdigen Geräten ist vor allem im Bereich des Online-Banking weit verbreitet. In den meisten Fällen realisieren sie mittels eines sogenannten *Challenge-Response* Verfahren eine sichere gegenseitige Authentifizierung zwischen dem Kunden und der Bank. Bei erfolgreicher Authentifizierung, wird dem Kunden im Rahmen einer *Session* der Zugang zum System und somit zu seinem Konto gewährt (die Übertragung der Daten wird durch eine SSL-Verbindung geschützt). Wie kürzlich publik gemacht wurde, reicht dieser Mechanismus jedoch nicht aus, um einen Angreifer abzuwehren, dem es zuvor gelungen ist, ein Schadprogramm auf dem PC des Bankkunden zu installieren.[1] Denn es kann eine zustande gekommene Session unbemerkt an den Angreifer weiterleiten, der dann unzulässige Transaktionen ausführen kann. Hierbei handelt es sich um eine sogenannte *Man-in-the-Browser*-Attacke.

  Ein besseres System ist zum Beispiel der sogenannte *Zone Trusted Information Channel* (ZTIC) der Firma IBM [44], bei dem über die Authentifizierung hinaus jede Transaktion vom Benutzer auf dem Gerät bestätigt werden muss.[2] Das Gerät selbst ist nicht personalisiert, das heisst, für den Betrieb muss eine personalisierte Kundenkarte hineingesteckt werden. Die Verbindung zum PC, auf dem die Online-Banking Session läuft und die Zahlungen erfasst werden, geschieht über die gängige USB-Schnittstelle. Auf dem zweizeiligen Display werden dann die Transaktionen angezeigt, die mittels zwei Eingabeknöpfen entweder bestätigt oder abgebrochen werden können. Die bestätigten Transaktionen werden anschliessend direkt auf dem Gerät verschlüsselt und signiert und via PC des Benutzers über das Internet an die Bank geschickt. Somit wird bezüglich der Korrektheit der in Auftrag gegebenen Zahlungen die unsichere Plattform des privaten Kunden-PCs umgangen. Entscheidend dabei ist das Bereitstellen eines *sicheren Displays*, dem die Benutzer vertrauen können. Die Privatsphäre könnte allerdings durch Schadprogramme weiterhin verletzt werden.

Neben diesen beiden Hardware-basierten Lösungsansätzen wäre auf Protokoll-Ebene noch das Code-Voting ein möglicher Lösungsansatz für das Problem der sicheren Plattform (siehe Abschnitt 2.2). Die verschiedenen Nachteile und die zusätzlichen Probleme von Code-Voting wurden bereits diskutiert. Aus diesen Gründen wird diese Variante in dieser Arbeit nicht weiter in Betracht gezogen.

In Anbetracht der obigen Diskussion sieht das Konzept den Einsatz eines Wahlgeräts vor, welches nach einem ähnlichen Prinzip wie das ZTIC-Gerät der Firma IBM funktioniert.

[1] Siehe *Kassensturz* (SF1) vom 31. Mai 2011.

[2] Dieses Gerät wird unter anderem von der UBS unter dem Namen *UBS Access Key* benutzt.

Entscheidend ist, dass die eigentliche Wahlhandlung auf dem Gerät bestätigt werden kann. Allerdings reicht das dem ZTIC-Gerät zugrunde liegende Prinzip nicht aus, um die Anforderungen eines sicheren Wahlgeräts zu erfüllen. Das Problem ist der fehlende Schutz des Wahlgeheimnisses, welches durch Schadprogramme in gleicher Weise verletzt werden könnte, wie ohne ein solches Gerät. Im Folgenden wird deshalb ein Wahlgerät vorgestellt, welches sich in einigen Punkten grundsätzlich vom ZTIC-Gerät unterscheidet, jedoch eine ähnlich einfache Handhabung bietet, selbst bei komplexen Wahlen mit frei zusammengestellten Listen. Das Wahlgerät wird gleichzeitig als Kartenleser für die Wahlkarte dienen und den Authentifizierungsprozess unterstützen.

Zum Bestätigen der Wahlhandlung benötigt das Wahlgerät mindestens eine Ausgabe (Display, Braillezeile) sowie eine einfache Eingabemöglichkeit. In Anbetracht der heutigen technischen Möglichkeiten würde sich als typisches Ausgabegerät ein relativ grosses, hochauflösendes und berührungsempfindliches Display (Touchscreen) anbieten, wie es in den modernen Smartphones oder Tablet-Computern üblich ist. Man kann sich gut vorstellen, wie auf einem solchen Gerät selbst sehr komplexe Wahlhandlungen (inkl. Kumulieren, Panachieren, Streichen, etc.) einfach und intuitiv umzusetzen wären. Problematisch bei einer solchen Lösung sind aber mindestens zwei Punkte. Zum einen wären die Kosten für die Entwicklung und Produktion des Geräts und der Systemsoftware äusserst gross. Dies könnte sich in Zukunft, wenn die Verfügbarkeit von entsprechenden Hardware-Komponenten weiter zunimmt, ändern. Aus heutiger Sicht ist diese Variante aber schon aus Kostengründen nicht realistisch. Zum anderen kommt hinzu, dass die hohe Komplexität eines solchen Geräts die Möglichkeit offen lassen müsste, Updates der Systemsoftware auf das Gerät spielen zu lassen. Dies wäre aber gleichzeitig eine Einfallspforte für Schadprogramme und würde deshalb das Prädikat „vertrauenswürdig“ grundsätzlich in Frage stellen. Idealerweise ist das Wahlgerät also genügend einfach, damit auf das Updaten der Systemsoftware verzichtet werden kann. Die im Folgenden vorgeschlagene Variante geht deshalb von einem minimalen, nicht berührungsempfindlichen Display aus. Ähnlich wie das ZTIC-Gerät der Firma IBM könnte es zum Beispiel zwei Zeilen zu je ca. 40 Zeichen besitzen. Für die Bestätigung der Wahlhandlung müssten zudem mindestens zwei Knöpfe (OK, Abbruch) vorhanden sein.

Funktionsweise des Wahlgeräts. Die Grundidee des Geräts liegt darin, dass die Wahlhandlung (z.B. das Auswählen oder Erstellen einer Liste von Kandidierenden) auf dem privaten Endgerät des Benutzers vorbereitet, jedoch nicht vollzogen wird. Für die Vorbereitung kommen die unterschiedlichsten Gerätetypen (PCs, Notebooks, Smartphones, Tablet-Computer, etc.) und Plattformen (Web, Java, Apps, etc.) in Frage. Die Wahlvorbereitung könnte sogar auf Papier erfolgen, insbesondere bei einfachen Ja/Nein-Abstimmungen (siehe unten). Das Ziel dabei ist, auch bei komplexen Wahlhandlungen den Wählerinnen und Wählern die hohe Benutzerfreundlichkeit ihrer vertrauten Endgeräte zur Verfügung zu stellen. Das Zusammenstellen einer Liste von Kandidierenden könnte zum Beispiel auf einem Tablet-Computer mit Touchscreen (iPad, Android) einfach und intuitiv umgesetzt werden.

Um beim Vorbereiten der Wahlhandlung auf einem unsicheren privaten Endgerät das Wahlgeheimnis nicht zu tangieren, darf das benutzte Gerät nicht erkennen können, zu

welchem Zeitpunkt die konkrete Wahlhandlung erfolgt. So muss in jedem Fall vermieden werden, dass nach Abschluss der Wahlvorbereitung diese Information gezielt an das Wahlgerät geschickt wird (wie es bei den Bank-Transaktionen mittels ZTIC-Gerät der Fall ist), weil gleichzeitig ein Schadprogramm die gleiche Information anderweitig verwenden könnte. Technisch gesehen darf zwischen den beiden Geräten keine synchrone Kommunikation stattfinden.

Um dies zu erreichen, sieht das Konzept vor, dass die Wahlhandlung optisch codiert am Display des privaten Endgeräts dargestellt wird. Dafür würde sich die Technologie der *Matrixcodes* (2D-Barcodes) bestens eignen. Diese haben eine genügend grosse Kapazität und können mittels einer preiswerten, ins Wahlgerät eingebrachten Kamera, einfach eingelesen werden.[3,4] Konkret könnte man sich also vorstellen, dass die Software für die Wahlvorbereitung ständig (z.B. beim Durchblättern durch die vorgegebenen Wahllisten) den entsprechenden Matrixcode anzeigt. Ein auf dem privaten Gerät des Benutzers installiertes Schadprogramm könnte somit nicht feststellen, wann der Matrixcode von der Kamera des Wahlgeräts erfasst wird. Bei Ja/Nein-Abstimmungen könnten sogar stets die Matrixcodes von beiden Optionen angezeigt werden, wobei nur einer davon eingelesen wird. Interessant bei diesem Vorgehen ist die Möglichkeit, die Matrixcodes zu drucken, zum Beispiel in den offiziellen Wahlunterlagen, in Zeitungen, auf Plakaten, etc. Das erfolgreiche Einlesen eines Matrixcodes auf dem Wahlgerät könnte durch ein optisches oder akustisches Signal bestätigt werden. Dieses Vorgehen ist in der Abbildung 3.2 schematisch dargestellt. Technisch gesehen führt der Bildschirm, auf dem der Matrixcode dargestellt wird, ein „optisches Broadcasting“ für ein anonymes Empfangsgerät durch.

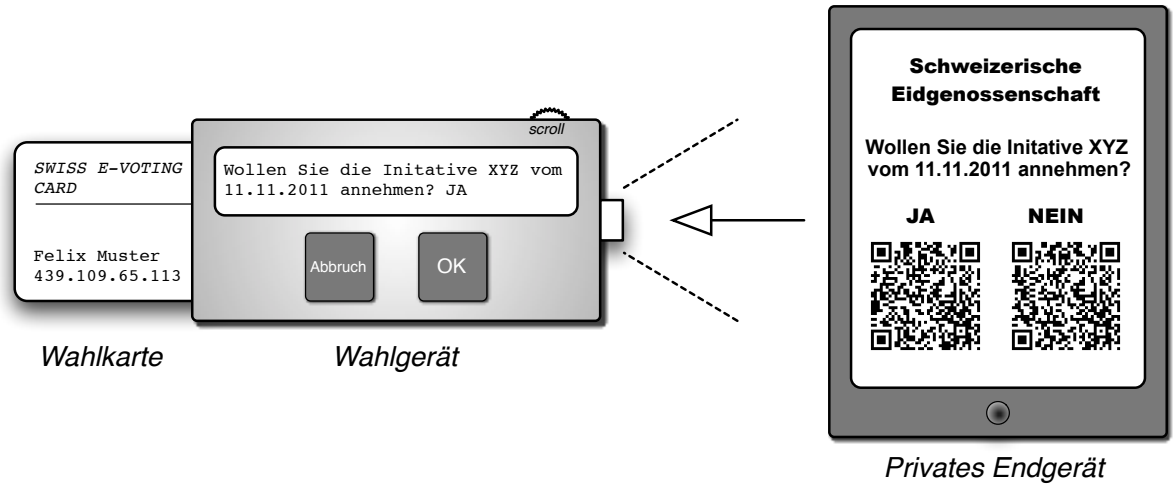

Abbildung 3.2.: Optische Datenübertragung mittels Matrixcode zwischen privatem Endgerät und Wahlgerät.

Um Täuschungen der Wählerinnen und Wähler mittels ungültigen oder vertauschten

[3]Die in Biel ansässige Firma AXSionics bietet ein ähnliches Gerät mit einem optischen Kanal an, der sogenannte *AXSionics Internet Passport*. Die dabei verwendeten *Flicker-Codes* besitzen aber eine kleinere Kapazität, sind im Gebrauch eher unbekannt, und können nicht gedruckt werden.

[4]Ein solche optische Datenübertragung mittels Matrixcode benutzen die SBB, um die auf einem Smartphone gekauften Fahrscheine zu kontrollieren.

Matrixcodes zu verhindern, gibt es zwei Vorkehrungen. Erstens kann die im Matrixcode enthaltene Information (oder Teile davon, z.B. das Datum und der offizielle Text der Vorlage) von der Wahlbehörde digital signiert und vor der Wahl veröffentlicht werden. Für diesen Fall muss das Wahlgerät mit dem öffentlichen Schlüssel der Wahlbehörde (oder einem entsprechenden Zertifikat) ausgestattet sein, um solche Signaturen überprüfen zu können. Eingelesene Codes mit ungültiger Unterschrift werden vom Gerät abgelehnt. Zweitens würde das Wahlgerät die erhaltene Information unmittelbar auf dem Display anzeigen. Bei einer Wahlliste, die zum Beispiel auf einem zweizeiligen Display keinen Platz findet, muss es somit die Möglichkeit geben, die Liste auf dem kleinen Display durchzuscrollen (z.B. mittels zweier Scroll-Knöpfe oder einem Scroll-Rad). In einem solchen Fall könnte das Gerät den Benutzer sogar anweisen, sich durch die ganze Liste durchscrollen zu müssen, bevor es eine Bestätigung der Wahl zulässt. Dabei geht es darum, dass die Wählerinnen und Wähler die Wahlhandlung auf dem Wahlgerät immer vollständig überprüfen und diese erst dann mittels der entsprechenden Eingabeknöpfe bestätigen oder verwerfen.

Wird eine Wahlhandlung auf dem Wahlgerät bestätigt, so wird die elektronische Stimme gemäss dem in Abschnitt 3.1 vorgestellten kryptographischen Protokoll erstellt und im Datenspeicher der Wahlkarte abgelegt. Dieser Datenspeicher könnte sich auch auf einem weiteren Gerät befinden, zum Beispiel auf einem herkömmlichen USB-Stick, der im Wahlgerät eingesteckt wird (ein weiteres Gerät würde das Konzept jedoch unnötig kompliziert machen und verteuern). Bei Wahlen oder Abstimmungen mit mehreren Vorlagen müsste dieser Vorgang (das Einlesen, Bestätigen und Abspeichern der Stimme) entsprechend oft wiederholt werden.

Zum Schluss müssen die gesammelten elektronischen Stimmen gemäss Protokoll über den anonymen Kanal an das öffentliche Anschlagbrett geschickt werden. Hierzu muss der Datenspeicher der Wahlkarte mit dem Internet verbunden werden, zum Beispiel über die weit verbreitete und kostengünstige USB-Schnittstelle. Um das Abschicken der Stimmen möglichst zu vereinfachen, könnten hierfür unterschiedliche Kanäle und Schnittstellen gleichzeitig zur Verfügung gestellt werden (z.B. NFC, WLAN, Bluetooth, etc.), dies würde jedoch die Kosten des Geräts entsprechend erhöhen. Wichtig ist, dass dieser letzte Schritt unter allen Umständen genauso intuitiv und zuverlässig abläuft wie die Schritte zuvor.

Aufbau des Wahlgeräts. Eine Möglichkeit für das äussere Aussehen und den Aufbau des Wahlgeräts ist in Abbildung 3.2 ersichtlich, wobei die Art, Grösse und Anordnung der einzelnen Komponenten ergonomisch optimiert werden müsste. Die minimalen äusseren Komponenten sind die folgenden:

- ein Schalter zum Ein- und Ausschalten des Geräts,
- ein Anschluss für die Wahlkarte,
- ein mindestens zweizeiliges Display zu je ca. 40 Zeichen,
- zwei Eingabeknöpfe zum Bestätigen oder Abbrechen,

- zwei Scroll-Knöpfe (Up/Down) oder ein Scroll-Rad,
- eine Kamera mit relativ geringer zweidimensionaler Auflösung (ab VGA),
- ein Auslöseknopf für die Kamera,
- entweder ein Batteriefach oder eine externe Stromversorgung (evtl. in Kombination mit einem Akku).

Aus ergonomischen Gründen könnte es sinnvoll sein, gewisse dieser Elemente zusammenzuführen, zum Beispiel der Auslöseknopf für die Kamera und der Knopf für die Bestätigung der Wahl. Zudem könnte eine USB-Schnittstelle zum Abschicken der Stimme nützlich sein, falls diese nicht bereits durch die Wahlkarte zur Verfügung gestellt wird. Diese könnte gleichzeitig als Stromquelle dienen. Und nicht zuletzt müsste für die Authentisierung des Benutzers gegenüber der Wahlkarte eine weitere Komponente die Eingabe der persönlichen Identifikationsmerkmale (PIN, Fingerabdruck, Sprachsample, etc.) ermöglichen. Eventuell könnte diese Aufgabe von der Kamera übernommen werden. Das erfolgreiche Authentisieren oder das Erkennen eines Matrixcodes könnte zudem noch durch ein akustisches Signal bestätigt werden.

Die internen Komponenten des Wahlgeräts dienen dazu, die äusseren Komponenten zu steuern und zu einem Gesamtsystem zusammenzufügen. Wichtig ist, dass dabei ein Rechenprozessor vorgesehen wird, der die benötigten Aufgaben (Erkennung und Decodierung des Matrixcodes, Berechnen von kryptographischen Primitiven, etc.) bewältigen kann. Auf eine genauere Beschreibung der inneren Systemarchitektur und der Systemsoftware wird an dieser Stelle verzichtet.

Eigenschaften und Kosten. Die Qualität eines vertrauenswürdigen Geräts wird anhand unterschiedlicher Kriterien beurteilt. Gemäss [44] beinhaltet diese Kriterienliste mindestens die folgenden sechs Punkte (auf eine deutsche Übersetzung der Begriffe wird verzichtet):

Reasonableness: Die durch das Gerät generierte Sicherheit sollte für den Benutzer intuitiv erkennbar und verständlich sein. Da das vorgestellte Wahlgerät wegen der optischen Datenübertragung nicht direkt mit dem Internet verbunden werden muss (siehe Abbildung 3.1), ist leicht zu erkennen, dass es nicht von Schadprogrammen befallen werden kann.

Convenience: Das Gerät sollte möglichst einfach zu bedienen sein und bekannten Interaktionsmustern entsprechen. Durch die minimale Ausstattung mit wenigen Eingabeknöpfen und klar definierten Funktionen sollte eine einfache Bedienung des vorgestellten Wahlgeräts auch bei komplexen Wahlhandlungen gegeben sein. Das Einlesen des Matrixcodes ist jedoch etwas unüblich, sollte aber mittels einfachen Instruktionen auch für technisch weniger versierte Benutzer zu bewältigen sein. Auch das allfällige Scannen des Fingerabdruckes ist nicht besonders weit verbreitet, stellt aber keine ausserordentlichen Anforderungen an die Benutzer.

Mobility: Das Gerät sollte leicht transportierbar und möglichst ohne Installation überall einsetzbar sein. Durch das kleine Display und die minimale Ausstattung sollte es möglich sein, ein Wahlgerät von bescheidener Grösse und Gewicht zu bauen. Installationen sind keine notwendig. Eine allfälliger USB-Anschluss für das Abschicken der Stimme ist auf allen gängigen PCs und Notebooks vorhanden.

Integration: Das Gerät sollte gut in bestehende System integrierbar sein. Ausser einer allfälligen USB-Schnittstelle, für welche die Integration praktisch überall gegeben ist, stellt das vorgestellte Wahlgerät diesbezüglich keine besonderen Anforderungen.

Administration: Das Gerät sollte einfach zu administrieren sein, zum Beispiel durch ein Fern-Update der Systemsoftware. Da das vorgestellte Wahlgerät aus den genannten Gründen auf System-Updates verzichtet, erübrigt sich dieses Kriterium.

Cost: Die Kosten für die Entwicklung und Produktion sollten pro Gerät relativ klein sein. Die minimale Ausstattung, insbesondere der Verzicht auf ein hochauflösendes und berührungsempfindliches Display, sollte das vorgestellte Wahlgerät nicht allzu teuer werden lassen. Genauere Angaben zu einem möglichen Preis können zurzeit jedoch nicht gemacht werden.

Da der Preis des Wahlgeräts bei einer möglichen Umsetzung dieses Konzepts ein wichtiger Faktor sein wird, könnte die Möglichkeit von grosser Bedeutung sein, das Wahlgerät statt an alle Wählerinnen und Wähler nur an alle Haushalte zu verteilen. Sollten mehr Wahlgeräte pro Haushalt erwünscht sein, könnten die Kosten für die zusätzlichen Geräte den entsprechenden Personen angelastet werden. Um die Kosten weiter zu senken, könnte man sich auch die Nutzung des Geräts für andere Zwecke vorstellen, zum Beispiel fürs Online Banking oder in Kombination mit der SuisseID.

Ein bemerkenswerter Punkt bezüglich einer möglichen Umsetzung ist die Tatsache, dass mit AXSionics und IBM zwei der weltweit führenden Firmen im Bereich von solchen Geräten in der Schweiz angesiedelt sind. Potentielle Industriepartner mit entsprechendem Knowhow sind also in unmittelbarer Nähe vorhanden.

3.2.3. Anonymer Kanal

Um sämtliche Aspekte des Wahlgeheimnisses zu wahren, ist gemäss Protokoll ein anonymer Kanal für die Stimmabgabe unerlässlich. Dieser verhindert, dass während des Wahlprozesses bekannt wird, wer bereits an der Wahl teilgenommen hat und wer nicht. Andernfalls könnten daraus unter gewissen Umständen vorzeitig Schlüsse über den Ausgang der Wahl gezogen werden und diese somit eine gerechte Wahl verhindern (siehe Abschnitt 2.1). Aus dem gleichen Grund ist auch für die individuelle Verifizierung ein anonymer Kanal erforderlich.

Konkret bedeutet dies, dass der Kanal zwischen der stimmberechtigten Person und dem öffentlichen Anschlagbrett gleichzeitig *Sender-anonym* (zum Abschicken der Stimme) und *Empfänger-anonym* (zum Empfangen der für die Verifizierung nötigen Information) sein muss, um die Stimmabgabe und die anschliessende Verifizierung in einem Schritt zu

erledigen. Technisch gesprochen ist also ein sogenannter *bidirektionaler anonymer Kanal* zwingend, der beide Anonymitätseigenschaften gleichzeitig anbietet. Im Folgenden werden verschiedene Techniken und Vorgehensweisen aufgezeigt, wie ein solcher Kanal in der Praxis realisiert werden könnte.

Stimmabgabe von zuhause aus. Die meisten Wählerinnen und Wähler werden es wohl bevorzugen, von zuhause aus ihre Stimme abzuschicken. In diesem Fall ergibt sich das Problem, dass die Internet-Provider die elektronische Abgabe der verschlüsselten Stimme zwangsweise nachvollziehen können, da sie den Datenverkehr vom heimischen Endgerät und zum heimischen Endgerät kennen. Sie können theoretisch also in Besitz des Wissens gelangen, wer (oder zumindest welcher Haushalt) abgestimmt hat. Um diesen Umstand zu vermeiden, muss der anonyme Kanal also bereits im Endgerät der Wählerinnen und Wähler seinen Anfang nehmen. Der Kanal muss somit, wie bereits erwähnt, die Eigenschaft eines bidirektionalen anonymen Kanales haben. Für den Bau von solchen Kanälen gibt es in der Literatur verschiedene Ansätze.

Eine konkrete Umsetzung eines anonymen Kanals mit genau dieser bidirektionalen Anonymitätseigenschaft ist beispielsweise mit der zweiten Generation von TOR grundsätzlich gegeben [17, 22]. TOR ist das wohl bekannteste der sogenannten *Anonymisierungsnetzwerken* und verarbeitet momentan weit mehr als 100′000 simultane Benutzeranfragen ohne längere Wartezeiten [29]. TOR beruht auf einem in der Wissenschaft als *Onion-Routing* bekanntes Verfahren, welches sehr gut erforscht und beschrieben ist [20]. Im kostengünstigsten Fall könnte also direkt auf diese Lösung zurückgegriffen werden. Es gilt zu beachten, dass der Einsatz solch eines Netzwerks den Wählerinnen und Wählern keinerlei Einschränkungen auferlegt, dementsprechend also die Akzeptanz sehr hoch sein sollte. Im Weiteren wäre es auch denkbar, eine eigene Implementierung und Infrastruktur dieser Art des anonymen Kanals zur Verfügung zu stellen, welche ausschliesslich für die Abgabe der elektronischen Stimme zum Einsatz käme. Dies ist möglich, da sowohl die Dokumentation als auch der Quellcode von TOR öffentlich zugänglich sind. Dennoch ist der Aufwand für eine auf die elektronische Stimmabgabe zugeschnittene Lösung nicht zu unterschätzen.

Stimmabgabe im öffentlichen Raum. Eine Möglichkeit, auf den Einsatz eines speziellen Anonymisierungsnetzwerkes zu verzichten, bietet die elektronische Stimmabgabe an einem öffentlichen Zugangspunkt zum Internet ohne personenbezogene Identifizierung. In diese Kategorie gehören öffentliche WLAN-Netze, welche in einzelnen Städten bereits an vielen Standorten angeboten werden, sowie fremde Endgeräte in Internet-Cafés, Bibliotheken, etc. Beim Einsatz eines persönlichen mobilen Endgeräts im öffentlichen Raum muss darauf geachtet werden, dass die Verbindung zum Internet nicht über das mobile Funknetz (3G, UMTS) realisiert wird, sondern immer über WLAN. Im mobilen Funknetz sind die Benutzer vertraglich an die Provider gebunden, und somit findet eine personenbezogene Identifikation statt.

Grundsätzlich bietet die Dislozierung in den öffentlichen Raum ein geeignetes Mittel, um eine akzeptable Anonymität zu erreichen. Allerdings ist dies für die Wählerinnen

und Wähler nicht immer sehr komfortabel, so dass diese Möglichkeit wohl nur im Ausnahmefall zum Einsatz kommen wird.

Abblauf der Stimmabgabe und der individuellen Verifizierung. Nachdem die Wählerin oder der Wähler die Stimme auf dem Wahlgerät bestätigt hat, wird der elektronische Stimmzettel gemäss dem Protokoll erstellt und im Speicher der Wahlkarte in Form von entsprechenden Dateien abgelegt (siehe Abschnitt 3.1.2 und Abschnitt 3.2.2). Die Frage stellt sich nun, wie diese Dateien über ein Anonymisierungsnetzwerk an das öffentliche Anschlagbrett geschickt werden.

Grundsätzlich erfolgt die eigentliche Stimmabgabe durch das Auslesen der Dateien über die vorhandene Schnittstelle an ein handelsübliches Endgerät. Ein im schreibgeschützten Bereich der Wahlkarte abgelegtes Programm, welches universell auf den Endgeräten ausgeführt werden kann, wird nun von den Wählerinnen und Wählern gestartet. Dieses initiiert sodann den Zugang zum anonymen Kanal. Sobald dieser aufgebaut ist, sendet das besagte Programm die Datei über diesen Kanal an das öffentliche Anschlagbrett und erwartet ab dann über diesen Kanal eine positive Rückmeldung. Diese Rückmeldung besteht im Wesentlichen aus dem von der Wahlbehörde signierten elektronischen Fingerabdruck der abgesandten Stimme. Die Rückmeldung schreibt das Programm in den öffentlich zugänglichen Speicher der Wahlkarte zurück. Ist dieser Vorgang beendet, wird der anonyme Kanal abgebaut und das Programm beendet. Nun kann die erhaltene Signatur auf dem Wahlgerät verifiziert werden. Erst jetzt ist sicher, dass die korrekte Stimme in der elektronischen Wahlurne angekommen ist und dort korrekt gespeichert wurde.

3.2.4. Öffentliches Anschlagbrett

Ein elektronisches, öffentliches Anschlagbrett bezweckt das vertrauenswürdige Publizieren von Informationen. Es besteht aus einer geordneten Liste von Einträgen. Jeder neue Eintrag wird am Ende der Liste angefügt. Ein Eintrag beinhaltet nebst der zu publizierenden Information zusätzliche Kontrolldaten. Würden ein oder mehrere bestehende Einträge gelöscht oder geändert, oder würden ein oder mehrere neue Einträge vor dem Ende eingefügt, so könnte dies aufgrund der bereits veröffentlichten Daten von einer beliebigen Person eindeutig nachgewiesen werden. Man spricht von der unveränderbaren Historie des Anschlagbretts [24]. Diese Eigenschaft wird durch das Verknüpfen des neuen Eintrags mit allen vorangehenden und einer digitalen Signatur erreicht.

Ein Eintrag kann nur von akkreditierten Personen, wie zum Beispiel von Wählerinnen oder Wählern, erfolgen. Die Überprüfung der Akkreditierung läuft auf das Prüfen der digitalen Unterschrift des Senders des Eintrags hinaus, was wiederum durch beliebige Personen gemacht werden könnte. Das Anschlagbrett bestätigt die Korrektheit der Kontrolldaten und der Signatur des Senders, indem es denselben Eintrag ebenfalls digital signiert.

Eine beliebige Person kann die Einträge des öffentlichen Anschlagbretts jederzeit lesen. Liest jemand den Inhalt des Anschlagbretts zu einem bestimmten Zeitpunkt, und liest

diese Person das Anschlagbrett nochmals zu einem späteren Zeitpunkt, so entspricht der Inhalt des Anschlagbretts des späteren Zeitpunkts genau dem Inhalt des ersten Zeitpunkts plus den in der Zwischenzeit zusätzlich hinzugefügten Einträgen. Alle anderen Einträge sind unverändert und ohne Änderung der Reihenfolge gleich. Ein Anschlagbrett mit dieser Eigenschaft wird als *append-only* bezeichnet.

Betrügerische Absprachen zwischen einer akkreditierten Person und dem Anschlagbrett können mit obigen Eigenschaften nicht verhindert werden. Somit könnte zum Beispiel eine akkreditierte Person mehrere Male Informationen auf dem Anschlagbrett publizieren. Dies könnte aber festgestellt werden, denn alle Einträge müssen die Signatur der betrügerischen akkreditierten Person sowie diejenige des Anschlagbretts enthalten. Ein Entfernen, Verändern oder Einfügen eines bestehenden Eintrags würde trotz der betrügerischen Absprache nach wie vor durch alle entdeckt.

Es ist allerdings nicht einfach, ein öffentliches Anschlagbrett zu implementieren, welches resistent gegenüber einem totalen Datenverlust, zum Beispiel durch den Totalausfall seiner Speichergeräte, ist. In [24] wird zwar auf die Möglichkeit, ein verteiltes öffentliches Anschlagbrett zu implementieren, hingedeutet, eine genaue Beschreibung fehlt jedoch. In seiner Master-Arbeit aber zeigt Peters [34], wie man ein verteiltes, robustes öffentliches Anschlagbrett zu implementieren hat. Die Implementierung stützt sich auf Arbeiten von Reiter ab [35, 36]. Diese beschreiben Lösungen für ein verteiltes, robustes öffentliches Anschlagbrett für den Fall, dass weniger als ein Drittel der beteiligten Komponenten ausfallen oder sich betrügerisch verhalten. Es konnte gezeigt werden, dass der Wert $1/3$ eine Schranke ist, welche unter keinen Umständen überschritten werden kann.

Wählerverzeichnis. Damit beliebige Personen überprüfen können, dass nur berechtigte Stimmen in die elektronische Urne gelegt und am Schluss gezählt werden, muss öffentlich bekannt sein, wer das Stimm- oder Wahlrecht hat. Dazu publiziert die Wahlbehörde die anonymisierten öffentlichen Schlüssel der Wählerinnen und Wähler auf dem öffentlichen Anschlagbrett. Folglich darf sich in der nachfolgend beschriebenen elektronischen Urne maximal ein Eintrag pro Schlüssel befinden, welcher von dessen Besitzerin oder Besitzer signiert ist. Dies kann von jedermann überprüft werden. Hierzu eignet sich eine spezielle Variante des öffentlichen Anschlagbretts, bei der die anonymisierten Schlüssel als eine einzelne Meldung von der Wahlbehörde publiziert werden.

Elektronische Urne. Die elektronische Urne ist ein öffentliches Anschlagbrett. Somit können die Wählerinnen und Wähler prüfen, ob ihre verschlüsselten Stimmen publiziert und ob sie später nicht verändert oder gelöscht wurden. Sie können sich auch vergewissern, dass nur Stimmen publiziert wurden, welche zu einem anonymisierten öffentlichen Schlüssel passen, der sich auf dem öffentlichen Anschlagbrett der Wahlbehörde befindet. Zur Bekanntgabe der Ergebnisse werden die entschlüsselten Stimmen durch die Wahlbehörde wiederum auf dem öffentlichen Anschlagbrett als eine einzelne Meldung publiziert.

Die volle temporale Verfügbarkeit des öffentlichen Anschlagbretts für die elektronische Urne führt unweigerlich dazu, dass man den zeitlichen Verlauf der Beteiligung der Wählenden kennt. Dies kann schon zu viel Information sein, die vor der Bekanntgabe des Resultats aus dem Wahlsystem entnommen werden kann. Eine Gegenmassnahme kann die temporale Einschränkung der Sichtbarkeit des öffentlichen Anschlagbretts sein. Man könnte zum Beispiel das Anschlagbrett erst nach Bekanntgabe des Resultats veröffentlichen, mit dem Nachteil, dass die Wählenden erst im Nachhinein ihre Prüfungen vornehmen könnten. Eine andere Gegenmassnahme wäre, das Anschlagbrett nicht öffentlich zu betreiben, sondern die Einträge nur für eine kleine Gruppe von berechtigten Personen, zum Beispiel Wahlbeobachter, sichtbar zu machen. Dies würde jedoch die Implementierung und den Betrieb eines Anschlagbretts weiter erschweren, weil zusätzliche Sicherheitsanforderungen erfüllt werden müssen.

3.2.5. Wahlplattform

Die beiden vorgeschlagenen Hardware-Komponenten (Wahlkarte, Wahlgerät) bilden zusammen mit dem anonymen Kanal und dem öffentlichen Anschlagbrett den Kern de Wahlsystems. Bei der Realisierung dieser Komponenten müssen die höchstmöglichen Sicherheitskriterien angewandt werden. Zudem muss die Zuverlässigkeit unter allen erdenklichen Gegebenheiten gewährleistet sein. Anders sieht es bei der offiziellen *Wahlplattform* aus, die von der Wahlbehörde der Wählerschaft zur Verfügung gestellt werden muss, damit diese die Stimmabgabe gemäss dem in Abschnitt 3.2.2 vorgestellten Verfahren vorbereiten können. Hierzu reicht eine einfache Webseite, die über eine gewöhnliche HTTPS-Verbindung zwischen Server und Client abgesichert ist. Entscheidend ist, dass die Wahl in jedem Fall auf dem vertrauenswürdigen Gerät bestätigt werden muss, so dass eine „gehackte“ Wahlplattform, in der zum Beispiel die Matrixcodes der verschiedenen Wahloptionen vertauscht worden sind, von den Wählerinnen und Wählern sofort erkannt würde. Da nur ein unidirektionaler Informationsfluss von der Plattform zu den Wahlgeräten stattfindet, kann der Inhalt der Wahlplattform zudem beliebig repliziert werden. Man könnte sich zum Beispiel vorstellen, dass man zur Wahlvorbereitung statt der offiziellen Wahlplattform die Webseite der bevorzugten Partei besucht, in welcher entsprechende Matrixcodes der Parteilisten angezeigt werden. Das Generieren der Matrixcodes ist übrigens sehr einfach zu bewerkstelligen.

Der Fakt, dass nur äusserst geringe Sicherheitsvorkehrungen bei der Wahlplattform nötig sind, ist eine der bemerkenswertesten Eigenschaften des vorgeschlagenen Konzepts. Es gibt keine registrierten Benutzer, keinen Login-Prozess und keine geheimen Daten. Demzufolge bietet die Plattform praktisch keine Angriffsfläche und ist entsprechend kostengünstig zu realisieren. Zusätzlich könnte die Plattform als spezialisierte Applikationen für die verschiedenen mobilen Geräte (Smartphones, Tablet-Computer, etc.) zur Verfügung gestellt werden, ohne wesentlich grössere Kosten zu verursachen.

Im Speziellen Fall von Ja/Nein-Abstimmungen (oder bei einfachen Wahlen mit wenigen Kandidierenden) wäre es auch denkbar, die beiden möglichen Matrixcodes auf Papier zu drucken und über klassische Kanäle zu verteilen. Das Einlesen der Codes ins Wahlgerät würde dann direkt ab Papier erfolgen. Solange das Abstimmungsmaterial weiterhin per

Post verschickt wird, könnten die beiden Codes einfach dem Material beigelegt werden. Alternativ könnten die Codes auch in Zeitungen (oder über andere vergleichbare Kanäle) publiziert werden. Interessant bei diesem Gedanken ist die Tatsache, dass es gar keine Wahlplattform mehr geben müsste.

3.2.6. Weitere Komponenten

Neben den zuvor beschriebenen Hauptkomponenten sind bei einer Realisierung des Systems einige zusätzliche Komponenten erforderlich. Diese betreffen die Wählerinnen und Wähler nicht direkt und sind somit leichter zu realisieren, weil die verwendeten Geräte gezielt gegen Schadprogramme oder andere Angriffe geschützt werden können. In der folgenden Auflistung werden die wichtigsten dieser Zusatzkomponenten und ihre Funktionen kurz diskutiert.

- Die Zertifizierungsstelle benötigt eine technische Lösung, um die von den Wählerinnen und Wählern generierten öffentlichen Schlüssel zu zertifizieren und in einem öffentlichen Zertifikatsverzeichnis abzulegen. Dazu muss der gesicherte Zugriff auf den privaten Schlüssel der Zertifizierungsstelle gewährleistet sein, da dieser sonst missbraucht werden könnte. Bei der Realisierung könnten entsprechende prozedurale Standards von bestehenden Zertifizierungsstellen übernommen werden.
- Die Wahlbehörde muss die Möglichkeit haben, mittels geeigneten technischen Hilfsmitteln die Wahlvorbereitung durchzuführen. Es geht dabei vor allem darum, die Beschreibung der Vorlage und die zulässigen Wahloptionen (Kandidierende, Listen, etc.) bequem erfassen und in das vorgegebene Format bringen zu können. Das Resultat dieses Prozesses muss zudem digital unterschrieben und publiziert werden. Auch hier ist der gesicherte Zugriff auf den eigenen privaten Schlüssel erforderlich.
- Die Treuhänder benötigen technische Hilfsmittel für insgesamt vier verschiedene Aufgaben. Diese sind alle relativ rechenintensiv und müssen deshalb auf einem entsprechend leistungsfähigen Computer ausgeführt werden. Konkret müssen auf diesem Gerät Applikationen zum
  - Mischen der öffentlichen Schlüssel,
  - Verifizieren der Stimmen,
  - Mischen der Stimmen
  - und Entschlüsseln der Stimmen

  zur Verfügung stehen. Diese erfordern zum Teil den sicheren Zugriff auf den jeweiligen privaten Teilschlüssel sowie eine sichere Kommunikation zum öffentlichen Anschlagbrett.
- Zum Ermitteln des Endergebnisses benötigt die Wahlbehörde ein (ausserordentlich einfaches) Hilfsmittel zum Zusammenzählen der entschlüsselten Stimmen. Hierfür müssen keine besonderen Sicherheitsmechanismen vorgesehen werden.

- Sollte es erlaubt sein, elektronische Stimmen über die traditionellen Kanäle zu revozieren, dann müsste der Wahlbehörde ein Hilfsmittel zur Verfügung gestellt werden, um die mitgelieferten Beweise zu überprüfen und die digitale Signatur zu generieren.
- Für die universelle Verifizierung wird ein Hilfsmittel benötigt, um sämtliche auf dem öffentlichen Anschlagbrett dokumentierten Rechenschritte nachvollziehen zu können. Da dieser Vorgang sehr rechenintensiv ist, muss dieses Hilfsmittel als Applikation realisiert werden, die auf einem leistungsfähigen Computer ausführbar ist. Da eine solche Anwendung einen *Single-Point-of-Failure* darstellt, wäre es wünschenswert, wenn es verschiedene Implementierungen von unterschiedlichen Interessensgruppen gäbe.
- Um den Wählerinnen und Wählern die Möglichkeit zu geben, sich mit dem System und der Handhabung des Wahlgeräts vertraut zu machen, könnte eine *Test-Plattform* zur Verfügung gestellt werden, die eine unverbindliche Durchführung des gesamten Wahlprozesses ermöglicht. Eine solche Test-Plattform könnte ständig verfügbar sein, also unabhängig von konkreten Wahl- oder Abstimmungsvorlagen.

Weitere Komponenten dienen der Schlüsselgenerierung in der Setup-Phase. Dabei ist das Generieren des gemeinsamen öffentlichen Schlüssels der Treuhänder ein etwas schwierigeres Problem, weil die entsprechenden Teile des privaten Schlüssels individuell erstellt werden müssen. Für dieses Problem gibt es in der Literatur aber passende Algorithmen.

3.3. Verifizierung

Der eigentliche Wahlprozess aus der Sicht der Wählerinnen und Wähler geht aus der Beschreibung des kryptographischen Protokolls und der vorgestellten Systemkomponenten hervor. Auch der Verifizierungsprozess wurde schon verschiedentlich zur Sprache gebracht. Da die Verifizierbarkeit in diesem Konzept die zentrale Systemeigenschaft darstellt, werden nachfolgend die einzelnen Schritte des Verifizierungsprozesses zusammengefasst und weiter präzisiert. Insgesamt werden drei Stufen vorgeschlagen, die unabhängig voneinander durchgeführt werden können. Alle drei Stufen zusammen erfüllen die gestellten Anforderungen der individuellen und universellen Verifizierbarkeit (siehe Abschnitt 2.1).

Stufe 1: Verifizierung des Wahlgeräts (vor der Wahl). Das Konzept geht grundsätzlich von einem vertrauenswürdigen Wahlgerät aus. Dennoch kann es Personen geben, die dieses grundsätzliche Vertrauen kategorisch in Frage stellen und demzufolge die Korrektheit des Geräts überprüfen möchten. Hierfür könnten die Treuhänder den Dienst anbieten, verschlüsselte Teststimmen, welche mit dem Wahlgerät generiert wurden, zu entschlüsseln. Dabei müssten die Teststimmen für die Treuhänder eindeutig als solche erkennbar sein, gleichzeitig aber dürfte das Wahlgerät diese Unterscheidung nicht

vornehmen können. Diese Anforderung liesse sich dadurch realisieren, dass die Treuhänder zu Testzwecken verschiedene Wahlen aufsetzen, deren Identifikationsmerkmale keine Unterscheidung zu echten Wahlen erlauben, somit bei der Herstellung der Geräte nicht bekannt sein konnten. Es wäre naheliegend, solche Test-Wahlen im Rahmen der im vorherigen Abschnitt vorgeschlagenen Test-Plattform durchzuführen. Diese würde so nicht mehr nur zum Austesten des Wahlprozesses dienen, sondern auch zum Verifizieren der Wahlgeräte (wobei für das letztere die Stimmen vor dem Mischen von den Treuhändern entschlüsselt werden). Durch wiederholtes Durchführen solcher Tests können die Wählerinnen und Wähler eine beliebige grosse statistische Evidenz generieren, aus der sie auf das korrekte Funktionieren des verwendeten Wahlgeräts schliessen können. Daraus können sie bei einer echten Wahl die Anforderung *cast-as-intended* ableiten, welche den ersten Teilschritt der individuellen Verifizierbarkeit darstellt. Ähnliche Prozeduren sind in der Fachliteratur unter dem Namen *ballot casting assurance* bekannt [3, 7].

Stufe 2: Automatische Verifizierung (während der Wahl). Nach der Stimmabgabe über den bidirektionalen anonymen Kanal generiert das öffentliche Anschlagbrett eine digital signierte Bestätigung, die der Wählerin oder dem Wähler auf das Wahlgerät (bzw. auf die Wahlkarte) zurückgeschickt wird. Die Korrektheit der Signatur wird vom Wahlgerät überprüft und der Wählerin oder dem Wähler mitgeteilt (durch ein akustisches Signal oder mittels einer Anzeige im Display). Dies führt zur Gewissheit, dass die Stimme auf dem Anschlagbrett unverändert angekommen ist und in die Liste der abgegebenen Stimmen aufgenommen wurde. Die Signatur der Bestätigung impliziert zudem, dass die Stimme nicht nachträglich vom Anschlagbrett entfernt oder verändert werden kann. Würde dies geschehen, könnte die Manipulation mittels der dritten Verifizierungsstufe nachgewiesen werden. Die Betreiber des Anschlagbretts müssten also damit rechnen, dass Manipulationsversuche mit grosser Wahrscheinlichkeit entdeckt würden. Die zweite Verifizierungsstufe impliziert somit die Anforderung *recorded-as-cast*, welche den zweiten Teilschritt der individuellen Verifizierbarkeit darstellt.

Stufe 3: Optionale Verifizierung (nach der Wahl). Nach Abschluss der Wahl sind sämtliche relevanten Daten auf dem öffentlichen Anschlagbrett verfügbar und können von beliebigen Personen als Gesamtpaket heruntergeladen werden. Mittels einer lokal installierten Verifizierungsapplikation können diese Personen dann sämtliche Schritte der Ergebnisermittlung nachrechnen und alle Beweise überprüfen. Wie weiter oben bereits erwähnt, wäre es wünschenswert, wenn es verschiedene solche Applikationen gäbe, die von unabhängigen Entwicklern gemäss der Protokoll-Spezifikation realisiert wurden. Aus dem erfolgreichen Überprüfen sämtlicher Protokoll-Schritte kann die Korrektheit des Ergebnisses abgeleitet werden. Durch diese Prozedur ist also die universelle Verifizierbarkeit gegeben. Deren Durchführung ist für einzelne Wählerinnen oder Wähler optional, es reicht, wenn die Verifizierung durch einige unabhängige Personen erfolgt und die Korrektheit kommuniziert wird.

Wenn es die Verifizierungsapplikation zudem erlaubt, mit Hilfe der auf der Wahlkarte gespeicherten Bestätigung der Stimmabgabe die eigene Stimme in der Liste der abgegebenen Stimmen zu erkennen, dann ist auch die dritte für die individuelle Verifizierbarkeit

wesentliche Anforderung *counted-as-recorded* erfüllt. Da dies voraussetzt, dass die Wählerinnen und Wähler die Verifizierungsapplikation auf einem privaten Gerät installieren und zudem das gesamte Anschlagbrett herunterladen, könnte dieser letzte Schritt auch an vertrauenswürdige Instanzen delegiert werden. Alternativ könnte eine Webapplikation für die Verifizierung bereitgestellt werden, mit der man über einen bidirektionalen anonymen Kanal kommunizieren müsste.

Weitere Möglichkeiten der Verifizierung. Aus den drei oben beschriebenen Verifizierungsstufen wissen die Wählerinnen und Wähler indirekt, dass ihre Stimme korrekt ins Endergebnis eingeflossen ist. Sie können jedoch die abgegebene Stimme auf dem Anschlagbrett nicht direkt (d.h. in Klartext) sehen, weil sie die Stimme vor dem Mischen nicht entschlüsseln können, und weil sie die Stimme nach dem Mischen nicht als die Ihrige erkennen können. Für die Entschlüsselung müsste die bei der Verschlüsselung verwendete Randomisierung bekannt sein, gemäss Spezifikation darf diese das Wahlgerät jedoch nicht verlassen. Um trotzdem die Stimme nachträglich in Klartext zu sehen, müssten die Treuhänder hinzugezogen werden, entweder durch gemeinsames Entschlüsseln der Stimme vor dem Mischen oder durch Aufdecken der entsprechenden Verknüpfung im Mix-Netzwerk. Da dabei das Wahlgeheimnis aufgehoben und eine Quittung erzeugt wird, dürfte diese Möglichkeit nur in äussersten Ausnahmefällen und mit ausdrücklicher Genehmigung der betroffenen Person in Betracht gezogen werden (z.B. bei einem konkreten Verdacht eines Betrugsversuches mittels eines gefälschten Wahlgeräts).

4. Implikationen

Das in Kapitel 3 vorgestellte Konzept eines verifizierbaren Internet-Wahlsystems für die Schweiz bringt im Vergleich zu den bestehenden Schweizer Systemen viele Neuerungen und Verbesserungen. Auch im internationalen Vergleich weist das konzipierte System Eigenschaften auf, die in ihrer Gesamtheit bisher bei keinem der in der Praxis eingesetzten Systeme anzutreffen sind. In diesem Kapitel werden diese Eigenschaften und Neuerungen zusammengefasst und die erreichten Verbesserungen vorgestellt. Das Hauptaugenmerk liegt dabei zunächst bei der Sicherheit. Im Anschluss daran werden die Auswirkungen einer möglichen Einführung eines solchen Systems auf die bestehenden Gegebenheiten dargelegt. Dabei kommen die nötigen Anpassungen beim Wahl- und Abstimmungsprozess ebenso zur Sprache, wie auch die Auswirkungen auf das Beschwerderecht, auf bestehende Schnittstellen (z.B. zu den existierenden Wählerregistern) und auf die Benutzerfreundlichkeit. Die Auswirkungen des Konzepts auf mögliche Zulassungsprozeduren bilden den Schluss des Kapitels.

4.1. Sicherheit

Die folgende Diskussion der Sicherheitseigenschaften orientiert sich an den Anforderungen, wie sie in Abschnitt 2.1 eingeführt wurden. Anschliessend werden die Unterschiede zu den bestehenden Schweizer Systemen und die im Vergleich dazu eingeführten Neuerungen und erzielten Verbesserungen erläutert. Dieser Abschnitt wird durch eine kurze Diskussion von einigen offenen Problemen abgerundet.

4.1.1. Anforderungen

Die in Abschnitt 2.1 eingeführten Sicherheitsanforderungen beziehen sich auf ein ideales System, welches als solches bis heute nicht existiert und auch in Zukunft in der Praxis kaum je realisiert werden kann. Beim vorgestellten Konzept geht also darum, das ideale System so gut wie möglich anzunähern. Die Annahmen, auf denen das Sicherheitskonzept aufgebaut ist, sollten demzufolge so klein und so realistisch wie möglich gehalten werden. Im Idealfall können sämtliche Sicherheitsaspekte auf die üblichen mathematischen und komplexitätstheoretischen Annahmen zurückgeführt werden, auf denen die moderne Kryptographie beruht. Auf diese Weise kann das Gefährdungspotential durch den „Faktor Mensch“ auf ein Minimum reduziert werden. Dieses ist bei auf hauptsächlich organisatorischen Massnahmen abgestützten Sicherheitskonzepten oft sehr ausgeprägt.

Dieser Abschnitt soll aufzeigen, inwiefern dieses Ziel der grösstmöglichen Sicherheit unter kleinstmöglichen Annahmen im vorgestellten Konzept erreicht wird. Die grösste Ausnahme von diesem Leitsatz stellt die Annahme der Existenz des in Abschnitt 3.2 vorgestellten vertrauenswürdigen Wahlgeräts und der dazugehörigen Wahlkarte dar. Auch wenn diese Annahme in ihrer Absolutheit nur schwer zu erfüllen ist, scheint es durch eine pragmatische Herangehensweise möglich zu sein, solche Geräte und Karten mit den gewünschten Eigenschaften herstellen und an die Wählerschaft verteilen zu können. Natürlich schliesst dies die Möglichkeit von nachträglich durchgeführten Manipulationen oder von gefälschten Geräten oder Karten nicht aus, die Auswirkungen von solchen Angriffen wären jedoch nicht skalierbar.

Korrektheit des Ergebnisses. Manipulierte Wahlergebnisse werden durch verschiedene Massnahmen abgewehrt. Diese sind eng mit der Offenlegung der Daten auf dem öffentlichen Anschlagbrett und der daraus resultierenden Möglichkeit der individuellen und universellen Verifizierung verknüpft. Das auf dem Anschlagbrett publizierte Wählerverzeichnis und das daran angeknüpfte überprüfbare Mischen der öffentlichen Schlüssel garantiert zum Beispiel, dass jede abgegebene Stimme implizit genau einer wahlberechtigten Person zugeordnet werden kann (jedoch ohne die konkrete Zuordnung explizit aufdecken zu müssen). Dies gilt allerdings nur unter der Annahme, dass die entsprechende Wahlkarte ausschliesslich von dieser Person benutzt wird und dass somit die der elektronischen Stimme beigelegte digitale Signatur authentisch ist. Da der anonymisierte öffentliche Schlüssel in der elektronischen Urne als Identifikator dient, kann eine mehrfach durchgeführte Stimmabgabe eindeutig erkannt und gemäss den im Wahlverfahren festgelegten Richtlinien behandelt werden. Die Signatur schützt zudem die Stimme vor nachträglichen Veränderungen. Da der Erhalt einer abgegebenen Stimme vom öffentlichen Anschlagbrett durch eine Signatur bestätigt wird, erhalten die Wählerinnen und Wähler eine verbindliche Garantie, dass die Stimme bei der Ergebnisermittlung korrekt mitberücksichtigt wird. Dies kann durch eine Inspektion des öffentlichen Anschlagbretts nach Ablauf der Wahl verifiziert werden. Auch eine Manipulation bei der Entschlüsselung oder bei der Auszählung kann wegen der Veröffentlichung sämtlicher Daten leicht erkannt und korrigiert werden.

Fazit: Unter den folgenden Annahmen sind sämtliche Anforderungen erfüllt, die zusammen die Korrektheit des Ergebnisses implizieren:

- Sämtliche Wahlkarten wurden bei der Registrierung korrekt den jeweiligen Besitzerinnen und Besitzern zugeordnet.
- Die Wahlkarten werden nur von den jeweiligen Besitzerinnen und Besitzern für die Stimmabgabe verwendet.
- Die Wahlkarte und das Wahlgerät führen die vorgesehenen Funktionen korrekt durch und besitzen die dafür notwendigen Eigenschaften (siehe Abschnitt 3.2.1 und Abschnitt 3.2.2). Es werden ausschliesslich die offiziell herausgegebenen Wahlgeräte für die Stimmabgabe verwendet.

- Die elektronische Urne auf dem öffentlichen Anschlagbrett besitzt die *append-only* Eigenschaft (siehe Abschnitt 3.2.4).
- Das auf dem öffentlichen Anschlagbrett publizierte Wählerverzeichnis ist vollständig und korrekt und kann nicht verändert werden.
- Mindestens eine vertrauenswürdige Person muss die Signaturen und die Zero-Knowledge Beweise auf ihre Korrektheit überprüfen und einen entsprechenden Bericht publizieren.

Im Weiteren muss das für die Signaturen verwendete Verfahren die üblichen kryptographischen Eigenschaften eines fälschungssicheren digitalen Signaturverfahrens besitzen. Zu beachten ist zudem, dass keine Annahmen bezüglich dem Vorhandensein einer sicheren Plattform getroffen werden müssen.

Geheimnis der Wahl. Damit die einzelnen Aspekte des Wahlgeheimnisses gewährt sind, sieht das Konzept verschiedene Massnahmen vor. Zentral dabei ist die Anonymisierung der öffentlichen Schlüssel, mit denen die abgegebenen Stimmen signiert sind. Zusammen mit dem anonymen Kanal für die eigentliche Stimmabgabe verhindert dieser Anonymisierungsprozess, dass die abgegebenen Stimmen mit den entsprechenden Wählerinnen oder Wählern in Verbindung gebracht werden können. Das Wahlgeheimnis hängt also stark von der Sicherheit dieser zentralen Systemkomponente ab, die durch die Auswahl der damit beauftragten Treuhänder beeinflusst werden kann. Um herauszufinden, ob und wie jemand gewählt hat, müssten sämtliche Treuhänder zusammenspannen. Es genügt also, wenn mindestens einer dieser Treuhänder vertrauenswürdig ist. Sollte der anonyme Kanal nicht die vorgesehenen Eigenschaften aufweisen, verhindert das zusätzliche Mischen der Stimmen, dass diese den entsprechenden Wählerinnen oder Wählern zugeordnet werden können.

Das Protokoll des vorgestellten Konzepts erlaubt es den Wählerinnen und Wählern, die abgegebene Stimme auf dem öffentlichen Anschlagbrett zu identifizieren. Somit ist es möglich, einer dritten Person gegenüber zu beweisen, dass man eine bzw. keine Stimme abgegeben hat. Um auch zu beweisen, wie man gewählt hat, müsste die verschlüsselte Stimme entweder entschlüsselt oder rekonstruiert werden können. Letzteres ist mit Hilfe der bei der Verschlüsselung verwendeten Randomisierung leicht möglich, die in diesem Fall als Quittung dient. Wenn jedoch gewährleistet ist, dass diese das Wahlgerät nicht verlässt, dann ist ein solcher Beweis nicht mehr möglich. Damit während oder nach der Wahl keine Teilresultate ermittelt werden können, ist der für die Entschlüsselung benötigte private Schlüssel mittels eines Schwellwert-Verfahrens unter verschiedenen Treuhändern aufgeteilt. Eine gerechte Wahl ist also gewährleistet, solange nicht eine Mehrheit der involvierten Treuhänder unerlaubterweise kollaboriert.

Fazit: Unter den folgenden Annahmen sind fast alle Anforderungen erfüllt, die zusammen das Geheimnis der Wahl garantieren. Ein kleines offenes Problem ist die Möglichkeit, mit Hilfe der Wahlkarte und des Wahlgeräts einer dritten Person gegenüber zu beweisen, eine bzw. keine Stimme abgegeben zu haben. So könnten also wahlberechtigte

Personen durch Nötigung oder Bestechung dazu gebracht werden, an der Wahl teilzunehmen bzw. der Wahl fernzubleiben. Aus Sicht der Autoren ist dieses Problem und die damit verbundene Einschränkung des Wahlgeheimnisses und der Freiheit der Wahl (siehe nächster Abschnitt) jedoch von untergeordneter Bedeutung, da entsprechende Attacken nur beschränkt skalierbar sind. Als Gegenmittel könnte man zudem leere oder ungültige Stimmen zulassen, um die Teilnahme an der Wahl vortäuschen zu können. Die erwähnten Annahmen sind die folgenden:

- Mindestens einer der für das Mischen der öffentlichen Schlüssel zuständigen Treuhänder ist vertrauenswürdig.
- Mindestens einer der für das Mischen der Stimmen zuständigen Treuhänder ist vertrauenswürdig.
- Die bei der Verschlüsselung verwendete Randomisierung kann nicht aus dem Wahlgerät ausgelesen werden (siehe Abschnitt 3.2.2).
- Der anonyme Kanal besitzt die gewünschten Eigenschaften (siehe Abschnitt 3.2.3).
- Die Stimmabgabe erfolgt ausschliesslich über den anonymen Kanal.
- In der Gruppe der mit der Entschlüsselung beauftragten Treuhänder gibt es keine genügend grosse Koalition (grösser als oder gleich dem Schwellwert), die während oder nach der Wahl gewillt sind, einzelne Stimmen oder Teilmengen von Stimmen zu entschlüsseln.

Zudem muss das verwendete asymmetrische Verschlüsselungsverfahren die üblichen geforderten kryptographischen Eigenschaften besitzen. Wiederum müssen keine Annahmen bezüglich dem Vorhandensein einer sicheren Plattform getroffen werden.

Freiheit der Wahl. Die Freiheit der Wahl im vollen Umfang und unter allen möglichen Umständen zu gewährleisten, ist eine der schwierigsten Aufgaben eines elektronischen Wahlsystems. Wenn das Wahlgerät wie im Abschnitt zuvor besprochen die Randomisierung der Verschlüsselung nicht preisgibt, dann bietet die daraus resultierende Quittungsfreiheit bereits einen relativ grossen Schutz vor dem Stimmenkauf oder anderen Beeinflussungen durch Dritte. Natürlich kann damit eine erzwungene Stimmabgabe durch unmittelbare physische Präsenz nicht verhindert werden, aber immerhin ist das nachträgliche oder automatisierte Einfordern eines Beweises damit verhindert. Beeinflussungen durch direkte physische Präsenz, zum Beispiel in Familienkreisen, sind zwar leicht möglich (ähnlich wie bei der Briefwahl), lassen sich aber nicht beliebig skalieren. Ein offenes Problem ist die im Abschnitt zuvor beschriebene Möglichkeit, mit Hilfe der Wahlkarte und dem Wahlgerät gegenüber Dritten einen Beweis für die erfolgte bzw. die nicht erfolgte Stimmabgabe zu erbringen.

Als zusätzliches Gegenmittel gegen Beeinflussungen durch Dritte könnte im Sinne eines *hybriden Systems* [40] die auf Seite 38 beschriebene Revozierungsprozedur implementiert werden. Damit könnten Stimmen, die durch Dritte beeinflusst wurden, nachträglich per Brief- oder Urnenwahl revoziert und durch eine neue Stimme ersetzt werden. Einen ähnlichen, etwas abgeschwächten Effekt könnte man erreichen, indem bereits abgegebene

elektronische Stimmen durch neue elektronische Stimmen überschrieben werden könnten. Diese Optionen existieren grundsätzlich, sind aber im gegebenen Kontext zurzeit nicht erwünscht (siehe Fussnote auf Seite 12).

Um zu verhindern, dass jemand sein Wahlkarte und damit seine Wahlrecht an eine dritte Person abgibt, muss die Karte wie in Abschnitt 3.2.1 gefordert mit biometrischen Identifikationsmerkmalen der Besitzerin oder des Besitzers ausgestattet sein. Das Verwenden der Karte verlangt also die physische Präsenz der Besitzerin oder des Besitzers, wodurch das Abtreten der Karte an Dritte die Freiheit der Wahl nicht beeinträchtigen kann. Die gleichen Bemerkungen treffen für den Fall eines Kartendiebstahls zu. Durch Beantragen einer neuen Wahlkarte kann in beiden Fällen der Zugang zum elektronischen Wahlsystem wieder hergestellt werden.

Fazit: Unter den folgenden Annahmen sind einige der Anforderungen erfüllt, die für die Freiheit der Wahl wesentlich sind:

- Das Geheimnis der Wahl ist durch die im vorherigen Abschnitt beschrieben Annahmen gegeben. Insbesondere darf es nicht möglich sein, die bei der Verschlüsselung verwendete Randomisierung aus dem Wahlgerät auszulesen.
- Die Wahlkarten können ausschliesslich von ihren Besitzerinnen oder Besitzern verwendet werden, zum Beispiel mit Hilfe von biometrischen Identifikationsmerkmalen und entsprechenden zuverlässigen Authentifizierungsmechanismen.
- Bei der Option des Überschreibens der Stimme mittels einer nachträglichen Brief- oder Urnenwahl müssen die involvierten Personen der Wahlbehörde vertrauenswürdig sein.

Das wichtigste offene Problem ist die Möglichkeit der Wählerinnen und Wähler, gegenüber einer dritten Person die Teilnahme an der Wahl oder die Stimmenthaltung zu beweisen. Diese und andere kleinere Einschränkungen sind jedoch nicht skalierbar.

Öffentlichkeit der Wahl. Indem sämtliche bei der Wahl und bei der Auszählung anfallenden Daten auf dem öffentlichen Anschlagbrett publiziert werden, liefert das vorgestellte Konzept die nötige Grundlage, um den Grundsatz der Öffentlichkeit der Wahl angemessen umzusetzen. Mittels der in Abschnitt 3.3 vorgestellten Verifikationsprozeduren haben die einzelnen Wählerinnen und Wähler die Möglichkeit, jeden einzelnen Schritt des Wahlprozesses selber nachzuvollziehen und somit die Korrektheit des Ergebnisses zu überprüfen. Auch der Einbezug der eigenen Stimme lässt sich durch Inspektion des öffentlichen Anschlagbretts verifizieren.

Fazit: Das vorgestellte Konzept bietet die beiden geforderten Eigenschaften der individuellen und universellen Verifizierung.

Andere Anforderungen. Im letzten Unterabschnitt von Abschnitt 2.1 sind fünf weitere wichtige Anforderungen aufgelistet. Auch diesen Punkten trägt das vorgestellte Konzept Rechnung. Die Robustheit und somit die ständige Verfügbarkeit des Systems ist durch den konsequenten Einsatz von Schwellwert-Verfahren gegeben, insbesondere auch bei der Realisierung des öffentlichen Anschlagbretts. Für das Problem der sicheren Plattform bietet das vorgeschlagene Wahlgerät eine umfassende Lösung, sofern dieses tatsächlich vertrauenswürdig ist. Die benötigte Rechenleistung für die einzelnen Schritte des Wahlprozesses können bei allen benötigten Systemkomponenten mittels handelsüblicher Rechenprozessoren zur Verfügung gestellt werden. Um das System vor Diskreditierung durch ungültige Stimmen zu schützen, können die in [23] vorgestellten Verfahren eingesetzt werden. Damit können Stimmen mit ungültigem Inhalt herausgefiltert werden, ohne sie zu entschlüsseln. Eine hohe Benutzerfreundlichkeit ist durch die Möglichkeit gegeben, die Stimmabgabe auf den persönlichen Endgeräten der Wählerinnen und Wähler vorzubereiten (siehe Abschnitt 4.5).

4.1.2. Vergleich zu den bestehenden Systemen

In diesem Abschnitt werden die Sicherheitseigenschaften des in Kapitel 3 vorgestellten Konzepts mit der Sicherheit eines der existierenden Schweizer Systeme verglichen. Als Referenz dient das Genfer System, weil darüber am meisten öffentlich zugängliche Dokumentation vorhanden ist. Da aber die anderen Systeme auf ähnlichen Konzepten beruhen, lassen sich viele der nachfolgenden Aussagen übertragen.

Korrektheit des Ergebnisses. Die Korrektheit des Ergebnisses des Genfer Systems hängt in erster Linie von der Korrektheit der Stimmen in der elektronischen Urne des Systems ab, welche nicht öffentlich einsehbar ist. Wegen fehlender individueller Verifizierbarkeit im Genfer System (siehe Abschnitt 2.1) muss die wahlberechtigte Person Vertrauen in eine Kette von Systemkomponenten und deren sicheren Betrieb haben. Das erste Glied in dieser Kette ist der persönliche Computer der wahlberechtigten Person. Hier muss die wahlberechtigte Person sicher sein, dass die Stimme unverfälscht erfasst und übermittelt wird. Das Genfer System dämmt dieses Problem ein, indem der auf Integrität geprüfte Wahlzettel der stimmberechtigten Person zusammen mit einem individuellen Rückantwortcode zurückgeschickt wird. Dadurch ist aber noch immer nicht erwiesen, dass die Stimme die Wahlserver wirklich unverfälscht erreicht hat (eine *Man-in-the-Browser*-Attacke ist nicht leicht zu erkennen). Selbstverständlich kann auch der Betreiber des elektronischen Wahlsystems rein aufgrund des empfangenen Chiffrats nicht beurteilen, ob die verschlüsselte Stimme dem Willen der wählenden Person entspricht.

Als zweite Komponente des Genfer Systems muss der Abstimmungsserver die Stimme der wahlberechtigten Person korrekt verschlüsseln und sie in die elektronische Urne ablegen. Würde dies der Abstimmungsserver aus irgendeinem Grund nicht richtig machen, zum Beispiel weil sich beim Abstimmungsserver eine Schadsoftware eingenistet hat oder weil die Software auf dem Abstimmungsserver nicht richtig funktioniert, so wäre die Korrektheit des Ergebnisses nicht gegeben. Die Korrektheit des Ergebnisses hängt aber auch

von der Legitimität der Stimmen ab, die sich in der elektronischen Urne befinden. Weil die Daten in der elektronischen Urne nicht öffentlich einsehbar sind, muss beim Genfer System durch prozedurale Massnahmen garantiert werden, dass keine bestehenden Daten entfernt oder neue Datensätze eingefügt werden.[1]

Die Korrektheit des Ergebnisses hängt beim Genfer System zudem vom korrekten Zählen der Stimmen und dem korrekten Publizieren des Ergebnisses ab. Die Korrektheit diese beiden Schritte kann nur durch prozedurale Massnahmen (u.a. durch das *Vier-Augen*-Prinzip) garantiert werden.

Fazit: Die Korrektheit der Ergebnisses hängt beim Genfer System von einer Reihe von Annahmen ab, die zum Teil auf der Einhaltung von prozeduralen Massnahmen beruhen und somit aus der Sicht der Wählerschaft schwer zu überprüfen sind. Zudem ist das Problem der sichereren Plattform ein ungelöstes Problem. Das in diesem Bericht vorgestellte Wahlsystem hingegen kann dank der Offenlegung der Daten auf dem öffentlichen Anschlagbrett und dank strikter, durch die Öffentlichkeit nachprüfbare Integritätsregeln die Korrektheit des Ergebnisses garantieren. Diese Eigenschaft und die vorgestellte Lösung für das Problem der sicheren Plattform sind zwei der grossen Verbesserungen im Vergleich zum Genfer System oder den anderen Schweizer Systemen.

Geheimnis der Wahl. Das Geheimnis der Wahl hängt in erster Linie von der Unverknüpfbarkeit des Wahlzettels mit der stimmberechtigten Person ab. Wie in Abschnitt 2.3.1 besprochen wurde, wird diese im Genfer System durch das strikte Einhalten der Prozesse garantiert. Eine Attacke zum Brechen des Geheimnisses der Wahl könnte aber im Abstimmungsserver erfolgen, denn dort ist sowohl die 16-stellige Nummer als auch die Stimme der stimmberechtigten Person während des Wahlaktes bekannt. Um den Namen der stimmberechtigten Person in Erfahrung zu bringen, müsste der Angreifer allerdings noch mit einer anderen Stelle kooperieren, zum Beispiel mit der für das Drucken der Stimmrechtsausweise beauftragten Druckerei.[2] Unabhängig davon ist es im Genfer System für Personen mit entsprechenden Zugriffsrechten möglich zu sehen (während oder nach der Wahl), wer an der Wahl teilgenommen hat. Bei einer strikten Auslegung des Wahlgeheimnisses ist dies nicht zulässig, weil mit dieser Information der Ausgang der Wahl beeinflusst werden könnte (siehe Abschnitt 2.1).

Ein anderer Angriff gegen das Wahlgeheimnis im Genfer System besteht darin, mittels Schadprogrammen auf den persönlichen Endgeräten der stimmberechtigten Personen deren Benutzerinteraktionen im Webbrowser und somit die eigentliche Wahlhandlung unbemerkt auszuspionieren. Die einzigen Möglichkeiten solche Angriffe durch Externe auf die Plattformen der Benutzer auszuschliessen liegen entweder in der Einführung *Code Voting* oder in der Verwendung eines geeigneten Wahlgeräts.

[1] Das Einfügen von unberechtigten elektronischen Stimmzetteln in die elektronische Urne wird in der Fachliteratur als *Ballot Stuffing* bezeichnet.

[2] Die Druckerei erhält eine CD mit Namen, Adressen, 16-stelligen Nummern und weiteren Informationen der stimmberechtigten Personen. Wenn es dem Angreifer gelänge, sich eine Kopie dieser CD zu beschaffen, dann wäre die nachträgliche Kooperation mit einer dritten Stelle hinfällig.

Fazit: Das Geheimnis der Wahl hängt beim Genfer System vom strikten Einhalten der Prozesse und von der korrekten Arbeitsweise des Abstimmungsservers ab. Zudem müssen die Daten, welche in einer Prozessstufe erzeugt und in der nachfolgenden Prozessstufe verwendet werden, vor dem Zugriff durch Drittpersonen geschützt werden. Ein weiteres Problem ist das Ausspionieren des Stimmverhaltens mittels Schadprogrammen auf den Endgeräten der Wählerinnen und Wähler. Im Gegensatz dazu garantiert das in diesem Bericht vorgestellte Wahlsystem das Wahlgeheimnis dank der Verwendung von anonymisierten öffentlichen Schlüsseln, welche aus dem Wählerverzeichnis durch einen verifizierbaren Misch-Mechanismus abgeleitet werden. Die anonymisierten Schlüssel können ohne Kenntnis des privaten Schlüssels der stimmberechtigten Person nur durch sämtliche beim Mischen beteiligten Treuhänder auf diese zurückgeführt werden. Der Schutz des Wahlgeheimnisses reduziert sich also auf den Schutz der privaten Schlüssel der Wählerschaft, sowie auf die Garantie, dass die beim Mischen beteiligten Treuhänder nicht alle in bösartiger Absicht kooperieren. Der Mechanismus mit der optischen Schnittstelle zwischen Wahlplattform und Wahlgerät verhindert zudem, dass Schadprogramme auf den Endgeräten der Wählerinnen und Wähler das Wahlgeheimnis brechen können.

Freiheit der Wahl. Da das Genfer System nicht auf die Möglichkeit der individuellen Verifizierung ausgerichtet ist, gibt es auch keine Quittung, die einer dritten Person als Beweis für die abgegebene Stimme vorgelegt werden könnte. Entsprechend ist die Gefahr des quittungsbasierten (und somit skalierbaren) Kaufens oder Erpressens von Stimmen nicht gegeben. Auf der anderen Seite ist es im Genfer System relativ einfach möglich, die persönlichen Zugangsdaten zum System an eine dritte Person abzutreten. Da diese Zugangsdaten jeweils nur für einen Wahl- oder Abstimmungstermin gültig sind, sind die Konsequenzen einer solchen Handlung nicht besonders gross. Eine Attacke könnte somit darin bestehen, vor der Wahl oder Abstimmung möglichst viele Zugangsdaten zusammenzutragen und den bereitwilligen Personen einen Belohnung in Aussicht zu stellen, zum Beispiel automatisiert über eine entsprechende Webseite auf einem Server im Ausland.

Fazit: Das Genfer System ist quittungsfrei und somit resistent gegenüber einer gross angelegten, quittungsbasierten Bestechung oder Nötigung der Wählerschaft. Das in diesem Bericht vorgestellte Wahlsystem ist jedoch nur dann quittungsfrei, wenn die Randomisierung das vertrauenswürdige Wahlgerät nicht verlassen kann (siehe Abschnitt 3.1.1). Da dies eine zusätzliche Annahme darstellt, ist das Genfer System in diesem Punkt gegenüber dem in diesem Bericht vorgestellten Konzept leicht im Vorteil. Auf der anderen Seite ist das Zusammentragen vieler Zugangsdaten bereitwilliger Personen beim Genfer System grundsätzlich einfach möglich, während dies beim vorgestellten Konzept relativ aufwendig ist. Gegenüber Beeinflussungen bei direkter physischer Präsenz (*Family Voting*, etc.) sind beide Systeme nicht resistent, weil das Überschreiben einer bereits abgegebenen Stimme nicht vorgesehen ist.

Öffentlichkeit der Wahl. Es liegt in der Natur des Genfer Systems, dass nur Teilmengen der Daten je nach Verarbeitungsstufe für bestimmte Gruppen von Personen einsehbar sein dürfen. Das heisst auch, dass hohe Sicherheitsstandards und -prozeduren

für jede Stufe zur Anwendung gelangen müssen. Die Gesamtheit der Daten zu einem beliebigen Zeitpunkt darf unter keinen Umständen weder von Personen des Betriebs noch von der Öffentlichkeit einsehbar sein. Weil die Daten wie teilweise auch die Prozesse rund um die Daten der Öffentlichkeit nicht zugänglich gemacht werden, können sich die Wählerinnen und Wähler nicht selber von der Korrektheit des Wahlvorgangs überzeugen.

Fazit: Wichtige Prozesse sind beim Genfer System weitgehend offengelegt. Allerdings liefert das System keinen mathematischen Beweis für die korrekte Verarbeitung der Daten. Bei dem in diesem Bericht vorgestellten Wahlsystem hingegen sind alle Daten öffentlich, ausser die privaten Schlüssel der Wählerinnen und Wähler sowie die der Treuhänder und der Wahlbehörde. Die Wählerinnen und Wähler können durch das Vorhandensein der Daten und durch die Offenlegung aller Prozeduren und Funktionen, welche auf die Daten angewendet werden, den Weg der Stimme von der Abgabe über die Auszählung bis zur Ermittlung des Ergebnisses vollständig nachvollziehen (sofern sie über das nötige technische Sachverständnis und geeignete Hilfsmittel verfügen).

4.1.3. Offene Probleme

Das in diesem Bericht vorgestellte Konzept eines Wahlsystems erhebt nicht den Anspruch, bezüglich allen möglichen Gesichtspunkten perfekt zu sein und alle Fragen umfassend zu beantworten. Im Folgenden werden einige der grössten offenen Probleme aufgeführt, sowie mögliche Massnahmen diskutiert.

Treuhänder. Die Wahrung des Wahlgeheimnisses beruht unter anderem auf der Annahme, dass nicht alle beim Mischen der öffentlichen Schlüssel und nicht eine Mehrheit der beim Entschlüsseln der Stimmen beteiligten Treuhänder unerlaubterweise kooperieren (siehe Abschnitt 4.1.1). Um dieses Risiko zu minimieren, muss die Auswahl der Treuhänder mit grosser Sorgfalt erfolgen. Es sollte sich um möglichst vertrauenswürdige, zuverlässige und unabhängige Personen oder Institutionen handeln. Wer konkret diese Funktion einnehmen soll, ist jedoch ein völlig offenes Problem. In Frage kommen politische Parteien, Notare, öffentliche Behörden, Universitäten, anerkannte Experten, Firmen, Privatpersonen, in- oder ausländische Nichtregierungsorganisationen, internationale Wahlbeobachter, etc. Auch die Anzahl der Treuhänder sowie die Wahl des Schwellenwerts sind offene Fragen, die bei einer Umsetzung des Konzepts beantwortet werden müssten.

Ein anderes offenes Problem ist die Frage, wie die Treuhänder den jeweiligen Teil des privaten Schlüssels sicher aufbewahren können, um so ihre Aufgabe auf sichere Weise erfüllen zu können. Hierzu müssen den Treuhändern Systeme zur Verfügung gestellt werden, die einfach zu bedienen sind und eine fehlerhafte Bedienung ausschliessen. Entsprechende Prozeduren für die Bedienung dieser Systeme müssen definiert und den Treuhändern in geeigneter Form mitgeteilt werden.

Langzeitsicherheit. Das Veröffentlichen der bei der Wahl anfallenden (verschlüsselten) Daten ist eine der zentralen Grundideen des vorgestellten Konzepts. Dies bedeutet aber, dass jedermann jederzeit diese Daten kopieren kann, um sie zum Beispiel offline zu bearbeiten. Es ist deshalb damit zu rechnen, dass die Daten auch nach sehr langer Zeit noch verfügbar sind. Somit stellt sich die Frage, ob die heute verwendeten kryptographischen Methoden ausreichen, um die Sicherheit der Daten auch in ferner Zukunft noch gewährleisten zu können. Konkret besteht also ein gewisses Risiko, dass das Geheimnis der Wahl mit zukünftigen Methoden und Technologien gebrochen werden kann. Um dieses Risiko zu minimieren, muss bei der Wahl der kryptographischen Parameter dieser Gesichtspunkt berücksichtigt werden. So sollten zum Beispiel Schlüssellängen gewählt werden, welche die heute geltenden Empfehlungen deutlich übersteigen. Ganz eliminieren lässt sich das Risiko der Langzeitsicherheit jedoch nicht.

Denial-of-Service Attacken. Die Verfügbarkeit des Wahlsystems kann in der Wahlperiode oder danach durch absichtlich herbeigeführte Serverüberlastungen beeinträchtigt werden. Besonders exponiert für eine sogenannte *Denial-of-Service* (DoS) Attacke (oder die noch stärkere Variante einer *Distributed Denial-of-Service* Attacke) ist das öffentliche Anschlagbrett. Solche Attacken können dazu führen, dass die stimmberechtigten Personen wichtige Funktionen wie das Ablegen der Stimmen auf dem Anschlagbrett, das Verifizieren der Stimme oder das Verifizieren des Ergebnisses nicht mehr wahrnehmen können. Als erste Gegenmassnahme sollte das öffentliche Anschlagbrett von Grund auf als verteilte Applikation realisiert werden (siehe Abschnitt 3.2.4). Zudem sind die bekannten Gegenmassnahmen wie dynamische Sperrlisten oder das Limitieren des Datenvolumens pro IP-Adresse in Betracht zu ziehen. Ganz ausschliessen lässt sich die Möglichkeit einer erfolgreichen Attacke dieser Art aber nicht. Im Extremfall könnte eine DoS-Attacke zum Beispiel darauf ausgerichtet sein, während der Wahlperiode das ganze Internet (oder Teile davon), zum Beispiel durch gezieltes Überlasten eines bestimmten Providers, lahmzulegen.

4.2. Wahl- und Abstimmungsprozess

Dieser Abschnitt beschreibt die nötigen Vorkehrungen, die seitens der Behörden zu treffen sind, um eine elektronische Wahl oder Abstimmung gemäss dem vorgestellten Konzept durchzuführen. Die Vorkehrungen unterscheiden sich wegen der Andersartigkeit des gewählten Protokolls von den bestehenden Schweizer Systemen. Im Folgenden werden die Implikationen aus der in Abschnitt 3.1.2 beschriebenen Prozedur abgeleitet.

Setup. Ziel dieser Phase ist das Publizieren von zwei öffentlichen Schlüsseln sowie der ElGamal-Parameter. Einer der beiden öffentlichen Schlüssel wird von einer Gruppe von Treuhändern gemeinsam generiert. Hierzu ist ein Verfahren zu definieren, mit dem die Gruppe der Treuhänder bestimmt wird. Das Verfahren kann dem Bestellen einer Wahlkommission gleichen. Es ist aber auch möglich, für ein spezielles Ereignis eine andere

Gruppe von Treuhändern zu bestimmen. Für die kryptographischen Operationen gilt zu beachten, dass alle Schritte zwingend auf sicheren Geräten durchgeführt werden.

Registrierung. Am Ende dieser Phase besitzt die stimmberechtigte Person eine Wahlkarte. Der ihr zugeordnete öffentliche Schlüssel ist mittels Zertifikat in einem öffentlichen Verzeichnis publiziert. Für diesen im Grundsatz einmaligen Akt ist ein Verfahren zu definieren, welches verlangt, dass die entsprechende Person bei der Zertifizierungsstelle persönlich erscheint, sich ausweist und ihren öffentlichen Schlüssel vorlegt (oder wahrscheinlicher, ihn vor Ort auf geeignete Weise auf der Wahlkarte generiert).[3] Eine weitere, wichtige Folgerung ist, dass dieser Person ab diesem Zeitpunkt keine Stimmrechtsausweise und Wahlunterlagen zugeschickt werden müssen.

Wahlvorbereitung. Am Ende dieser Phase ist das Wählerverzeichnis, die Liste der anonymisierten öffentlichen Schlüssel, die Liste der Wahloptionen sowie ein weiterer ElGamal-Parameter publiziert. Die dazu notwendigen Verfahren sind pro Wahlereignis auszuführen. Das Verfahren für die Erstellung des Wählerverzeichnisses definiert, wie aus der Menge der registrierten Personen die Teilmenge der wahlberechtigten Personen bestimmt, signiert und auf dem Anschlagbrett publiziert wird. Ein zweites, daran anschliessendes Verfahren definiert, wie die Treuhänder die Liste der öffentlichen Schlüssel anonymisieren und den weiteren ElGamal-Parameter erstellen. Ein drittes, unabhängiges Verfahren definiert, wie die Wahlbehörde die Liste der Wahloptionen erstellt, signiert und auf dem öffentlichen Anschlagbrett publiziert.

Stimmabgabe. Im Normalfall wird die wahlberechtigte Person ihren elektronischen Wahlzettel gemäss dem in Abschnitt 3.1.2 beschriebenen Verfahren erstellen und an das öffentliche Anschlagbrett schicken. Es ist aber auch möglich, dass eine wahlberechtigte Person trotz elektronischer Wahlkarte ausnahmsweise postalisch oder an der Urne wählen möchte. Für diesen Fall ist ein Verfahren festzulegen, durch welches die wahlberechtigte Person beweisen kann, dass sie noch nicht elektronisch gewählt hat, um so die Stimme auf Papier (per Post oder im Wahllokal) abgeben zu können. Es geht also darum, die Möglichkeit von Mehrfachstimmen auszuschliessen. Der zu erbringende Beweis besteht darin, dass die Person ihren anonymisierten öffentlichen Schlüssel aufdeckt, was nur mit Hilfe der Wahlkarte und dem Wahlgerät möglich ist. Die Karte legt den Beweis im auslesbaren Teil des Speichers ab, so dass dieser in Form eines maschinenlesbaren Codes ausgedruckt und der Papierstimme beigelegt werden kann.

Wahlnachbereitung. Bei der Wahlnachbereitung werden die gültigen Stimmen, wie in Abschnitt 3.1.2 beschrieben, von den Treuhändern ermittelt und die ungültigen Stimmen herausgefiltert. Hierzu sind den Treuhändern entsprechende technische Hilfsmittel zur Verfügung zu stellen. Es muss zudem ein Verfahren zur Handhabung der Papierstimmen festgelegt werden, die von registrierten Personen abgegeben wurden. Nur diejenigen

[3] Für Auslandschweizerinnen und -schweizer sind dafür stellvertretende Behörden wie Botschaften oder Konsulate vorzusehen.

Papierstimmen werden zugelassen, deren Beweis korrekt ist und die zeigen, dass die entsprechende Person noch nicht elektronisch gewählt hat. Dazu wird der Beweis maschinell eingelesen und automatisch ausgewertet. Falls die Auswertung ergibt, dass der Beweis nicht korrekt ist oder dass bereits eine elektronische Stimme in der Urne vorliegt, so wird die Papierstimme für ungültig erklärt und nicht gezählt.

Auszählung. Bei der Auszählung werden die entschlüsselten Stimmen zusammengezählt und publiziert. Die dazu benötigten Verfahren lehnen sich an die bestehenden, papierbasierten Verfahren an.

Verifizierung. Im Abschnitt 3.3 wurden drei Stufen des Verifizierens beschrieben. Die dazu notwendigen Verfahren betreffen nur die Wählerinnen oder Wähler, sowie andere Personen, die an einer Verifizierung interessiert sind (z.B. internationale Wahlbeobachter). Aus der Sicht der Behörden sind keine weiteren Verfahren notwendig als die in Abschnitt 3.3 beschriebenen.

Revozieren. Obwohl noch keine gesetzliche Grundlage für dieses Verfahren existiert und somit im gegebenen Kontext nicht erwünscht ist, soll es hier aus der Sicht der Treuhänder beschrieben werden. Im Falle eines Revozierens erwarten die Wahlbehörden von der revozierenden Person den Beweis für ihren anonymisierten öffentlichen Schlüssel und eine Wiederverschlüsselung der abgelegten Stimme. Dieser Beweis und die wiederverschlüsselte Stimme können automatisch von der revozierenden Person mit Hilfe der persönlichen Wahlkarte und des Wahlgeräts erzeugt werden. Die Wahlkarte legt die Informationen im auslesbaren Teil des Speichers ab, so dass sie zuhause ausgedruckt oder im Wahllokal ausgelesen werden können. Anschliessend wird mit der Stimmabgabe gleich verfahren wie bei der Stimmabgabe auf Papier (an der Urne oder brieflich). Bei der Wahlnachbereitung gilt es aber zu beachten, dass im Falle des korrekten Revozierens die Wahbehörde die wiederverschlüsselte Stimme signieren und in eine separate elektronische Urne legen, denn bei der Auszählung müssen diese Stimmen vom Gesamtergebnis subtrahiert werden.

4.3. Beschwerderecht

Das beschriebene Konzept kann nicht bedingungslos ausschliessen, dass aus Sicht einer wahlberechtigten Person einmal etwas schiefgeht. In einem solchen Fall muss die Möglichkeit von Beschwerden in Betracht gezogen werden. Dabei kann zwischen verschiedenen Arten von Beschwerden unterschieden werden. Die folgende Liste ist nicht abschliessend.

Fehlender Eintrag im Wählerverzeichnis. Dies kann zwei Ursachen haben. Zum einen kann die betroffene Person für das entsprechende Wahlereignis gar nicht wahlberechtigt sein. Somit ist dies kein Fehler im eigentlichen Sinn. Zum anderen kann bei der Erstellung des Wählerverzeichnisses ein echter Fehler passiert sein.

Beschwerdegang: In beiden Fälle wird sich die betroffene Person bei der Wahlbehörde beschweren. Die Wahlbehörde prüft und stellt im ersten Fall fest, dass die betroffene Person eben nicht wahlberechtigt ist. Der zweite Fall ist komplizierter, denn das bestehende Wählerverzeichnis darf nicht mehr geändert werden. Eine mögliche Lösung besteht darin, der wahlberechtigten Person einen Stimmrechtsausweis auszuhändigen, so dass sie damit per Brief oder im Wahllokal abstimmen kann.[4] Für den nächsten Wahlgang muss eine neue Wahlkarte bestellt werden.

Fehlende Stimme in der Testwahl. Eine mündige und urteilsfähige Person kontrolliert das korrekte Funktionieren ihrer Wahlkarte (siehe Abschnitt 3.3, Stufe 2) und findet ihre Stimme nicht im Testbereich des Anschlagbretts.

Beschwerdegang: Die betroffene Person beschwert sich beim Betreiber des Anschlagbretts. Dazu muss sie ihre Wahlkarte und das verwendete Wahlgerät mitbringen. Die Wahlkarte, das Wahlgerät und das Anschlagbrett werden kontrolliert. Falls das Wahlgerät defekt ist, wird es eingezogen. Falls die Wahlkarte defekt ist, muss sich die betroffene Person neu registrieren, um eine neue Wahlkarte zu erhalten. Das Zertifikat des zur alten Karte passenden Schlüssels wird revoziert.

Fehlende Bestätigung bei Stimmabgabe. Eine wahlberechtigte Person schickt ihre Stimme zum öffentlichen Anschlagbrett, aber sie erhält keine signierte Bestätigung und die Stimme erscheint nicht auf dem öffentlichen Anschlagbrett, auch nicht nach mehreren Wiederholungen.

Beschwerdegang: Die wahlberechtigte Person beschwert sich bei der Wahlbehörde. Sie gibt ihren anonymisierten öffentlichen Schlüssel bekannt. Die Behörde prüft das öffentliche Anschlagbrett und bestätigt das Fehlen der Stimme. Die Karte wird eingezogen und das Zertifikat des passenden Schlüssels wird revoziert. Die wahlberechtigte Person erhält, wie oben schon beschrieben, einen Stimmrechtsausweis, so dass sie danach per Brief oder im Wahllokal abstimmen kann. Für den nächsten Wahlgang muss eine neue Wahlkarte bestellt werden.

Fehler beim Auszählen. Eine wahlberechtigte Person bestätigt, dass sich ihre Stimme auf dem öffentlichen Anschlagbrett befindet, diese wurde aber nicht richtig gezählt.

Beschwerdegang: Die wahlberechtigte Person beschwert sich bei der Wahlbehörde. Die Behörde überprüft die Beweise für das korrekte Mischen der erhaltenen Stimmen, die korrekte Entschlüsselung der gemischten Stimmen und deren Auszählung.

[4] Elektronische Lösungen wären auch denkbar, wurden aber von den Autoren bisher nicht weiterverfolgt.

Verlust der Wahlkarte vor Erstellung des Wählerverzeichnisses. Eine wahlberechtigte Person verliert ihre Wahlkarte.

Beschwerdegang: In diesem Fall ist keine Beschwerde möglich. Die betroffene Person beantragt eine neue Wahlkarte bei der Zertifizierungsstelle. Das Zertifikat des öffentlichen Schlüssels der verlorenen Karte wird revoziert.

Verlust der Wahlkarte nach Erstellung des Wählerverzeichnisses. Eine wahlberechtigte Person verliert ihre Wahlkarte.

Beschwerdegang: In diesem Fall ist keine Beschwerde möglich. Die wahlberechtigte Person ist vom aktuellen Wahlereignis ausgeschlossen. Dieser Fall kann mit dem Verlust des Stimmrechtsausweises bei der Papierwahl verglichen werden.

4.4. Schnittstellen

Das in diesem Bericht vorgestellte Wahlsystem hat zwingend Schnittstellen zu bestehenden Systemen. Im Folgenden wird kurz auf die offensichtlichen Schnittstellen und die sich aufdrängenden Folgerungen eingegangen.

Öffentliches Personenverzeichnis. Damit eine Person mittels des vorgestellten Wahlsystems wählen oder abstimmen kann, muss sie im Besitz einer Wahlkarte sein. Der Erhalt der Wahlkarte bedingt zwingend einen Behördengang. Zusätzlich werden nebst der Personenidentifikation Daten aus einem Quellregister, zum Beispiel aus dem Personenregister, benötigt. Zusammen mit dem Erstellen der Wahlkarte und des entsprechenden Schlüsselpaars, muss ein Eintrag in ein neu zu erstellendes, öffentliches Personenverzeichnis (siehe Abschnitt 3.1.2, Phase 2: Registrierung) erfolgen. Für diesen Eintrag kann eine Teilmenge des Meldungsformats des Standards eCH-0045 verwendet werden.[5] Dieses Personenregister wäre somit Bestandteil einer landesweiten *Public-Key Infrastruktur*. Die Quellverzeichnisse sind je nach Kanton zentral (z.B. Kanton Genf) oder dezentral (z.B. Kanton Zürich) organisiert. Diese unterschiedlichen Organisationsformen sind im Standard eCH-0045 berücksichtigt.

Wählerverzeichnis. Die Einträge im Wählerverzeichnis des vorgeschlagenen Wahlsystems können wiederum nach dem Meldungsformats des Standards eCH-0045 organisiert werden. Dieser definiert Operationen, die auf ein *virtuelle Stimm- und Wahlregister* angewendet werden können. Die Operationen für das Erstellen des Verzeichnisses oder das Hinzufügen von wahlberechtigten Personen können für das Wählerverzeichnis übernommen werden. Die zwei weiteren Operationen „*changing voting rights*“ und „*remove voter*“ dürfen nicht verwendet werden, da das Wählerverzeichnis wird auf dem öffentlichen Anschlagbrett publiziert (ein öffentliches Anschlagbrett erlaubt nur, Einträge anzufügen,

[5] eCH, www.ech.ch, Standard eCH-0045.

nicht aber zu modifizieren oder zu löschen). Aus den gleichen Gründen, die im Standard erwähnt werden, müsste man in der Phase der Vorbereitung mit einem temporären, noch nicht öffentlichen Wählerverzeichnis arbeiten, welches alle im Standard vorgesehenen Operationen zulässt. Erst am Stichtag würde das Wählerverzeichnis eingefroren und auf dem öffentlichen Anschlagbrett publiziert.

Vermittlung des Ergebnisses Nach dem Auszählen wird das Ergebnis auf dem öffentlichen Anschlagbrett publiziert. Für das Bereitstellen der Daten, zum Beispiel für die Medien, ist ein Meldungsformat zu definieren. Dabei kann man sich an den Standard eCH-0045 oder eventuell auch an den Standard *EML*[6] anlehnen.

4.5. Benutzerfreundlichkeit

Wahlberechtigte Personen interagieren in verschiedenen Phasen mit dem vorgestellten Wahlsystem. Im Vordergrund steht die Interaktion in der Phase der Stimmabgabe (siehe Abschnitt 3.1.2, Phase 2, Stimmabgabe). Aber auch in anderen Phasen kann die wahlberechtigte Person bzw. auch Nichtbeteiligte mit dem Wahlsystem interagieren. Im Folgenden wird die Benutzerfreundlichkeit der jeweiligen Situationen untersucht und bewertet. Am Schluss dieses Abschnittes wird auf die Stimmabgabe von sehbehinderten Personen eingegangen.

Stimmabgabe. Die Phase der Stimmabgabe unterteilt sich in die Phase der Vorbereitung auf dem privaten Endgerät und in die Phase des Überprüfens, Verschlüsselns und Versendens der Stimme (siehe auch Abschnitt 3.2.2).

Die Vorbereitung der Stimme erfolgt auf dem privaten Endgerät (PCs, Notebooks, Smartphones, Tablet-Computer, etc.) in Verbindung mit einer Plattform (Web, Java, Apps, etc.). Die Benutzerführung für die eigentliche Wahlhandlung (Auswählen oder Erstellen einer Liste von Kandidierenden) ist auf den ersten Blick vergleichbar mit den heutigen Wahlsystemen in der Schweiz. Genauer betrachtet ist dieser Vorgang noch etwas einfacher, denn die Eingabe einer Nutzerkennung (z.B. die 16-stellige Nummer beim Genfer System) sowie weiterer Angaben im Falle der Bestätigung der Wahl entfallen. Die zu erwartende Benutzerfreundlichkeit ist also sehr gut.

Ist die eigentliche Wahlhandlung vollzogen, so beginnt die Phase des Überprüfens und Verschlüsselns der Stimme. Das Fotografieren der optisch codierten Wahlhandlung, das Überprüfen der Wahloption auf dem zweizeiligen Display sowie die Eingabe eines persönlichen Identifikationsmerkmals (PIN, Fingerabdruck, Sprachsample, etc.) erfordert von der wahlberechtigten Person ein höheres Mass an Aufmerksamkeit, da die zur Verfügung stehende Hardware eingeschränkt ist. Wir erwarten hier eine ähnliche Erfahrung, wie sie Benutzer von anderen Smartcards, zum Beispiel der SuisseID, her kennen. Die in dieser Phase zu erwartende Benutzerfreundlichkeit ist dementsprechend eher geringer.

[6] *Election Markup Language*, OASIS, 2006, siehe http://xml.coverpages.org/eml.html.

Das Versenden der verschlüsselten Stimme kann mit der Verbreitung entsprechender Infrastruktur (sowohl bei der Stimmabgabe von zuhause aus wie auch im öffentlichen Raum) grösstenteils automatisiert werden. Dazu gehört auch die automatische Verifizierung während der Wahl. Somit erwarten wir hier eine gute Benutzerfreundlichkeit.

Verifizierung. Die Stufen der Verifizierung sind in Abschnitt 3.3 detailliert beschrieben worden. Die Benutzerfreundlichkeit der Stufe 1 (Verifizierung des Wahlgeräts vor der Wahl) besitzt dieselbe Benutzerfreundlichkeit wie oben unter Stimmabgabe beschrieben.

Die Stufe 2 (Automatische Verifizierung während der Wahl) besitzt eine hohe Benutzerfreundlichkeit, denn sie ist (nach Abgabe der Stimme) automatisiert. Ein akustisches Signal oder eine entsprechende Anzeige bestätigt, dass die Stimme beim Anschlagbrett aufgezeichnet wurde.

Bei der Stufe 3 (Optionale Verifizierung nach der Wahl) besorgt sich die interessierte Person sämtliche relevanten Daten vom öffentlichen Anschlagbrett. Unter Anwendung von spezifischen Verifizierungsapplikationen, die von verschiedenen Gruppierungen zur Verfügung gestellt werden, kann die Korrektheit der Daten des Anschlagbretts überprüft werden. Diese Stufe ist etwas aufwendig und auch rechenintensiv.

Benutzerfreundlichkeit für Sehbehinderte. Für die Phase der Vorbereitung der Stimme müssen Sehbehinderte Computer mit einer Sprachausgabe verwenden. Dazu muss die Software auf dem privaten Eingabegerät für die Sprachausgabe vorbereitet sein. Das Wahlgerät muss auch ein akustisches Signal von sich geben, sobald es den Matrixcode erfolgreich gescannt und dekodiert hat. In Bezug auf Sehbehinderte ist hier eine gute Benutzerfreundlichkeit zu erwarten.

Für die Überprüfung und Verschlüsselung der Stimme muss das Wahlgerät ebenfalls eine Sprachausgabe bereitstellen.[7] Die Benutzerfreundlichkeit ist in diesem Fall ähnlich wie bei Wählerinnen und Wählern ohne Sehbehinderung.

4.6. Homologation

Eine inhärente Systemeigenschaft des vorgeschlagenen Wahlsystems ist, dass alle Daten (ausser den privaten Schlüsseln) jederzeit und vollständig auf dem öffentlichen Anschlagbrett publiziert werden. Diese Eigenschaft bewirkt nach Ansicht der Autoren eine massive Reduktion des Umfanges und der Kosten der Zulassungsprozedur (Homologation) des Wahlsystems. Im Folgenden wird auf die nötigen Zulassungsprozeduren in den einzelnen Phasen eingegangen.

[7] Hierfür sind spezifische Wahlgeräte zu fabrizieren.

Phase 1: Setup. Die Wahlbehörde, die Zertifizierungsstelle sowie die Treuhänder publizieren öffentliche Schlüssel mit Hilfe von Zertifikaten. Jedermann kann dies prüfen. Die dazugehörigen ElGamal-Parameter werden auch publiziert, und die Güte dieser Parameter kann allgemein überprüft werden. Die Homologation dieser Phase beschränkt sich somit auf das Prüfen der Prozesse zur Erstellung der öffentlichen Daten.

Phase 2: Registrierung. In dieser Phase ist erstmals die Wahlkarte involviert. Dazu braucht es vermutlich eine Typenprüfung. Zudem könnten Hilfsmittel zur Verfügung gestellt werden, mit denen die Eigentümer von Karten deren Funktionsweise jederzeit selber überprüfen können. Gleichzeitig würde auch die Korrektheit des öffentlichen Schlüssels der Eigentümer geprüft. Die Homologation dieser Phase beschränkt sich auf die Typenprüfung der Karte.

Phase 3: Wahlvorbereitung. Das Resultat dieser Phase sind das Wählerverzeichnis und die publizierten öffentlichen Schlüssel der Wählerschaft, welche von den Treuhändern durch einen Mischprozess erstellt werden. Die Öffentlichkeit (oder Gruppierungen, welche die Öffentlichkeit in einem gewissen Sinne vertreten) prüfen stichprobenartig die publizierten Daten. Die Homologation dieser Phase beschränkt sich somit auf das Prüfen der Prozesse zur Erstellung der öffentlichen Daten, der Liste der Wahloptionen und dem Generator $\hat{g}$.

Phase 4: Stimmabgabe. Für die Stimmabgabe sind die Wahlkarte der wahlberechtigten Person sowie das Wahlgerät zentral. Die Funktionsweise der Wahlkarte ist durch die Typenprüfung und die optionale Prüfung der Karte durch die Eigentümer gegeben. Die korrekte Funktionsweise des Wahlgeräts ist wesentlich für das korrekte Funktionieren des Wahlsystems. Der Herausgeber des Wahlgeräts müsste eine Behörde sein, die für jedes einzelne Gerät garantieren kann, dass es korrekt funktioniert. Das heisst, dass jedes einzelne Wahlgerät homologiert werden muss. Jedoch ist die Menge der Funktionen des Wahlgeräts klein und begrenzt, und die Prüfung kann vermutlich automatisiert werden.

Phase 5: Wahlnachbereitung. Die für die Wahlnachbearbeitung vorhandenen Daten und die in dieser Phase erzeugten Daten sind öffentlich überprüfbar. Die Homologation beschränkt sich somit auf das Prüfen der involvierten Prozesse. Der Betrieb des öffentlichen Anschlagbretts ist vergleichbar mit dem sicheren Betrieb von Rechenzentren. Deshalb genügt es, jedes involvierte Rechenzentrum mit bekannten Standards, zum Beispiel der ISO-27000-Reihe, zu homologieren.

Phase 6: Auszählung. Das Ergebnis der Auszählung sind öffentlich verifizierbare Daten. Die Homologation dieser Phase beschränkt sich somit auf das Prüfen der Prozesse zur Erstellung der öffentlichen Daten.

Phase 7: Verifizierung. Für die individuelle und universelle Verifizierung soll die notwendige Software von verschiedenen unabhängigen Herstellern zur Verfügung gestellt werden. Die Prüfung der Software könnte man mit zum Beispiel Testdaten, die einmalig auf dem öffentlichen Anschlagbrett publiziert werden, bewerkstelligen. Eine amtliche Homologation entfällt daher.

Phase 8: Revozieren. Alle beim Revozieren involvierten Komponenten sind in den obigen Schritten bereits einer Prüfung unterzogen worden. Die Homologation dieser Phase beschränkt sich somit auf das Prüfen des Prozesses.

5. Schlussbemerkungen

Das in diesem Bericht vorgelegte Konzept ist ein erster Schritt in Richtung eines Wahl- und Abstimmungssystems der *zweiten Generation*, welches es den Wählerinnen und Wähler erlaubt, den Weg der abgegebenen elektronischen Stimme und die Berücksichtigung der Stimme bei der Auszählung nachvollziehen und die Korrektheit des Endergebnisses überprüfen zu können. Diese Eigenschaft besitzen die bestehenden Schweizer Systeme nicht. Auch auf dem internationalen Parkett gibt es bisher kein verifizierbares System, das für verbindliche politische Wahlen oder Abstimmungen eingesetzt wurde. Als vertrauensbildende Massnahme und für die Weiterführung der Schweizer Pionierrolle wäre die Einführung eines solchen Systems äusserst wünschenswert. Auch wenn dies kurzfristig aus unterschiedlichen Gründen vielleicht nicht realisierbar ist, könnte das vorgestellte System die Rolle eines *Referenz-Systems* einnehmen, an das sich die bestehenden Systeme stufenweise annähern könnten.

In den folgenden zwei Abschnitten werden die wichtigsten Schlussfolgerungen dieser Arbeit kurz zusammengefasst und ein Ausblick auf das mögliche weitere Vorgehen dargelegt. Selbstverständlich sind damit nicht alle Probleme gelöst und alle Fragen beantwortet, aber einige der wichtigsten Grundpfeiler sind damit gelegt.

5.1. Fazit

In Abschnitt 1.2 wurden aus der vorgegebenen Aufgabenstellung 12 Zielsetzungen formuliert. Beim Erarbeiten dieses Konzepts dienten diese als Orientierungspunkte. Die nachfolgende Diskussion dieser 12 Punkte fasst die erreichten Ziele und die noch offenen Probleme zusammen.

1. Die Verifizierbarkeit der Wahl- und Abstimmungsergebnisse ist eine der zentralen Eigenschaften des vorgeschlagenen Systems. Hierzu werden die abgegebenen Stimmen auf einem öffentlichen Anschlagbrett veröffentlicht, damit sowohl der Einbezug einer einzelnen Stimme wie auch die Korrektheit des Gesamtergebnisses überprüft werden können. Die verschiedenen Aspekte der Verifizierbarkeit wurden in entsprechenden Verifikationsprozeduren umfassend berücksichtigt und umgesetzt (siehe Abschnitt 3.3). In diesem Punkt unterscheidet das vorgestellte System grundsätzlich von den existierenden Schweizer Systemen.
2. Das Problem der sicheren Plattform ist im Konzept so gelöst, dass die eigentliche Wahlhandlung nicht auf den persönlichen Endgeräten der Wählerinnen und

Wähler stattfindet, sondern auf vertrauenswürdigen Wahlgeräten, die bei der Registrierung zusammen mit einer persönlichen Wahlkarte verteilt werden. Das vorgestellte Gerät und das damit verbundene Verfahren ist ähnlich zu den Lösungen, die im Bereich des Online-Banking von einigen Banken zur Verfügung gestellt werden. Die Bank-Transaktionen werden dabei im Web-Browser erfasst und müssen auf dem vertrauenswürdigen Gerät bestätigt werden. Im Vergleich dazu stellt die Geheimhaltung der abgegebenen Stimme eine zusätzliche Forderung dar, welcher dadurch Rechnung getragen wird, dass die persönlichen Endgeräte aufgrund der optischen Schnittstelle zum Wahlgerät die eigentliche Wahlhandlung nicht „beobachten“ können.

3. Die Möglichkeit, eine Wahlhandlung durch Dritte zu beeinflussen (z.B. durch Bestechung oder Nötigung), ist im vorgestellten Konzept dadurch stark eingeschränkt, dass das System unter gewissen Annahmen quittungsfrei ist. Diese Annahmen beziehen sich vor allem auf eine Eigenschaft des Wahlgeräts, nämlich dass die bei der Verschlüsselung der Stimme verwendetet Zufallszahl nicht ausgelesen werden kann. Da es im vorgegebenen Kontext nicht vorgesehen ist, dass eine abgegebene elektronische Stimme überschrieben werden kann (elektronisch oder auf Papier), ist eine Beeinflussung durch physisch präsente dritte Personen aber weiterhin möglich. Entsprechende *Vote Updating*-Prozeduren werden aber vom Wahlprotokoll unterstützt und könnten ins Konzept aufgenommen werden.

4. Das Wahlgeheimnis wird im vorgestellten Konzept durch verschiedene Massnahmen umfassend geschützt. Der Schutz entsteht in erster Linie durch die Verschlüsselung der Stimme und den Einsatz des vorgestellten Schwellwertverfahrens, bei dem der private Schlüssel für die Entschlüsselung unter mehreren Treuhändern geteilt wird. Der private Schlüssel, von dem das Geheimnis des Wahl massgebend abhängt, muss dabei weder explizit generiert, abgespeichert oder rekonstruiert werden. Somit hängt die Geheimhaltung der Stimmen nicht davon ab, dass der Zugriff auf einen entsprechen Datenspeicher eingeschränkt ist, sondern nur auf der Annahme, dass keine Mehrheit der Treuhänder in böswilliger Absicht kooperiert. Diese Eigenschaft ist eine weitere wichtige Neuerung gegenüber den existierenden Schweizer Systemen. Hinzu kommt die vorgestellte Lösung für das Problem der sicheren Plattform, bei der die persönlichen Endgeräte der Wählerinnen und Wähler die abgegebene Stimme nicht in Erfahrung bringen können.

5. Das vorgestellte Konzept beruht vollumfänglich auf dem heutigen Stand der wissenschaftlichen Forschung. Aus den existierenden Protokoll- und Systemvorschlägen wurden die aus der Sicht der Autoren geeignetsten Verfahren ausgewählt und auf den vorgegebenen Kontext zugeschnitten. Auch der in der Literatur übliche Anforderungskatalog wurde als Messlatte dem Konzept zugrunde gelegt.

6. Das vorgestellte Konzept geht von einer einmaligen Registrierung aus, bei dem die Wählerinnen und Wähler ihre Wahlkarten und Wahlgeräte erhalten. Danach ist das Versenden der Wahl- und Abstimmungsunterlagen per Post nicht mehr erforderlich. Besonders für Auslandschweizer mit häufig wechselnden Wohnorten ist diese Möglichkeit von grossem Interesse. Zudem stellt es für die Wahlbehörden

ein grosses Potential für Kosteneinsparungen dar, wenn mittel- oder langfristig sich ein grosser Teil der Wählerschaft für die elektronische Stimmabgabe entscheidet.

7. Das es im vorgegebenen Kontext weiterhin möglich sein muss, die Stimme über einen traditionellen Kanal abzugeben, dürfen die registrierten *E-Wähler* nicht von dieser Möglichkeit ausgeschlossen sein. Das Konzept geht allerdings davon aus, dass dies ein Ausnahmefall darstellt und deshalb eine geringer Mehraufwand seitens der betroffenen Person zumutbar ist. Konkret muss dabei ein Beweis erbracht werden, dass keine elektronische Stimme abgegeben wurde. Dies geschieht mit Hilfe der Wahlkarte, entweder durch die Wählerin oder den Wähler selbst (durch Ausdrucken eines maschinenlesbaren Codes), oder durch eine entsprechende Prozedur im Wahllokal.

8. Eine der grössten Herausforderungen beim Design des Wahlgerätes bestand darin, dieses so einfach wie möglich zu halten, jedoch gleichzeitig ein Höchstmass an Benutzerfreundlichkeit zu bieten. Durch die vorgeschlagene Kombination mit den persönlichen Endgeräten der Wählerinnen und Wähler (siehe Abschnitt 3.2.2), die den Einsatz aller möglichen heutigen und zukünftigen Geräten und Technologien zulässt, ist dies aber vollumfänglich gelungen. Gewisse Einschränkungen an der Benutzerfreundlichkeit gibt es jedoch bei der Prozedur mit der optischen Schnittstelle zum Wahlgerät, die vielen Personen relativ ungewohnt oder umständlich erscheinen mag. Durch die Möglichkeit, diesen Personen eine ständig verfügbare Testwahl zur Verfügung zu stellen, können sie sich jedoch im Voraus mit dieser Prozedur vertraut machen.

9. Um die ständige Verfügbarkeit und die Ausfallssicherheit des Systems garantieren zu können, sind im vorgestellten Konzept alle kritischen Single-Points-of-Failure durch entsprechende Schwellwertverfahren ersetzt worden. Diese können den Ausfall einzelner Komponenten durch technische Probleme oder gezielte Angriffe kompensieren. Eines der grössten offenen Probleme diesbezüglich ist der Bau eines robusten öffentlichen Anschlagbretts, zum dem es bisher in der Literatur nur wenig Ansätze gibt.

10. Das vorgestellte Konzept ist umfassend darauf vorbereitet, den Besonderheiten des Schweizer Wahl- und Abstimmungskontexts Rechnung zu tragen. So ist es zum Beispiel problemlos möglich, gleichzeitig Wahlen oder Abstimmungen auf den verschiedenen politischen Stufen durchzuführen. Dazu müssen die Einträge auf dem öffentlichen Anschlagbrett logisch voneinander getrennt werden, so dass bei der Auszählung einer einzelnen Vorlage die relevanten Einträge herausgefiltert werden können. In gleicher Weise können die Teilresultate der einzelnen Gemeinden, Bezirke oder Kantone ermittelt werden. Die für die Durchführung von nationalen Vorlagen benötigten Rechenleistungen sind mit den heute verfügbaren Computersystemen relativ leicht zu erbringen.

11. Das Konzept sieht vor, dass die Spezifikationen sämtlicher Komponenten und Prozeduren offengelegt werden können, ohne dadurch die Sicherheit in irgendeiner Weise zu tangieren. Für die Verifizierbarkeit werden sogar sämtliche Daten einer Wahl oder Abstimmung der Öffentlichkeit zur Verfügung gestellt. Mit Ausnahme

der involvierten privaten Schlüssel der beteiligten Personen gibt es also im gesamten System keinerlei Geheimnisse. Dadurch ist ein Höchstmass an Transparenz gewährleistet.

12. Die Kosten einer möglichen Umsetzung des vorgestellten Konzepts sind zurzeit noch weitgehend unbekannt. Im Vergleich zu den bestehenden Schweizer Systemen stellen vor allem das Wahlgerät und die Wahlkarte zwei kostenkritische Komponenten dar. Aus diesem Grund wurde die Funktionalität des Geräts so einfach wie möglich gehalten. Eine andere unbekannte Kostengrösse ist die Realisierung und der sichere Betrieb des öffentlichen Anschlagbretts. Hierzu können im Moment keine Angaben gemacht werden. Auf der anderen Seite bietet das vorgestellte Konzept auch ein grosses Potential für Kosteneinsparungen, zum Beispiel beim nicht länger benötigten Versand der Abstimmungsunterlagen, bei der einfachen Realisierung der Wahlplattform, oder bei den grundsätzlichen Vereinfachungen (z.B. bezüglich Serverinfrastruktur oder Homologation), die die Offenlegung der Daten mit sich bringt.

Gesamthaft betrachtet ist im Licht der obigen Diskussion die grosse Mehrheit der gestellten Zielsetzungen zufriedenstellend erfüllt. Viele der erwähnten Gesichtspunkte stellen im Vergleich zu den bestehenden Schweizer Systemen substantielle Neuerungen und Verbesserungen dar.

5.2. Weiteres Vorgehen

Aus Sicht der Autorenschaft stellt das vorgelegte Konzept einen ersten Schritt und eine Diskussionsgrundlage für ein mögliches zukünftiges Schweizer *Vote Électronique* System dar. Als erster nächster Schritt wäre es deshalb wünschenswert, wenn das Konzept verschiedensten nationalen und internationalen Experten zur Begutachtung und Beurteilung vorgelegt würde. Dabei geht es vor allem darum, mögliche Schwachstellen oder Verbesserungen aufzudecken, die von den Autoren im vorliegenden Bericht übersehen wurden. Im Idealfall entsteht dabei eine Art Konsens darüber, wie dieses zukünftige Schweizer System aussehen müsste.

Im Weiteren sollte das Konzept der von der Bundeskanzlei geleiteten Arbeitsgruppe *Vote Électronique* vorgelegt werden, um die Meinung der Personen einzuholen, die sich in den Kantonen mit diesem Thema befassen. Das Konzept könnte auch dazu dienen, bei den bestehenden Systemen punktuelle Verbesserungen zu realisieren. Entscheidend dabei ist, dass das Vorlegen dieses Berichts zur Diskussion über die möglichen Eigenschaften zukünftiger elektronischer Wahlsysteme beiträgt. Die Autoren erklären sich bereit, an einer solchen Diskussion aktiv und mit einer konstruktiven Grundhaltung teilzunehmen.

Unabhängig davon wird die Autorenschaft an einigen der offenen Fragestellungen weiterarbeiten. Aus wissenschaftlicher Sicht ist vor allem eine detailliertere Spezifikationen des Wahlgeräts und der Wahlkarte von grossem Interesse. Für die Realisierung eines robusten öffentlichen Anschlagbrettes wurden bereits Arbeiten in Angriff genommen.

Es ist auch geplant, im Rahmen von studentischen Arbeiten einzelne Komponenten des Systems zu realisieren.

A. Kryptographische Grundlagen

Auf den folgenden Seiten werden einige wichtige kryptographische Grundlagen eingeführt, die für das Verständnis des vorgestellten Konzepts und der darin enthaltenen Komponenten nützlich sein können. Für eine vertiefte Darstellung dieser Themen verweisen sei auf entsprechende Fachliteratur oder Resourcen im Internet verwiesen.

Verschlüsselung. Bei einer Verschlüsselung wird mit Hilfe eines geheimen *Schlüssels* k ein sogenannter *Klartext* m (Text, Datei, E-Mail, etc.) in einen *Chiffriertext* $c = \mathit{Encrypt}_k(m)$ umgewandelt, wobei *Encrypt* den gewählten Verschlüsselungsalgorithmus bezeichnet. Dies geschieht so, dass es nicht möglich ist, ohne Kenntnis des geheimen Schlüssels k den Klartext m aus c herzuleiten. Dazu muss zum Beispiel die Anzahl der möglichen Schlüssel so gross sein, dass es nicht möglich ist, alle Schlüssel einzeln durchzuprobieren. Wenn nun c anstelle von m über einen unsicheren Übertragungskanal (z.B. über das Internet) verschickt wird, dann kann die Nachricht m von niemandem gelesen werden, auch wenn jemand in den Besitz von c gelangen sollte. Man kann so also die *Vertraulichkeit* bei der Übertragung einer Nachricht garantieren.

Bei einem *symmetrischen* Verschlüsselungssystem muss der Empfänger des Chiffriertextes c den gleichen Schlüssel k kennen, damit er mit Hilfe des Entschlüsselungsalgorithmus *Decrypt* die Nachricht $m = \mathit{Decrypt}_k(c)$ wiederherstellen kann. Das Problem bei einem solchen Verfahren ist der sichere *Schlüsselaustausch*, für den man nicht auf den unsicheren Übertragungskanal zurückgreifen kann. Der heutige symmetrische Verschlüsselungsstandard ist AES (Advanced Encryption Standard), welcher mit Schlüsseln der Länge 128 bis 256 Bits arbeitet.

Ein *asymmetrischen* Verschlüsselungssystem geht von zwei unterschiedlichen Schlüsseln aus, einer für die Verschlüsselung (der sogenannte *öffentliche* Schlüssel e) und einer für die Entschlüsselung (der sogenannte *private* Schlüssel d). Die Verschlüsselung wird somit durch $c = \mathit{Encrypt}_e(m)$ und die Entschlüsselung durch $m = \mathit{Decrypt}_d(c)$ beschrieben. Der Vorteil gegenüber einem symmetrischen Verfahren liegt darin, dass der öffentliche Schlüssel nicht geheim ist, was den sicheren Schlüsselaustausch stark vereinfacht. Die meisten bekannten asymmetrischen Verfahren arbeiten mit sehr grossen Zahlen (ca. 300 bis 600 Dezimalstellen). Entsprechend besitzen die Schlüssel eine Länge von ca. 1024 bis 2048 Bits. Da die asymmetrischen Verfahren relativ rechenintensiv sind, werden diese oft nur dazu verwendet, um einen geheimen Schlüssel für eine symmetrische Verschlüsselung auszutauschen (*hybrides* Verschlüsselungssystem).

Die wichtigsten asymmetrischen Verfahren sind RSA und ElGamal. Im Gegensatz zu RSA, ist ELGamal ein sogenanntes *randomisiertes* Verfahren, bei welchem ein zufälliger Wert in die Verschlüsselung einfliesst (die sogenannte *Randomisierung*). Wenn also

der gleiche Klartext m mehrfach mit dem gleichen öffentlichen Schlüssel e ElGamal-verschlüsselt wird, entsteht immer ein anderer Chiffriertext.

Digitale Signaturen. Das Konzept einer digitalen Unterschrift geht, wie die asymmetrische Verschlüsselung von zwei Schlüsseln aus. Der private Schlüssel wird dabei verwendet, um eine Signatur $s = \mathit{Sign}_d(m)$ eines Dokumentes oder einer Nachricht m zu erzeugen. Diese kann dann mit Hilfe des öffentlichen Schlüssels e überprüft werden. Bei erfolgreicher Überprüfung, das heisst, wenn $\mathit{Verify}_e(m, s) = \mathit{true}$ ergibt, dann ist sichergestellt, dass das Dokument einerseits von einer bestimmten Person (dem Besitzer des privaten Schlüssels) stammen muss und andererseits nicht verändert wurde. Somit wird mit einer digitalen Signatur die *Authentizität* und die *Integrität* eines Dokumentes gewährleistet.

Die beiden bekanntesten Signaturverfahren sind mit den Verschlüsselungsverfahren RSA und ElGamal verwandt. Die ElGamal-Variante ist unter dem Namen *Digital Signature Algorithm* (DSA) bekannt. Es handelt sich ebenfalls um ein randomisiertes Verfahren, bei dem ein Zufallswert in die Signatur einfliesst, das heisst, verschiedene Signaturen des gleichen Dokumentes sehen völlig unterschiedlich aus.

Digitale Zertifikate. Um sicher zu sein, dass ein öffentlicher Schlüssel einer bestimmten Person gehört, können diese von einer vertrauenswürdigen Instanz zertifiziert werden. Technisch gesehen wird dabei der Schlüssel mit der Identität der Person (z.B. ein eindeutiger Name oder eine E-Mail-Adresse) verknüpft und von der Zertifizierungsstelle digital unterschrieben. Durch Überprüfen dieser Signatur lässt sich so die Echtheit des Schlüssels verifizieren (unter der Annahme, dass die Zertifizierungsstelle tatsächlich vertrauenswürdig ist).

Kryptographische Protokolle. Ein kryptographisches Protokoll ist eine Vereinbarung zwischen Kommunikationspartnern über die Art, den Inhalt und die Reihenfolge von ausgetauschten Nachrichten. Diese Nachrichten enthalten kryptographische Elemente (Verschlüsselungen, digitale Signaturen, etc.), die zur Erreichung von bestimmten Sicherheitszielen dienen. Kryptographische Protokolle bilden somit die Schnittstelle für die Umsetzung der Kryptographie in der Praxis. Ein bekanntes kryptographisches Protokoll ist SSL (Secure Socket Layer), sowie dessen Nachfolger TLS (Transport Security Layer), welches unter den Namen HTTPS für die sichere Datenübertragung im World Wide Web eingesetzt werden.

Secret Sharing. Viele kryptographische Protokolle beruhen darauf, dass einige der involvierten Kommunikationsteilnehmer ein Geheimnis (z.B. einen privaten Schlüssel) für sich behalten. Damit die Sicherheit des Protokolls nicht gefährdet ist, falls ein solches Geheimnis gestohlen oder absichtlich preisgegeben wird, gibt es sogenannte *Secret Sharing* Verfahren, um ein Geheimnis unter mehreren Personen zu teilen. Diese Verfahren sind so aufgebaut, dass es mindestens t (von n) viele Personen braucht, um das Geheimnis wiederherstellen zu können. Das Fehlverhalten von einzelnen Personen kann somit

die Sicherheit des Systems nicht mehr gefährden. Durch den gezielten Einsatz dieses Verfahrens erhöht sich somit die *Robustheit* eines Systems. Dabei wird der Wert t als *Schwellwert* bezeichnet.

Handelt es sich beim geteilten Geheimnis um einen privaten Schlüssel eines asymmetrischen Verschlüsselungssystems, dann ist es sogar möglich, einen Chiffriertext als Gruppe mit Hilfe der entsprechenden Teilschlüssel zu entschlüsseln, ohne dass die einzelnen Teilschlüssel preisgegeben werden müssen oder der gemeinsame private Schlüssel rekonstruiert wird. Auf diese Art können vertrauliche Nachrichten an eine Gruppe übermittelt werden, wobei für die Entschlüsselung jeder einzelnen Nachricht jeweils das Einverständnis einer Mehrheit der Gruppenmitglieder nötig ist, da der private Schlüssel nie bekannt wird.

Zero-Knowledge Beweise. Beim Design von kryptographischen Protokollen gilt es zu berücksichtigen, dass die involvierten Parteien gezielt vom Protokoll abweichen könnten, um zum Beispiel eines der Sicherheitsziele zu umgehen. Um solches Fehlverhalten zu verhindern, werden oft sogenannte *Zero-Knowledge* Beweise ins Protokoll eingebaut, welche die Teilnehmer zwingen, sich dem Protokoll entsprechend zu verhalten. Mit solchen Beweisen kann zum Beispiel jemand überzeugt werden, dass man Kenntnis von einem Geheimnis hat, ohne jedoch das Geheimnis selbst oder Teile davon preisgeben zu müssen. Wer das Geheimnis nicht kennt, kann diesen Beweis nur mit einer verschwindend kleinen Wahrscheinlichkeit erzeugen, das heisst, der Versuch vom Protokoll abzuweichen würde mit überwältigend grosser Wahrscheinlichkeit entdeckt. Ein anderes Beispiel ist der Beweis, dass ein Chiffriertext einen bestimmten Klartext aus einer Menge von möglichen Klartexten enthält, ohne jedoch einen Hinweis darauf zu geben, welchen davon.

Verifizierbare Mix-Netzwerke. Während viele kryptographische Anwendungen darauf ausgerichtet sind, die Authentizität einer verschlüsselten Nachricht zu gewährleisten, gibt es auch Fälle, wo genau das Gegenteil davon erreicht werden soll, nämlich den Ursprung bzw. den Urheber einer verschlüsselten Nachricht zu verbergen. Bei randomisierten Verschlüsselungsverfahren, zum Beispiel bei ElGamal, gibt es dazu die Möglichkeit, eine *Wiederverschlüsselung* einer verschlüsselten Nachricht durchzuführen. Man führt dabei auf der verschlüsselten Nachricht eine Operation durch, welche die Randomisierung der Verschlüsselung verändert, ohne jedoch den darin verborgenen Klartext zu verändern. Um nun die Urheber von mehreren verschlüsselten Nachrichten zu verbergen, werden diese in einem *Mix-Netzwerk* von sogenannten *Mix-Servern* mehrfach hintereinander wiederverschlüsselt und gemischt. Am Ende des Netzwerkes werden so Wiederverschlüsselungen der ursprünglich verschlüsselten Nachrichten ausgegeben. Diese können aber nicht mehr miteinander in Beziehung gebracht werden (hierzu müssten alle Mix-Server zusammenspannen). Um zu garantieren, dass die Mix-Server ihren Dienst vorschriftsgemäss verrichtet haben, müssen entsprechende Zero-Knowledge Beweise publiziert werden, die dies bezeugen. In einem Mix-Netzwerk findet also eine verifizierbare Anonymisierung von verschlüsselten Nachrichten statt. Ähnliche Techniken werden eingesetzt, um sogenannte *anonyme Kanäle* zu realisieren oder um *anonyme Authentifizierungen* durchzuführen.

Literaturverzeichnis

[1] B. Adida. Helios: Web-based open-audit voting. In P. Van Oorschot, editor, *SS'08, 17th USENIX Security Symposium*, pages 335–348, San Jose, USA, 2008.

[2] B. Adida, O. de Marneffe, O. Pereira, and J. J. Quisquater. Electing a university president using open-audit voting: Analysis of real-world use of Helios. In D. Jefferson, J. L. Hall, and T. Moran, editors, *EVT/WOTE'09, Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, Montreal, Canada, 2009.

[3] B. Adida and C. A. Neff. Ballot casting assurance. In D. S. Wallach and R. L. Rivest, editors, *EVT'06, USENIX/ACCURATE Electronic Voting Technology Workshop*, Vancouver, Canada, 2006.

[4] R. Araújo, R. Robbana N. Ben Rajeb, J. Traoré, and S. Youssfi. Towards practical and secure coercion-resistant electronic elections. In S. H. Heng, R. N. Wright, and B. M. Goi, editors, *CANS'10, 9th International Conference on Cryptology And Network Security*, LNCS 6467, pages 278–297, Kuala Lumpur, Malaysia, 2010.

[5] P. Beaucamps, D. Reynaud-Plantey, J. Y. Marion, and E. Filiol. On the impact of malware on internet voting. In *1st Luxembourg Day on Security and Reliability*, 2009.

[6] J. Benaloh. Simple verifiable election. In D. S. Wallach and R. L. Rivest, editors, *EVT'06, USENIX/ACCURATE Electronic Voting Technology Workshop*, Vancouver, Canada, 2006.

[7] J. Benaloh. Ballot casting assurance via voter-initiated poll station auditing. In *EVT'07, USENIX/ACCURATE Electronic Voting Technology Workshop*, Boston, USA, 2007.

[8] J. Beuchart. Append-only web bulletin board. Project report, Bern University of Applied Sciences, Biel, Switzerland, 2011.

[9] D. Chaum. Blind signature system. In *CRYPTO'83, 3rd International Cryptology Conference*, pages 153–156, Santa Barbara, USA, 1983.

[10] J. Clark and U. Hengartner. Selections: Internet voting with over-the-shoulder coercion-resistance. In G. Danezis, editor, *FC'11, 15th International Conference on Financial Cryptography*, LNCS 7035, pages 47–61, St. Lucia, 2011.

[11] M. Clarkson, B. Hay, M. Inge, D. Wagner, and A. Yasinsac. Software review and security analysis of scytl remote voting software. Technical report, Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, USA, 2008.

[12] M. R. Clarkson, S. Chong, and A. C. Myers. Civitas: Toward a secure voting system. In *SP'08, 29th IEEE Symposium on Security and Privacy*, pages 354–368, Oakland, USA, 2008.

[13] Council of Europe. *Legal, Operational and Technical Standards for e-Voting.* Rec(2004)11. Council of Europe Publishing, 2004.

[14] Council of Europe. *Guidelines on Transparency of E-Enabled Elections.* GGIS (2010) 5 fin. E. Council of Europe Publishing, 2011.

[15] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In W. Fumy, editor, *EUROCRYPT'97, International Conference on the Theory and Application of Cryptographic Techniques*, LNCS 1233, pages 103–118, Konstanz, Germany, 1997.

[16] Die Bundesbehörden der Schweizerischen Eidgenossenschaft. Bericht über die Pilotprojekte zum Vote électronique. *Bundesblatt*, 158(25):5459–5538, 2006.

[17] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In M. Blaze, editor, *SS'04, 13th USENIX Security Symposium*, pages 303–320, San Diego, USA, 2004.

[18] E. Dubuis, S. Fischli, R. Haenni, U. Serdült, and O. Spycher. Selectio Helvetica: A verifiable remote e-voting system. In *CeDEM'11, Conference for E-Democracy and Open Government*, Krems, Austria, 2011.

[19] Eric Dubuis, O. Spycher, and M. Volkamer. Vertrauensbildung bei Internetwahlen. *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2:96–99, 2011.

[20] J. Feigenbaum, A. Johnson, and P. Syverson. Probabilistic analysis of onion routing in a black-box model. In P. Ning and T. Yu, editors, *WPES'07, 6th ACM Workshop on Privacy in Electronic Society*, pages 1–10, Alexandria, USA, 2007.

[21] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In J. Seberry and Y. Zheng, editors, *ASIACRYPT'92, Workshop on the Theory and Application of Cryptographic Techniques*, LNCS 718, pages 244–251, Gold Coast, Australia, 1992.

[22] I. Goldberg. On the security of the Tor authentication protocol. In G. Danezis and P. Golle, editors, *PET'06, 6th Workshop on Privacy Enhancing Technologies*, pages 316–331, Cambridge, U.K., 2006.

[23] R. Haenni and O. Spycher. Secure internet voting on limited devices with anonymized DSA public keys. In *EVT/WOTE'11, Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, San Francisco, USA, 2011.

[24] J. Heather and D. Lundin. The append-only web bulletin board. In P. Degano, J. Guttman, and F. Martinelli, editors, *FAST'08, 5th International Workshop on Formal Aspects in Security and Trust*, LNCS 5491, pages 242–256, Malaga, Spain, 2008.

[25] J. Heather, P. Y. A. Ryan, and V. Teague. Pretty good democracy for more expressive voting schemes. In D. Gritzalis, B. Preneel, and M. Theoharidou, editors, *ESORICS'10, 5th European Conference on Research in Somputer Security*, pages 405–423, Athens, Greece, 2010.

[26] J. Helbach. *Eingrenzung des Secure Platform Problems bei Internetwahlsystemen mit Hilfe von Code Voting*. PhD thesis, Department of Electrical Engineering and Information Science, Ruhr University, Bochum, Germany, 2010.

[27] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In V. Atluri, S. De Capitani di Vimercati, and R. Dingledine, editors, *WPES'05, 4th ACM Workshop on Privacy in the Electronic Society*, pages 61–70, Alexandria, USA, 2005.

[28] R. Koenig, R. Haenni, and S. Fischli. Preventing board flooding attacks in coercion-resistant electronic voting schemes. In J. Camenisch, S. Fischer-Hübner, Y. Murayama, A. Portmann, and C. Rieder, editors, *SEC'11, 26th IFIP International Information Security Conference*, volume 354, pages 116–127, Lucerne, Switzerland, 2011.

[29] K. Loesing, S. J. Murdoch, and R. Dingledine. A case study on measuring statistical data in the Tor anonymity network. In R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako, and F. Sebe, editors, *FC'10, 14th International Conference on Financial Cryptograpy and Data Security*, pages 203–215, Tenerife, Spain, 2010.

[30] C. A. Neff. Verifiable mixing (shuffling) of ElGamal pairs. Technical report, VoteHere, Inc., 2004.

[31] R. Oppliger. How to address the secure platform problem for remote internet voting. In *SIS'02, 5th Conference on "Sicherheit in Informationssystemen"*, pages 153–173, Vienna, Austria, 2002.

[32] R. Oppliger. E-voting auf unsicheren client-plattformen. *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 8(2):82–85, 2008.

[33] R. Oppliger, J. Schwenk, and J. Helbach. Protecting code voting against vote selling. In A. Alkassar and J. H. Siekmann, editors, *Sicherheit'08, 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V.*, pages 193–204, Saarbrücken, Germany, 2008.

[34] R. A. Peters. A secure bulletin board. Master's thesis, Department of Mathematics and Computing Science, Technische Universiteit Eindhoven, The Netherlands, 2005.

[35] M. K. Reiter. Secure agreement protocols: Reliable and atomic group multicast in Rampart. In *CCS'94, 2nd ACM Conference on Computer and Communications Security*, pages 68–80, Fairfax, USA, 1994.

[36] M. K. Reiter. A secure group membership protocol. *IEEE Transactions on Software Engineering*, 22(1):31–42, 1996.

[37] K. Sako and J. Kilian. Receipt-free mix-type voting scheme: A practical solution to the implementation of a voting booth. In L. C. Guillou and J. J. Quisquater, editors, *EUROCRYPT'95, 15th International Conference on the Theory and Applications of Cryptographic Techniques*, LNCS 921, pages 393–403, Saint-Malo, France, 1995.

[38] G. Schryen and E. Rich. Security in large-scale Internet elections: A retrospective analysis of elections in Estonia, the Netherlands, and Switzerland. *IEEE Transactions on Information Forensics and Security*, 4(4):729–744, 2009.

[39] O. Spycher and R. Haenni. A novel protocol to allow revocation of votes in a hybrid voting system. In *ISSA'10, 9th Annual Conference on Information Security – South Africa*, Sandton, South Africa, 2010.

[40] O. Spycher, R. Haenni, and E. Dubuis. Coercion-resistant hybrid voting systems. In R. Krimmer and R. Grimm, editors, *EVOTE'10, 4th International Workshop on Electronic Voting*, number P-167 in Lecture Notes in Informatics, pages 269–282, Bregenz, Austria, 2010. Gesellschaft für Informatik E.V.

[41] O. Spycher, R. Koenig, R. Haenni, and M. Schläpfer. A new approach towards coercion-resistant remote e-voting in linear time. In G. Danezis, editor, *FC'11, 15th International Conference on Financial Cryptography*, LNCS 7035, pages 182–189, St. Lucia, 2011.

[42] O. Spycher, M. Volkamer, and R. Koenig. Transparency and technical measures to establish trust in Norwegian Internet voting. In *VoteID'11, 3rd International Conference on E-Voting and Identity*, Tallinn, Estonia, 2011.

[43] The Verified Voting Foundation. Computer technologists' statement on internet voting. http://verifiedvoting.org/downloads/InternetVotingStatement.pdf, 2008.

[44] T. Weigold and A. Hiltgen. Secure confirmation of sensitive transaction data in modern Internet banking services. In *WorldCIS'11, World Congress on Internet Security*, pages 125–132, London, U.K., 2011.