Verifizierbare Internet-Wahlen an Schweizer Hochschulen mit UniVote

E. Dubuis, S. Fischli, R. Haenni, S. Hauser, R. E. Koenig, P. Locher,
J. Ritter, P. von Bergen

Research Institute for Security in the Information Society
Berner Fachhochschule
Quellgasse 21, CH-2501 Biel, Schweiz
eric.dubuis@bfh.ch

Abstract: Dieser Bericht dokumentiert den erstmaligen Einsatz des Internet-Wahlsystems UniVote anlässlich der Wahl des Studierendenrats an drei Schweizer Hochschulen im Frühling 2013. Mittels kryptographischer Methoden garantiert UniVote eine anonyme und geheime Stimmabgabe und ermöglicht gleichzeitig die Verifizierung des Wahlresultats durch Dritte mittels unabhängiger Software. Dazu werden sämtliche Wahldaten veröffentlicht.

1 Einführung

Die meisten Studierenden an einer Schweizer Hochschule sind Mitglied eines Studierendenverbandes, der in hochschulpolitischen Fragen die Interessen der Studierenden vertritt. Diese Verbände werden von einem demokratisch gewählten *Studierendenrat* (StuRa) geleitet und repräsentiert. Entsprechende StuRa-Wahlen finden alle 1–2 Jahre statt. Die Wahl- und Repräsentationsmodelle sind lokal leicht unterschiedlich. Im Vergleich zu Deutschen Hochschulen vereint der Studierendenrat die Funktionen des Studierendenparlaments (StuPa) und des Allgemeinen Studierendenausschusses (AStA).

Bisher wurden StuRa-Wahlen an Schweizer Hochschulen mehrheitlich in Form von Brief- oder Urnenwahlen durchgeführt. Der organisatorische und finanzielle Aufwand dazu ist erheblich und kann von den Studierendenverbänden nur schwer bewältigt werden. Deshalb ist in den vergangenen Jahren der Wunsch entstanden, StuRa-Wahlen zukünftig in elektronischer Form über das Internet durchzuführen. An der Universität Bern entwickelte ein StuRa-Mitglied selbst ein einfaches System, das für die StuRa-Wahlen 2011 einmalig eingesetzt wurde. Da dieses System nur bescheidene Sicherheitseigenschaften besitzt und es somit potentiell die Korrektheit des Wahlresultats und das Stimmgeheimnis der Wähler[1] gefährdet, wurde von der weiteren Verwendung des Systems abgesehen.

Aus dieser Ausgangslage entstand im Frühling 2012 an der Berner Fachhochschule das Pro-

[1] Zugunsten der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet und die männliche Nominalform angeführt. Gemeint und angesprochen sind jedoch immer beide Geschlechter.

jekt *UniVote*.[2] Das Ziel des Projekts ist die Realisierung eines neuen Internet-Wahlsystems für StuRa-Wahlen an Schweizer Hochschulen, welches möglichst viele Eigenschaften eines sicheren Internet-Wahlsystem besitzt. Vor allem soll es möglich sein, das Wahlergebnis im Nachhinein mittels unabhängiger Software zu überprüfen. Diese Eigenschaft – die sogenannte *Verifizierbarkeit* – wird heute von vielen Experten als Minimalanforderung für ein elektronisches Wahlsystem vorausgesetzt. Erreicht wird Verifizierbarkeit dadurch, dass sämtliche für eine Wahl relevanten Daten auf einem sogenannten *Bulletin Board* veröffentlicht werden. Die Schwierigkeit dabei ist, gleichzeitig das Stimmgeheimnis zu gewährleisten. Die Forschung hat verschiedene kryptographische Wahlprotokolle hervorgebracht, um genau dies zu erreichen. Allerdings setzen die meisten heute existierenden elektronischen Wahlsysteme diese Protokolle nicht oder nur ansatzweise um.

UniVote, Version 1, wurde im Februar 2013 fertiggestellt und in Betrieb genommen.[3] Kurz darauf wurden die StuRa-Wahlen der Universität Bern, der Berner Fachhochschule, und der Universität Zürich mit UniVote erfolgreich durchgeführt. Weitere StuRa-Wahlen an den Universitäten Luzern und Basel finden im Herbst 2013 statt. Den drei durchgeführten Wahlen liegt das schweizerische Proporzwahlrecht zugrunde, bei dem Partei- und Kandidatenstimmen erfasst werden. Obwohl die aktuelle UniVote-Implementierung noch keine vollständige Verifizierungskette bietet, existiert bereits eine unabhängige Software zur Verifizierung des Wahlergebnisses [SS13]. Die Lücken in der Verifizierungskette werden in der kommenden Version von UniVote geschlossen.

Dieses Dokument liefert eine einführende technische Beschreibung von UniVote (Abschnitt 2), sowie eine Zusammenstellung der wichtigsten Ergebnisse und Erkenntnisse aus der Durchführung der oben erwähnten StuRa-Wahlen (Abschnitt 3). Damit dokumentiert der Bericht die gesammelten Erfahrungen beim Entwickeln und Betreiben eines verifizierbaren Internet-Wahlsystems. Eine Zusammenstellung der unmittelbar bevorstehenden Ausbauarbeiten und ein Ausblick auf mögliche Weiterentwicklungen (Abschnitt 4) runden den Bericht ab.

2 UniVote

Dieser Abschnitt deckt die technische Beschreibung von UniVote ab. Es werden die Anforderungen an das kryptographische Wahlprotokoll erläutert sowie dessen Eigenschaften aufgelistet. Daraus leitet sich das Design der System-Architektur ab und es impliziert verschiedene Aspekte der konkreten Implementierung.

2.1 Sicherheitsanforderungen und Eigenschaften

Die Sicherheitsanforderungen an das Protokoll richten sich nach dem Standard demokratischer Wahlsysteme. Demnach muss das Protokoll das Wahlgeheimnis respektieren,

[2] Siehe Projekt-Webseite unter http://e-voting.bfh.ch/projects/univote.
[3] Siehe UniVote-Webseite unter http://www.univote.ch.

keine Resultate vor Wahlende erstellen können und garantieren, dass jeder Wahlberechtigte genau eine gültige Stimme abgeben kann. Zusätzlich soll das Protokoll End-to-End (E2E) verifizierbar sein, also die individuelle Verifizierbarkeit (*cast-as-intended* und *recorded-as-cast*), die universelle Verifizierbarkeit (*counted-as-recorded*), sowie die Verifizierung des Elektorats ermöglichen.

Zur Durchsetzung der Integrität der abgegebenen Stimme, sowie der Einhaltung des Wahlgeheimnisses, stützt sich UniVote auf das Vorhandensein einer sicheren Plattform seitens des Wählers ab. Es wird also angenommen, dass die Wähler Zugang zu einem Computer besitzen, der frei von Schadprogrammen ist, die gezielt die Stimmabgabe mit UniVote attackieren. Es ist klar, dass eine solche Annahme allgemein nicht gilt. Im Kontext der StuRa-Wahlen wird dies aber als akzeptables Restrisiko angesehen.

Grundsätzlich fügt sich UniVote in die Reihe der Systeme ein, die in einem akademischen Umfeld entwickelt wurde, um das Konzept der Verifizierbarkeit zu demonstrieren. Zu dieser Reihe gehört auch Helios [Adi08, AdPQ09]. Es gibt aber zwei wichtige Unterschiede, welche nachfolgend erläutert werden:

Anonyme Stimmabgabe Zusätzlich zur Wahrung des Stimmgeheimnisses ermöglicht UniVote eine anonyme Stimmabgabe. Das bedeutet, dass nicht nur der Inhalt einer Stimme sondern auch deren Urheber geheim bleibt. Dieses Verschleiern der Tatsache, dass jemand gestimmt hat, kann als Erweiterung des Stimmgeheimnisses angesehen werden. Das verwendete kryptographische Wahlprotokoll garantiert diese Eigenschaft, ohne auf die Verifizierbarkeit des Elektorats verzichten zu müssen [HS11].

Quittung Um die individuelle Verifizierung zu ermöglichen, liefert UniVote dem Wähler eine vom Bulletin Board signierte Quittung der abgegebenen Stimme zurück. Der Wähler kann damit verifizieren, ob die Stimme auf dem Bulletin Board korrekt veröffentlicht wurde und in die Endauszählung eingeflossen ist. Um zudem die Integrität der Stimme verifizieren zu können, beinhaltet die Quittung zusätzlich den Zufallswert, welcher zur Verschlüsselung der Stimme benutzt wurde. Der Zufallswert ermöglicht die Entschlüsselung und somit die Überprüfung der abgegebenen Stimme. Der Zufallswert selbst liegt in verschlüsselter Form vor.

Folgende Überlegungen motivieren die Rechtfertigung dieser starken Quittung: Da das umgesetzte Protokoll auf Wählerseite grundsätzlich auf einer unsicheren Plattform ausgeführt wird, kann das Wahlgeheimnis (und somit auch der Schutz des benutzten Zufallswerts für die Verschlüsselung der Stimme) per Definition nicht garantiert werden. Somit kann das umgesetzte Protokoll weder als erpressungsresistent gelten, noch kann es den Stimmenkauf verhindern. Die individuelle Herausgabe des verschlüsselten Zufallswertes, welcher zur Verschlüsselung der Stimme benutzt wurde, stellt demnach keine grundsätzliche Abschwächung des Protokolls dar, jedoch vereinfacht sie rein technisch den Beweis über die abgegebene Stimme. Auf diese Art kann die Integrität der abgegebenen Stimme vollständig und für den Wähler verständlich überprüft werden. Wichtig dabei ist, dass diese Überprüfung auf einem Gerät erfolgt, das verschieden und möglichst unabhängig vom benutzten Wahlcomputer ist. Diese Art der Überprüfung steht im Gegensatz zur Verifizierungsmöglichkeit anderer Systeme, bei denen der Wähler durch das wiederholte Testen

des Systems (*voter-initiated auditing*) eine Vertrauensbasis in die korrekte Stimmabgabe aufbaut [Ben07, KOKV11].

Zusammenfassend erlaubt UniVote also die anonyme Teilnahme an einer Wahl, was einer Attacke zur Nichtteilnahme an einer Wahl (*forced voter abstention*) entgegenwirkt. UniVote erzeugt zudem eine Quittung für die Verifizierung der Stimme sowie deren korrekter Übermittlung und Speicherung. Dies wirkt zwar einer Attacke auf die heimliche Veränderung der Stimme entgegen, aber es eröffnet auch die Möglichkeit der erzwungenen Stimmabgabe. Falls Eigenschaften der Erpressungsresistenz oder die Unterbindung des kommerziellen Handels mit Stimmen angestrebt werden, dann sollte UniVote in einem hybriden Wahlsystem zum Einsatz kommen, in welchem elektronische Stimmen durch Papierstimmen annulliert werden können [SH10].

2.2 Protokoll und Ablauf

Der Ablauf einer Wahl mit UniVote ist in vier Phasen aufgeteilt: Registrierung, Wahlvorbereitung, Stimmabgabe und Wahlabschluss. Diese vier Phasen werden nachfolgend kurz vorgestellt. Dabei werden Aspekte der konkreten Implementierung der entsprechenden Protokollvorlage entgegengestellt.

Phase 1: Registrierung Grundsätzlich ist UniVote darauf ausgerichtet, dass sich die Wähler vor Beginn der Wahlperiode registrieren und dadurch einen persönlichen Wahlschlüssel erhalten. Dies verunmöglicht jedoch die spontane Wahlteilnahme einer nichtregistrierten Person während der Wahlphase. Dieser Umstand wurde im Kontext der StuRa-Wahlen als nicht tragbar angesehen. Deshalb erlaubt UniVote auch sogenannte Spätregistrierungen, welche es dem Wähler ermöglichen, sich unmittelbar vor der Stimmabgabe zu registrieren. In einem solchen Fall kann aber die Anonymität der Stimmabgabe nicht mehr garantiert werden. Eine (vor oder während einer Wahl) erfolgte Registrierung gilt auch für zukünftige Wahlen. Für den Fall, dass ein bereits registrierter Wähler bei einer zukünftigen Wahl keinen Zugriff mehr auf seinen persönlichen Wahlschlüssel hat, kann er die Registrierung jederzeit wiederholen.

Protokoll Das Ziel der Registrierung gemäss Protokoll ist das Bereitstellen einer Public-Key-Infrastruktur (PKI) über das gesamte Elektorat [HS11]. Dazu muss ein einzelner Wähler seinen persönlichen *Wahlschlüssel* (ein Schlüsselpaar für Signaturen gemäss Schnorr[4]) erstellen und den öffentlichen Teil davon zertifizieren lassen. Für die Zertifizierung muss die Zertifizierungsstelle die Identität des Wählers eindeutig ermitteln können. Die Zertifikate werden allesamt in einem öffentlichen Verzeichnis bereitgestellt.

Umsetzung Die Zertifizierung der Wähler bei UniVote stützt sich auf SWITCHaai ab. Hier-

[4] Grundsätzlich ist jedes Signaturverfahren geeignet, das auf der Schwierigkeit des diskreten Logarithmus basiert. In der Originalpublikation des Protokolls wird DSA vorgeschlagen, dieses ist aber bezüglich Schlüssellänge weniger flexibel als das Verfahren von Schnorr.

bei handelt es sich um einen zentralen Authentifizierungs- und Autorisierungs-Dienst sämtlicher Schweizer Hochschulen. Die Qualität und Aktualität der vorhandenen Daten über die Studierenden bei SWITCHaai gilt als hoch. Da die Studierenden den Umgang mit SWITCHaai für andere Dienstleistungen gewohnt sind, stellt dies in Sachen Benutzbarkeit keine Hürde dar. Nach erfolgreicher SWITCHaai-Authentifizierung generiert der Wähler seinen Wahlschlüssel in der UniVote-Webapplikation (siehe Anhang A.1). Der öffentliche Teil des Wahlschlüssels wird von UniVote zertifiziert und veröffentlicht. Aufgrund der Einschränkungen der Browser-Technologie kann der Wähler den privaten Teil des Wahlschlüssels nicht direkt lokal abspeichern.[5] Dieser wird daher mittels eines vom Wähler eingegebenen Passwortes verschlüsselt, an UniVote übermittelt und von dort per E-Mail an den Wähler geschickt. Die E-Mail-Adresse des Wählers wird UniVote durch SWITCHaai bekannt gegeben.

Phase 2: Wahlvorbereitung Vor der eigentlichen Wahlphase müssen einige vorbereitende Schritte durchgeführt werden. Der wichtigste Schritt ist die Anonymisierung der Wahlschlüssel, damit die registrierten Wähler ihre Stimme anonym abgeben können. Der zweite wichtige Schritt ist der Erzeugen eines gemeinsamen Schlüssels für die Verschlüsselung der Stimmen. Zudem legt die *Wahladministration* die Kandidatenliste und das Elektorat fest.

Protokoll Gemäss Prokoll geschieht die Anonymisierung durch einen Generator-Wechsel im Schnorr-Signatursystem und durch das gleichzeitige Durcheinandermischen der öffentlichen Wahlschlüssel [HS11]. So können die transformierten Wahlschlüssel nicht mehr auf die ursprünglichen Schlüssel zurückgeführt werden. Dieser Schritt wird von verschiedenen unabhängigen *Mixern* mehrfach wiederholt, wobei jeder einzelne Mixer mit Hilfe kryptographischer Beweisverfahren die Korrektheit der durchgeführten Transformation beweisen muss. Die Erzeugung des Schlüssels für die Stimmabgabe erfolgt in einem verteilten Verfahren, bei dem eine bestimmte Anzahl sogenannter *Dechiffrierer* beteiligt sind. Diese teilen sich dann den privaten Teil des ElGamal-Schlüssels, so dass die Stimmen nur dann entschlüsselt werden können, wenn sich eine minimal Anzahl (Schwellwert) der Dechiffrierer daran beteiligt.

Umsetzung Bei der aktuellen Umsetzung der Wahlvorbereitung sind drei Mixer und drei Dechiffrierer beteiligt. Die Wahlschlüssel, die erst während der Wahl erzeugt werden, erfahren zwar die gleiche mathematische Transformation, können aber aufgrund der individuellen Behandlung nicht gemischt und somit nicht anonymisiert werden. Im Vergleich zum Protokoll gibt es zudem zwei wichtige Vereinfachungen (siehe Abschnitt 4). Einerseits erzeugen die Mixer zur Zeit keine kryptographischen Beweise, andererseits sind die Teile des gemeinsamen ElGamal-Schlüssels so konstruiert, dass sich bei der Entschlüsselung alle drei Dechiffrierer beteiligen müssen.

Phase 3: Stimmabgabe Die Stimmabgabe ist aus Sicht des Wählers der zentrale Schritt im Gesamtablauf. Diese erfolgt mit Hilfe der UniVote-Webapplikation, nachdem die ei-

[5] Das Erstellen und Herunterladen einer Datei im Browser mittels JavaScript findet erst mit HTML5 eine breite Unterstützung. Den privaten Wahlschlüssel mittels Copy-and-Paste in einer Textdatei abzuspeichern, wurde wegen mangelnder Benutzerfreundlichkeit nicht in Betracht gezogen.

gentliche Parteien- und Kandidatenauswahl in einer intuitiven Benutzeroberfläche erfasst wurden. Danach wird die abgegebene Stimme auf dem Bulletin Board publiziert.

Protokoll Damit die Parteien- und Kandidatenauswahl kryptographisch verarbeitet werden können, muss jede Stimme durch eine einzelne Zahl codiert werden. Die codierte Stimme wird anschliessend verschlüsselt (ElGamal) und mit dem anonymisierten Wahlschlüssel signiert. Nach Erhalt einer vollständigen Stimmabgabe wird mit Hilfe des anonymisierten öffentlichen Wahlschlüssels geprüft, ob der Wähler zum Elektorat gehört und ob dieser nicht bereits gewählt hat.[6] Ist diese Überprüfung erfolgreich, wird die signierte verschlüsselte Stimme auf dem Bulletin Board publiziert. Gemäss Protokoll muss die signierte verschlüsselte Stimme über einen anonymen Kanal ans Bulletin Board geschickt werden.

Umsetzung Bevor die UniVote-Webapplikation dem Wähler die möglichen Parteien und Kandidaten zur Wahl präsentiert, wird der Wähler aufgefordert, den verschlüsselten privaten Teil des Wahlschlüssels zusammen mit dem Passwort einzugeben (mittels Copy-and-Paste aus der erhaltenen E-Mail, siehe Anhang A.2). Nach erfolgreicher Entschlüsselung des privaten Wahlschlüssels, bietet die UniVote-Webapplikation dem Wähler die Möglichkeit, den Wahlzettel interaktiv zusammenzustellen und abzuschicken (siehe Anhang A.3). In Abweichung zum Protokoll muss für das Verschicken der Stimme kein anonymer Kanal verwendet werden (das Wahlgeheimnis ist durch das nachträgliche Mischen aller abgegebenen Stimmen dennoch garantiert).[7] Danach wird der Wähler über die Annahme oder die Ablehnung seiner Stimme informiert. Nachdem die Stimme angenommen und auf dem Bulletin Board publiziert wurde, wird die Quittung in Form eines QR-Codes angezeigt (siehe Abschnitt 2.1 und Anhang A.4).

Phase 4: Wahlabschluss In der letzten Phase geht es im Anschluss an die eigentliche Wahlperiode um die Ermittlung des Wahlresultates aufgrund der publizierten Stimmen auf dem Bulletin Board. Im Wesentlichen werden dazu die Stimmen entschlüsselt, decodiert und zusammengezählt, wobei ungültige Stimmen herausgefiltert werden. Sämtliche dieser Schritte werden auf dem Bulletin Board dokumentiert und können somit im Nachhinein verifiziert werden.

Protokoll Gemäss Protokoll wird für jede einzelne Stimme geprüft, ob der anonymisierte Wahlschlüssel zum Elektorat gehört, ob es zum gleichen Wahlschlüssel keine andere Stimme gibt und ob die Signatur und der kryptographische Beweis korrekt sind. Die gültigen Stimmen werden danach in einem Schwellwert-Verfahren entschlüsselt, bei dem die minimal geforderte Anzahl Dechiffrierer partizipiert. Die Korrektheit der Entschlüsselung wird mit kryptographischen Beweisen gezeigt. Anschliessend werden die entschlüsselten Stimmen decodiert und zusammengezählt. Bei der Auszählung werden Stimmen, die nicht den Wahlregeln entsprechen, aussortiert.

[6] Es wäre grundsätzlich möglich, eine bereits abgegebene Stimme mit einer neuen Stimme zu überschreiben, im vorgegebenen Kontext der StuRa-Wahlen ist dies aber nicht erwünscht.

[7] Dies hindert die Wähler jedoch nicht daran, dennoch einen anonymen Kanal (z.B. Tor) oder einen fremden Computer für die Stimmabgabe zu benutzen.

Umsetzung In der konkreten Umsetzung dieser Schritte wird vor dem Entschlüsseln der Stimmen ein zusätzlicher Schritt eingeschoben, in welchem die Stimmen kryptographisch gemischt werden. Dieser Schritt ist nötig, um auch das Wahlgeheimnis für die Wähler zu gewährleisten, die sich nicht vorab registriert haben und somit nicht anonym abstimmen konnten. Für das Mischen kommen die gleichen drei Mixer zum Einsatz, welche bereits die Stimmen anonymisiert haben. Auch hier liefert die aktuelle Implementierung noch keine kryptographischen Beweise (siehe Abschnitt 4).

2.3 Architektur und Technologien

Damit UniVote plattformunabhängig ist und für die Wähler ohne vorheriges Installieren von Programmen unmittelbar benutzt werden kann, wird auf Seite des Wählers eine Browser-basierte Lösung mit HTML und JavaScript eingesetzt. Serverseitig besteht UniVote aus verschiedenen Komponenten, die mittels Java EE-Technologien (EJB für die Logik, JPA für die Persistenz) realisiert und auf je einem GlassFish-Applikationsserver installiert wurden. Die Kommunikation zwischen diesen Komponenten einerseits und der Webapplikation andererseits erfolgt über SOAP-basierte Webservices. Die Spezifikation der entsprechenden Schnittstellen mit der plattformunabhängigen Sprache WSDL würde die Implementierung einzelner Komponenten auch auf anderen Technologie-Plattformen wie .NET erlauben.

Der Aufbau des UniVote-Systems ergibt sich aus dem Protokoll und beinhaltet eine Webapplikation und verschiedene Server-Komponenten.

Webapplikation Die UniVote-Webapplikation besteht aus einem Java-Servlet, einer HTML-Empfangsseite und zwei JavaScript-Anwendungen, eine für die Registrierung des Wählers und eine für die Stimmabgabe. JavaScript ermöglicht einerseits eine sehr intuitive Benutzerführung mittels Drag-and-Drop, andererseits wird es für die Berechnung der kryptografischen Operationen verwendet. Für die Registrierung muss sich ein Wähler zunächst über SWITCHaai authentisieren. Dies geschieht mit einem vorgeschalteten Apache-Webserver, auf dem das Shibboleth-Modul installiert wurde. Die Stimmabgabe erfolgt dann über die Webservices des Bulletin Boards. Zum Schluss wird mittels JavaScript die signierte Quittung in einen QR-Code umgewandelt, der dem Benutzer angezeigt wird.

Registrierung Die Registrierung wird vom Servlet der Webapplikation über eine interne EJB-Schnittstelle angesprochen. Sie stellt zudem einen Webservice zur Verfügung, über welchen der Koordinator (siehe unten) die Zertifikate der Wähler abfragen kann. Der Koordinator kann sich bei diesem Webservice auch registrieren, damit ihm neu erstellte Zertifikate automatisch zugestellt werden (*Publish-Subscribe*-Muster).

Bulletin Board Das Bulletin Board ist ein virtuelles Anschlagbrett für das Publizieren und Lesen aller systemrelevanten Daten. Diese können nicht gelöscht werden, ohne dass dies zu einem nachweisbar inkonsistenten Zustand des Bulletin Boards führen würde (*Append-*

Only).[8] Ein Webservice definiert alle Leseoperationen, mit denen die bisher publizierten Daten jederzeit ausgelesen werden können. In der aktuellen Version von UniVote kann nur der Koordinator direkt auf das Bulletin Board schreiben, d.h., die Daten der anderen Komponenten gelangen jeweils über den Koordinator auf das Board.

Koordinator Der Koordinator steuert den Ablauf einer Wahl. Sobald die Wahladministration ein Wahlereignis definiert hat, werden die drei Phasen Wahlvorbereitung, Stimmabgabe und Wahlabschluss automatisch durchgeführt. Die entsprechende Ablaufsteuerung erfolgt durch einen Zustandsautomaten, dessen Zustand persistiert wird, sodass ein Neustart jederzeit möglich ist. Zeitlich bedingte Ereignisse wie das Öffnen und Schliessen der Wahlurne werden mithilfe des EJB-Timerservices ausgelöst. Externe Verarbeitungen, welche lange dauern, werden durch asynchrone Aufrufe der entsprechenden Servicemethoden zeitlich entkoppelt. Der Koordinator ist auch verantwortlich für das Verteilen der Aufgaben an die Mixer und Dechiffrierer sowie das Einfordern der entsprechenden Ergebnisse mittels Polling.

Mixer Ein Mixer stellt einen Webservice zur Verfügung, über den er vom Koordinator signierte Aufgaben entgegennimmt. Die für den Generator-Wechsel benötigte geheime Zufallszahl ist verschlüsselt abgelegt. Beim Auslesen wird die Zufallszahl mit dem vorher eingegebenen Passwort entschlüsselt, sodass sich der entschlüsselte Wert immer nur im Hauptspeicher des Mixers befindet. Erfolgt ein Neustart eines Mixers, so muss das entsprechende Passwort erneut eingegeben werden.

Dechiffrierer Ähnlich wie beim Mixer stellt der Dechiffrierer einen Webservice zur Verfügung, über den er vom Koordinator signierte Aufgaben entgegennimmt. Der für die Entschlüsselung der Stimmen benötigte private Teil des ElGamal-Schlüssels ist ebenfalls verschlüsselt abgelegt, und die Freischaltung erfolgt analog wie beim Mixer.

2.4 Implementierung

In diesem Abschnitt werden zwei ausgewählte Aspekte der Implementierung kurz erläutert. Es handelt sich dabei um Aspekte, die bei ähnlichen Projekten zu analogen Fragestellungen führen werden. Die gemachten Erfahrungen und gefundenen Lösungen könnten deshalb auch ausserhalb von UniVote von Bedeutung sein.

JavaScript Die Implementierung der UniVote-Webapplikation mittels JavaScript brachte einige interessante Herausforderungen mit sich. Zwar hat sich JavaScript in den letzten Jahren sehr stark verbreit, doch ist der Anwendungsbereich oft auf das Benutzerinterface oder dessen Funktionalität beschränkt. So gibt es grosse Unterstützung für DOM-Manipulationen,

[8] In der aktuellen Version sind die für diese Eigenschaft notwendigen Mechanismen noch nicht vollständig umgesetzt.

Animationen, Formularvalidierungen oder auch die Serverkommunikation mittels AJAX. Für mathematische oder sogar kryptographische Aufgaben sind die Voraussetzungen in JavaScript aber eher ungünstig. Zum Beispiel bietet JavaScript keinen nativen Datentyp für grosse Zahlen an. Es gibt auch keine grossen und etablierten Bibliotheken für mathematische oder kryptographische Aufgaben.

Die geforderte Funktionalität des Benutzerinterfaces zu implementieren, stellte die kleinere Herausforderung dar. Die Steuerung des Ablaufs mit dem Ein- und Ausblenden einzelner Schritte oder auch die Drag-and-Drop-Funktionalität, welche beim Erstellen des komplexen Wahlzettels wertvolle Hilfe leisten, wurden mit Hilfe von etablierten Bibliotheken (jQuery und jQuery UI) implementiert. Ein Vorteil des Beizugs solcher Bibliotheken ist die Sicherheit, dass sie auf allen gängigen Benutzerplattformen erprobt und getestet sind.

Die grössere Herausforderung war die Implementierung der kryptographischen Komponenten. Die UniVote-Webapplikation muss fähig sein, Signaturen zu erstellen und zu überprüfen, einen privaten Wahlschlüssel zu generieren und diesen zu verschlüsseln, einen Wahlzettel zu codieren und zu verschlüsseln und nicht zuletzt entsprechende kryptographische Beweise zu erstellen. Da es keine Bibliothek gibt, die alle diese Funktionen nach den gegebenen Bedürfnissen anbietet, wurden sie aufbauend auf Leemons BigInt-Bibliothek individuell implementiert.[9] Gemein ist all diesen Funktionen, dass sie auf sehr rechenintensive Operationen (modulares Potenzieren) zurückgreifen. Dies muss bei Implementierungen in JavaScript mit nur einem einzigen Thread speziell berücksichtigt werden.[10] Einerseits ist die Ausführungszeit eines Scriptblocks in jedem Browser begrenzt, andererseits reagiert der Browser während dessen Ausführung nicht auf Benutzereingaben.[11] Dies erforderte zwingend eine asynchrone Implementierung der Kernfunktionen, ein Umstand, der Auswirkungen auf die gesamte JavaScript-Implementierung der UniVote-Webapplikation hatte.

UniCrypt Obwohl es verschiedene Bibliotheken für allgemeine kryptographische Aufgaben gibt (JCA, Bouncy Castle, Keyczar, Jasypt), konnte keine befriedigende Lösung gefunden werden, welche die Mathematik der Kryptographie für das E-Voting zufriedenstellend objektorientiert abbildet. Anfänglich wurde die Bibliothek Qilin[12] in Betracht gezogen, doch verschiedene Unzulänglichkeiten führten dazu, dass eine eigene Implementierung vorgezogen wurde. Das Ziel der Bibliothek *UniCrypt* besteht darin, die kryptographischen Anforderungen eines Wahlprotokolls möglichst präzis und vollständig objektorientiert abbilden zu können. Die erste Implementierung, welche verschiedene kryptographische Funktionen (Schnorr-Signaturen, ElGamal-Verschlüsselung, nicht-interaktive kryptographische Beweise, Mix-Netzwerke, usw.) basierend auf der Gruppentheorie anbietet, ist als mathematische Grundlage von UniVote im Einsatz und konnte anlässlich der StuRa-Wahlen bereits unter realen Bedingungen getestet werden.

[9] Siehe Projekt-Webseite unter http://leemon.com/crypto/BigInt.html.

[10] Die Zukunft von HTML5 mit Web Workers lässt diesbezüglich Hoffnung aufkommen, doch ist es noch zu früh, sich auf diese abzustützen, wenn ein breites Publikum erreicht werden soll.

[11] Die Problematik dieses Sachverhalts nimmt bei modernen Browsern auf modernen Rechnern ab, doch sind noch immer viele ältere Browser im Einsatz, insbesondere auf PCs mit dem Microsoft-Betriebssystem.

[12] Siehe Projekt-Webseite unter http://qilin.seas.harvard.edu.

3 Ergebnisse und Erfahrungen der StuRa-Wahlen

Die im Frühling 2013 durchgeführten StuRa-Wahlen an der Universität Bern, der Berner Fachhochschule und der Universität Zürich waren in vielerlei Hinsicht äusserst aufschlussreich. Es hat sich gezeigt, dass die praktische Durchführung einer echten Wahl eine Vielzahl kleiner Probleme hervorbringt, die im Vornherein nicht oder nur schwer vorhersehbar sind. Diese Probleme in nützlicher Zeit und zur Zufriedenheit aller Beteiligten zu lösen, war eine grosse Herausforderung. Einige dieser Probleme hätten vermutlich vermieden werden können, wenn es möglich gewesen wäre, im Vorfeld eine Testwahl mit einer heterogenen Test-Wählerschaft durchzuführen. Eine solche Testwahl war geplant, wurde aber aus Zeitgründen gestrichen.

Verzögerungen im Zeitplan waren generell die Ursache für viele der aufgetretenen Probleme. Zu Beginn des Projekts, zirka ein Jahr vor der ersten Wahl, wurde der erstellte Zeitplan von allen Beteiligten als realistisch beurteilt. Praktisch alle Phasen des Projekts – vom Erstellen der Protokoll-Spezifikation bis zur Inbetriebnahme des System – dauerten dann aber wesentlich länger als geplant. Insgesamt führte dies zu einer Verzögerung von bis zu zwei Monaten. Da im vorgegebenen akademischen Umfeld kurzfristig keine zusätzlichen Ressourcen bereitgestellt werden konnten, konnte das Projekt nur deshalb rechtzeitig und erfolgreich beendet werden, indem die beteiligten Personen gegen Ende des Projektes ihren Einsatz massiv erhöhten. Zudem wurde in Kauf genommen, dass das System nicht alle Elemente der Spezifikation von Beginn weg unterstützt. Und wie bereits erwähnt, wurden die vorgesehenen Tests auf ein Minimum reduziert. Retrospektiv betrachtet führte dies zu einem enormen Reputationsrisiko für alle beteiligten Personen und Organisationen. Glücklicherweise konnten aber grössere Pannen vermieden werden.

3.1 Elektorat und Wahlbeteiligung

Das Elektorat bestand in allen drei Fällen aus mehreren Tausend Studierenden (Tabelle 1, Zeile 1). Im Fall der Universität Zürich entspricht dies in etwa dem Gesamtelektorat eines kleineren Schweizer Kantons oder eines Kleinstaates wie Liechtenstein. Die Wahlbeteiligung bei allen drei StuRa-Wahlen war relativ gering (Tabelle 1, Zeile 2), so dass die Verarbeitung und Auszählung dieser Stimmen von der bereitgestellten Server-Infrastruktur problemlos und in kürzester Zeit zu bewältigen war.

Wie in Abschnitt 2 erklärt, ist eine Vorab-Registrierung Voraussetzung für eine anonyme Stimmabgabe. Die Studierenden wurden im Vorfeld der Wahlen per E-Mail darauf aufmerksam gemacht. Im Fall der Universität Bern haben aber nur zirka 2% der Studierenden bzw. 20% der Wähler von dieser Möglichkeit Gebrauch gemacht (Tabelle 1, Zeile 3).[13] Es scheint, als ob die Bedeutung der StuRa-Wahl für die meisten Studierenden zu gering ist, um einem durch wenige Worte ausgedrückten Sicherheitsargument genügend Beachtung zu schenken und entsprechend zu handeln.

[13] Durch einen organisatorischen Fehler wurde die Aufforderung zur Vorab-Registrierung an der Universität Zürich nicht rechtzeitig verschickt. Entsprechend klein sind die Prozentzahlen in Tabelle 1 (Zeile 3).

	Universität Bern			*Berner FH*			*Universität Zürich*		
Elektorat	11249	100%		5720	100%		25833	100%	
Anzahl Stimmzettel	1008	9.0%	100%	269	4.7%	100%	3138	12.1%	100%
Vorab registriert	211	1.9%	20.9%	126	2.2%	46.8%	45	0.2%	1.4%
Feedback	101	0.9%	10.0%	25	0.4%	9.3%	184	0.7%	5.9%

Tabelle 1: Die Kennzahlen der drei durchgeführten StuRa-Wahlen bezüglich Elektorat, Stimmbeteiligung, Registrierung und Wähler-Befragung.

3.2 Befragung der Wählerschaft

Nach erfolgreicher Stimmabgabe wurden die Studierenden aufgefordert, an einer Befragung teilzunehmen. Ungefähr 10% der Wähler haben von dieser Möglichkeit der Rückmeldung Gebrauch gemacht (Tabelle 1, Zeile 5). Es gab Fragen zu drei unterschiedlichen Kategorien: Fragen zu UniVote, Fragen zur Sicherheit und allgemeine Fragen zu E-Voting. Nachfolgend werden die Resultate dieser Befragung kurz zusammengefasst und interpretiert.

Fragen zur Benutzung von UniVote Es wurden insgesamt vier allgemeine Fragen zur Benutzung und Verständlichkeit von UniVote gestellt (Tabelle 2). Zudem konnten allfällige Problem beschrieben und mögliche Verbesserungen mitgeteilt werden. Bei allen vier Fragen sind zirka 75% der Antworten positiv oder sehr positiv. Wenn man berücksichtigt, dass bei solchen Befragungen tendenziell eher die Leute mit Problemen oder Kritik Rückmeldungen verfassen, ist dies ein sehr gutes Resultat. Dieses Resultat überrascht vor allem auch deshalb, weil aus Zeitgründen sowohl das Design der Webapplikation wie auch die zur Verfügung gestellten Informationen eher minimalistisch gehalten wurden. Die zirka 15% der Personen mit kleineren oder grösseren Problemen sind auf die technischen und organisatorischen Mängel zurückzuführen, die im nachfolgenden Abschnitt beschrieben werden. Ein anderes Problem war, dass einige den verschlüsselten Wahlschlüssel nicht korrekt aus der E-Mail herauskopierten. Einige Personen bemängelten generell, dass der Registrierungsprozess zu kompliziert sei, und würden deshalb bei StuRa-Wahlen Abstriche beim Stimmgeheimnis oder der Anonymität in Kauf nehmen.

Fragen zur Sicherheit von UniVote Weiter wurden fünf Fragen zur Sicherheit von UniVote gestellt (Tabelle 3). Obwohl nur sehr wenig Information zu den einzelnen Elementen des Sicherheitskonzepts bereitgestellt wurde, haben über 80% der Personen eine hohes oder sehr hohes Vertrauen, dass UniVote zum korrekten Wahlresultat führt und dass das Wahlgeheimnis und die Anonymität ausreichend geschützt sind. Die Werte bei der Frage nach den bereitgestellten Informationen zur Sicherheit sind ein wenig schlechter, was aber nicht überrascht. Dieses insgesamt sehr gute Ergebnis ist auch darauf zurückzuführen, dass das Vertrauen in Abstimmungen und Wahlen in der Schweiz allgemein sehr hoch ist. Interessant ist noch das Resultat der letzten Frage, wonach fast die Hälfte der Personen eine Internet-Wahl mit UniVote als sicherer einstufen als klassische Wahlen auf Papier.

Allgemeine Fragen zu Internet-Wahlen Abschliessend wurden drei Fragen zum Gesamteindruck und allgemein zur Zukunft von Internet-Wahlen gestellt (Tabelle 4). Das Resultat bezüglich Gesamteindruck widerspiegelt die spezifischen Resultate zu UniVote und zur Sicherheit. Etwa 80% ziehen ein positives bis sehr positives Fazit und empfehlen, StuRa-Wahlen auch in Zukunft mit UniVote durchzuführen. Interessant ist auch zu sehen, dass mehr als die Hälfte der Personen es begrüssen würde, Internet-Wahlen flächendeckend, also auch für politische Wahlen, einzuführen. Dazu ist anzumerken, dass es bei den bestehenden Schweizer Internet-Systemen bisher keine grösseren Pannen gab und deshalb der Diskurs über die Sicherheit von solchen System in der Öffentlichkeit kaum geführt wurde.

3.3 Herausforderungen im produktiven Betrieb

Im Sinne, dass alle beteiligten Personen das ermittelte Wahlresultat akzeptiert haben, konnten alle drei Wahlen erfolgreich abgeschlossen werden. Es zeigte sich aber, dass manche Hürden und daraus resultierende Herausforderungen erst kurz vor oder sogar erst nach der Inbetriebnahme des Systems auftauchen können. Im Folgenden werden einzelne Aspekte beschrieben, welche in der Theorie einfach erscheinen, sich in der Praxis aber als überraschend schwierig und facettenreich herausstellten.

Probleme bei der Wählerliste Ursprünglich war die eindeutige Immatrikulationsnummer als Identifikator der Wähler in UniVote vorgesehen. Diese Nummern wurden im Testsystem durch SWITCHaai korrekt zur Verfügung gestellt. Entsprechend musste die kurz vor Wahlbeginn eingespeiste Gesamtliste des Elektorats aus genau diesen Nummern bestehen. Erst bei der Inbetriebnahme des produktiven Systems wurde jedoch ersichtlich, dass die Immatrikulationsnummern aus Datenschutzgründen nicht automatisch zur Verfügung gestellt werden. Deshalb wurde kurzfristig die studentische E-Mail-Adresse als Identifikator eingeführt, jedoch unter der ungeprüften Annahme, dass diese in den jeweiligen Universitäten eindeutig ist. An der Universität Bern und der Berner Fachhochschule war dies der Fall, jedoch nicht an der Universität Zürich, wo die Studierenden bis zu 4 oder 5 Adressen besitzen. Dort musste wiederum sehr kurz vor Wahlbeginn ein neuer Identifikator (eine interne Nummer) eingeführt werden.

Weiter stellte sich die Qualität der Wählerliste als mangelhaft heraus. Es gab zum Beispiel doppelte oder fehlende Einträge oder uneinheitliche Einträge bezüglich Gross- und Kleinschreibung. Da es klar war, dass jede kleine Abweichung in diesen Listen bei den betroffenen Wählern die Stimmabgabe beeinträchtigen kann, musste jeweils eine manuelle Prüfung durchgeführt werden. Dieser delikate Prozess wurde durch den Umstand erschwert, dass die jeweiligen Wählerlisten von den Universitätsverwaltungen erst wenige Tage vor Wahlbeginn zur Verfügung gestellt wurden. Eine zusätzliche Hürde stellte der Umstand dar, dass aus Datenschutzgründen ausschliesslich mit den Hash-Werten der jeweiligen Identifikatoren gearbeitet wurde.

Um diese Probleme zu beheben, mussten oft unter Druck Entscheidungen getroffen und absolut korrekt umgesetzt werden. In einigen wenigen Fällen gelang dies nicht perfekt, wes-

halb betroffene Personen entweder an der Stimmabgabe gehindert wurden[14] oder mehr als eine Stimme abgeben konnten. Mehrfachstimmen werden aber in der Wahlabschlussphase automatisch herausgefiltert (siehe Abschnitt 2.2).

Probleme bei der Stimmabgabe Auch wenn die UniVote-Webapplikation ausgiebig unter vielen verschiedenen Konfigurationen getestet wurde, konnten nicht alle möglichen Fälle im Voraus erkannt und abgedeckt werden. So wurden zum Beispiel einzelne Wähler an der Stimmabgabe gehindert, wenn diese ihren Wahlschlüssel per Copy-and-Paste aus Microsoft Outlook in den Browser übertrugen. Das Problem war, dass der Wahlschlüssel dabei mit versteckten Zeichen kompromittiert wurde. Hier schaffte nur eine Modifizierung der UniVote-Implementierung im laufenden Betrieb Abhilfe.

Ein weiterer unvorhergesehener Fall trat kurz vor dem Ende einer Wahlperiode auf. Eine Wählerin wurde an der Stimmabgabe gehindert, weil die kryptographischen Berechnungen im Browser länger dauerten, als es die maximale Ausführungszeit des Browsers erlaubte. Dies geschah, weil der benutzte Computer zu schwach war. Dieses Problem wäre zwar technisch lösbar, jedoch mit unvertretbarem Aufwand verbunden gewesen. So wurde diese Person gebeten, die Stimme auf einem anderen Computer abzugeben.

Probleme mit der Infrastruktur Obwohl in der Theorie stets Redundanz der Systeme gefordert wird, war das Vertrauen in die verfügbare Infrastruktur (Server und Netzwerk der Berner Fachhochschule) zu gross. Dies führte am Vorabend der Urnenschliessung an der Universität Bern zu einem schwerwiegenden Zwischenfall. Das gesamte Netzwerk der Berner Fachhochschule, in welchem die UniVote-Server untergebracht sind, erlitt um ca. 22 Uhr einen Totalausfall wegen eines Fehler in einer zentralen Komponente. Der Ausfall dauerte bis ca. 9 Uhr am folgenden Morgen, ungefähr 3 Stunden vor der geplanten Urnenschliessung um 12 Uhr. Weil üblicherweise viele Stimmen erst kurz vor Schluss abgegeben werden, ist anzunehmen, dass dieser Zwischenfall einige Personen an der Stimmabgabe gehindert hat. Die Zahl der betroffenen Personen ist aber nicht zu eruieren.

4 Ausblick und Fazit

Aufgrund der beschränkten Ressourcen und dem knappen Zeitplan konnten einige UniVote-Komponenten nicht vollständig realisiert werden. Dadurch entstanden Abweichungen zur Systemspezifikation und entsprechende Lücken in der Verifizierungskette. Diese gilt es so schnell wie möglich zu schliessen. Nachfolgend werden die wichtigsten kurz erläutert.

Verifizierbares Mix-Netzwerk Die fehlenden kryptographischen Beweise der beteiligten Mixer stellen zur Zeit die grösste Lücke in der Verifizierungskette dar. Die Wahlschlüssel und die Stimmen werden zwar kryptographisch gemischt, doch weil die

[14] An der Universität Bern gab es zwei solche Fälle. Die betroffenen Personen konnten ihre Stimme auf Papier abgeben. Deshalb unterscheiden sich das offizielle und das von UniVote ermittelte Wahlresultat leicht.

Korrektheit dieser Schritte zur Zeit nicht bewiesen wird, könnten die Mixer theoretisch das Wahlergebnis beliebig manipulieren. Auf diese Beweise wurde bis anhin verzichtet, weil sie kryptographisch relativ komplex sind und in der vorgegeben Zeit nicht umgesetzt werden konnten [Wik09, TW10, Gro10].

Unabhängige Verifizierungssoftware Eine Verifizierungssoftware erfüllt nur dann ihren Zweck, wenn sie von einer oder mehreren unabhängigen Stellen her erzeugt wird. Deshalb stellt UniVote selber keine Verifizierungssoftware zur Verfügung. Stattdessen wird zur Zeit eine erste Bachelorarbeit ausgearbeitet, die möglichst frei (d.h. ohne Einsicht in den Code von UniVote und ohne der Hilfe von UniCrypt) eine Referenzimplementation einer Verifizierungssoftware für UniVot darstellt.

Schwellwert-Entschlüsselung oder Schlüssel-Wiederherstellung In UniVote wird das Schlüsselpaar für die Verschlüsselung der Stimmen durch die Dechiffrierer verteilt erstellt. Dadurch wird sichergestellt, dass niemand alleine die Stimmen entschlüsseln kann. Zur Zeit braucht es für die Entschlüsselung alle Dechiffrierer, was die Gefahr birgt, dass beim Ausfall eines einzelnen Dechiffrierers oder beim Verlust eines einzelnen Teilschlüssels alle Stimmen unwiderruflich verloren sind. Dieses Risiko wird entweder mit einer echten Schwellwert-Entschlüsselung oder mit einer verteilten Schlüssel-Wiederherstellung abgewehrt.

Zu den grössten offenen Problemen im Umfeld von Internet-Wahlen gehört die unsichere Plattform seitens der Wähler. Bei StuRa-Wahlen wird dieser Aspekt nicht als sehr schwerwiegend betrachtet, aber eine umfassendere Lösung dafür wäre trotzdem sehr wünschenswert. Es ist beabsichtigt, weiter daran zu arbeiten und existierende Konzepte umzusetzen [DHK12].

Aktuell besteht zwischen UniVote und dessen Bulletin Board eine sehr starke Kopplung. Es ist jedoch wünschenswert, das Bulletin Board möglichst zu entkoppeln und dessen Funktionalität soweit zu erhöhen, dass es die Eigenschaften eines robusten Bulletin Boards abdecken kann [HL08].

Zudem soll in Zukunft UniVote einer breiteren Öffentlichkeit zugänglich gemacht werden, also auch für Wahlen ausserhalb von Hochschulen. Dazu wäre die Einbindung weiterer Authentifizierungsdiensten wie zum Beispiel Facebook oder Google+ nützlich. Dabei müsste für das Definieren von neuen Wahlen und Abstimmungen ein einfach zu bedienendes Benutzerinterface bereit gestellt werden.

Fazit Diese Arbeit zeigt, dass das Konzept eines verifizierbaren Internet-Wahlsystems im Rahmen einer angewandten Forschung praktisch umgesetzt werden kann. Die Realisierung ist trotz des sehr knappen Zeitplans und der beschränkten Ressourcen gelungen. Von grosser Bedeutung war, dass die beteiligten Personen sich in Bezug ihre Kompetenzen gegenseitig ideal ergänzen (Kryptographie, Software-Engineering, Programmierung, Technologien, Benutzerschnittstellen, Projekt-Management). Wichtig war die ausgiebige Diskussion aller zentralen Aspekte zu Beginn des Projekt, in welcher eine gemeinsame Marschrichtung definiert wurde. Daraus ist eine detaillierte Systemspezifikation entstanden, die als Grundlage und Leitfaden für die anschliessende Realisierung von zentraler Bedeutung war.

Danksagung

Dieser Bericht zu UniVote wurde im Rahmen eines Forschungsprojektes realisiert, das vom *Schweizerischen Nationalfonds* (SNF) gefördert wird (Projekt-Nr. 200021L_140650). Besonderen Dank geht auch an die Studierendenverbände der am Projekt beteiligten Hochschulen für die grosszügige Unterstützung und das entgegengebrachte Vertrauen.

Literatur

[Adi08] B. Adida. Helios: Web-Based Open-Audit Voting. In P. Van Oorschot, Hrsg., *SS'08, 17th USENIX Security Symposium*, Seiten 335–348, San Jose, USA, 2008.

[AdPQ09] B. Adida, O. de Marneffe, O. Pereira und J. J. Quisquater. Electing a University President using Open-Audit Voting: Analysis of Real-World Use of Helios. In D. Jefferson, J. L. Hall und T. Moran, Hrsg., *EVT/WOTE'09, Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, Montreal, Canada, 2009.

[Ben07] J. Benaloh. Ballot Casting Assurance Via Voter-Initiated Poll Station Auditing. In *EVT'07, USENIX/ACCURATE Electronic Voting Technology Workshop*, Boston, USA, 2007.

[DHK12] E. Dubuis, R. Haenni und R. E. Koenig. Konzept und Implikationen eines verifizierbaren Vote Électronique Systems. Studie im Aufrag der Schweizerischen Bundeskanzlei, April 2012.

[Gro10] J. Groth. A Verifiable Secret Shuffle of Homomorphic Encryptions. *Journal of Cryptology*, 23(4):546–579, 2010.

[HL08] J. Heather und D. Lundin. The Append-Only Web Bulletin Board. In P. Degano, J. Guttman und F. Martinelli, Hrsg., *FAST'08, 5th International Workshop on Formal Aspects in Security and Trust*, LNCS 5491, Seiten 242–256, Malaga, Spain, 2008.

[HS11] R. Haenni und O. Spycher. Secure Internet Voting on Limited Devices with Anonymized DSA Public Keys. In H. Shacham und V. Teague, Hrsg., *EVT/WOTE'11, Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, San Francisco, USA, 2011.

[KOKV11] F. Karayumak, M. M. Olembo, M. Kauer und M. Volkamer. Usability Analysis of Helios – An Open Source Verifiable Remote Electronic Voting System. In H. Shacham und V. Teague, Hrsg., *EVT/WOTE'11, Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, San Francisco, USA, 2011.

[SH10] O. Spycher und 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.

[SS13] G. Scalzi und J. Springer. VoteVerifier: Independent Vote Verifier for UniVote Elections. Bachelor thesis, Bern University of Applied Sciences, Biel, Switzerland, 2013.

[TW10] B. Terelius und D. Wikström. Proofs of Restricted Shuffles. In D. J. Bernstein und T. Lange, Hrsg., *AFRICACRYPT'10, 3rd International Conference on Cryptology in Africa*, LNCS 6055, Seiten 100–113, Stellenbosch, South Africa, 2010.

[Wik09] D. Wikström. A Commitment-Consistent Proof of a Shuffle. In C. Boyd und J. González Nieto, Hrsg., *ACISP'09, 14th Australasian Conference on Information Security and Privacy*, LNCS 5594, Seiten 407–421, Brisbane, Australia, 2009.

A Screenshots der UniVote-Webapplikation

A.1 Registrierung

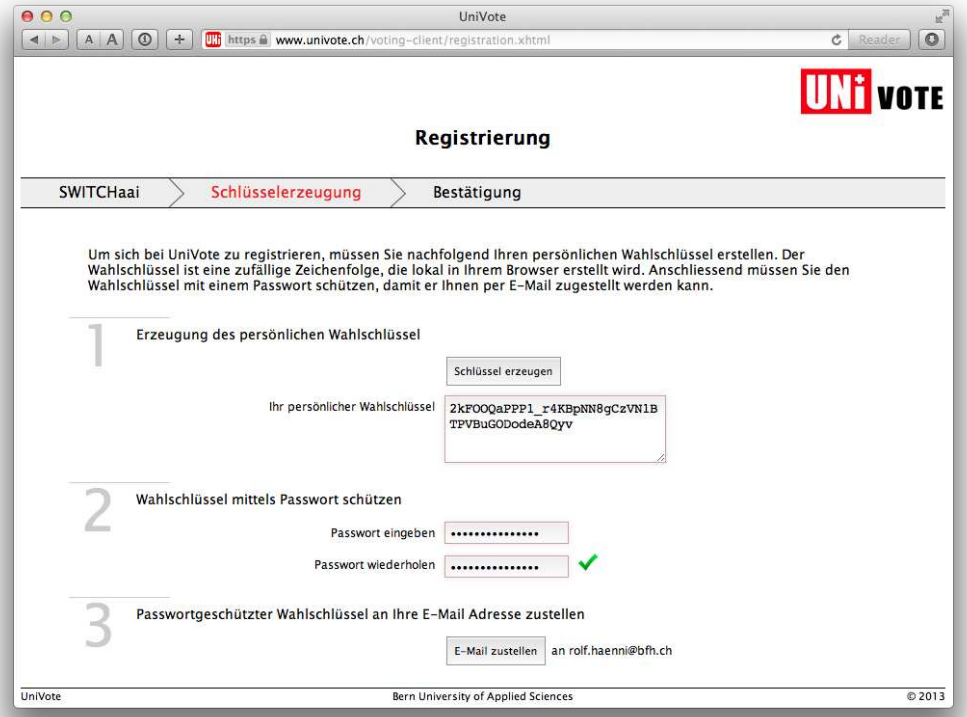


Abbildung 1: Screenshots der UniVote-Webapplikation: Registrierung.

A.2 Eingabe des privaten Wahlschlüssels

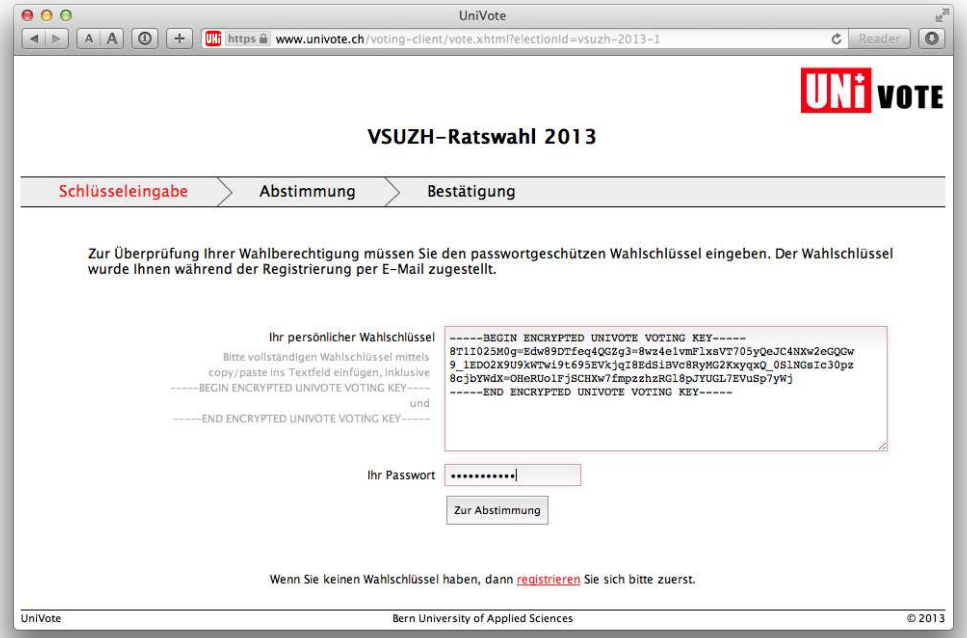


Abbildung 2: Screenshots der UniVote-Webapplikation: Eingabe des privaten Wahlschlüssels.

A.3 Erfassen des Stimmzettels

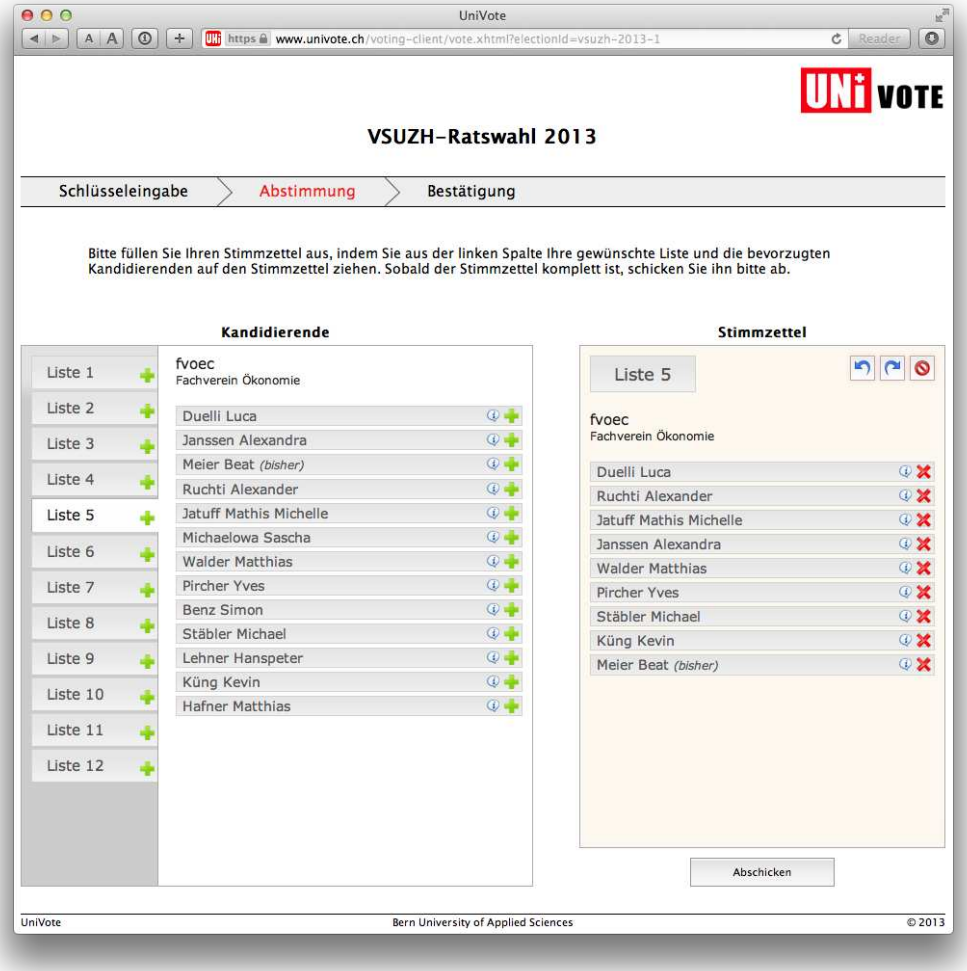


Abbildung 3: Screenshots der UniVote-Webapplikation: Erfassen des Stimmzettels.

A.4 Anzeige der Quittung

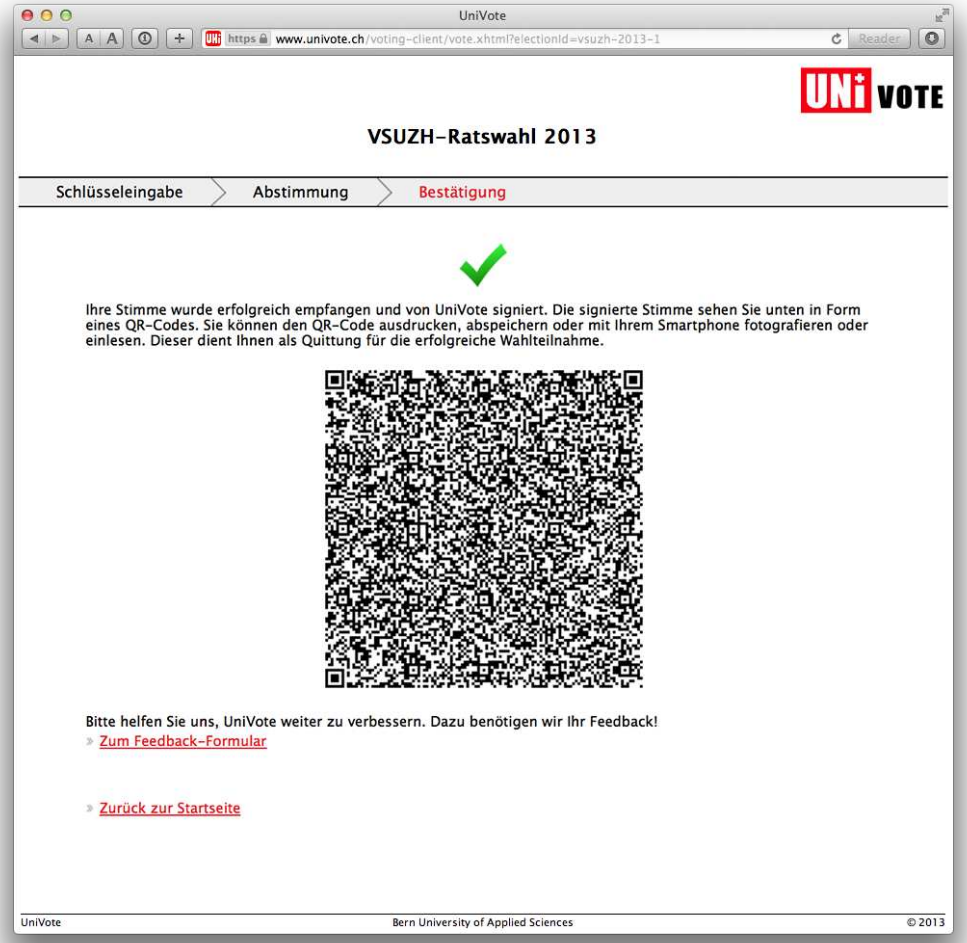


Abbildung 4: Screenshots der UniVote-Webapplikation: Anzeige der Quittung.

B Resultate der Wählerschaftsbefragung

B.1 Fragen zur Benutzung von UniVote

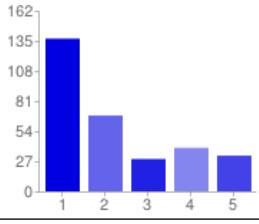
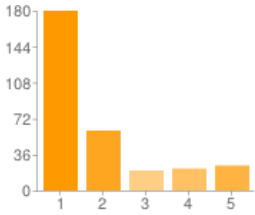
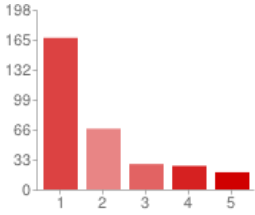
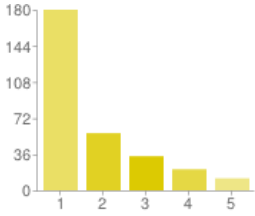
Die Abstimmungsprozedur mit UniVote ist:	einfach	1	137	45%	
		2	68	22%	
		3	29	10%	
		4	39	13%	
	kompliziert	5	32	10%	
Die Registrierung und die Stimmabgabe verliefen:	ohne Probleme	1	180	59%	
		2	60	20%	
		3	20	7%	
		4	22	7%	
	mit Problemen	5	25	8%	
Die Bedienung des Systems ist:	einfach	1	167	54%	
		2	67	22%	
		3	28	9%	
		4	26	8%	
	kompliziert	5	19	6%	
Die bereitgestellten Information und Erklärungen zur Benutzung des Systems sind:	ausreichend	1	180	59%	
		2	57	19%	
		3	34	11%	
		4	21	7%	
	ungenügend	5	12	4%	

Tabelle 2: Resultate der Wählerbefragung: Fragen zur Benutzung von UniVote.

B.2 Fragen zur Sicherheit von UniVote

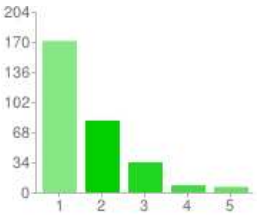
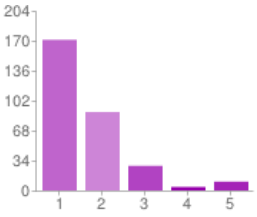
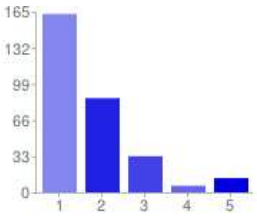
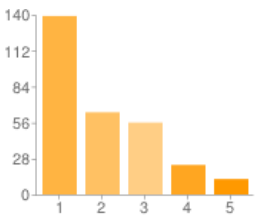
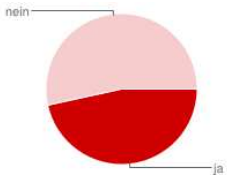
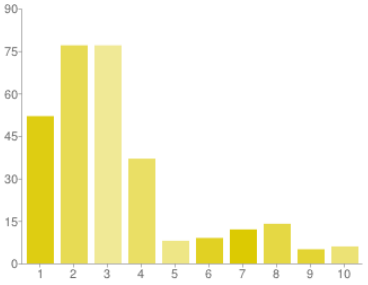
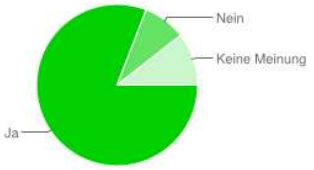
Mein Vertrauen, dass der Einsatz von UniVote zu einem korrekten Wahlresultat führt, ist:	hoch	1	171	57%	
		2	81	27%	
		3	34	11%	
		4	8	3%	
	klein	5	6	2%	
Mein Vertrauen, dass UniVote mein Stimmgeheimnis ausreichend schützt, ist:	hoch	1	171	57%	
		2	89	29%	
		3	28	9%	
		4	4	1%	
	klein	5	10	3%	
Mein Vertrauen, dass UniVote eine anonyme Stimmabgabe ermöglicht, ist:	hoch	1	163	54%	
		2	86	29%	
		3	33	11%	
		4	6	2%	
	klein	5	13	4%	
Die bereitgestellten Information und Erklärungen zur Sicherheit von UniVote sind:	ausreichend	1	139	47%	
		2	64	22%	
		3	56	19%	
		4	23	8%	
	ungenügend	5	12	4%	
Sind Wahlen mit UniVote sicherer als klassische Wahlen auf Papier?	ja		129	47%	
	nein		148	53%	

Tabelle 3: Resultate der Wählerbefragung: Fragen zur Sicherheit von UniVote.

B.3 Allgemeine Fragen zu Internet-Wahlen

Mein Gesamteindruck zu UniVote ist:	sehr gut	1	52	18%
		2	77	26%
		3	77	26%
		4	37	12%
		5	8	3%
		6	9	3%
		7	12	4%
		8	14	5%
		9	5	2%
	schlecht	10	6	2%
Möchten Sie zukünftige Hochschul-Wahlen erneut mit UniVote durchführen?	ja		245	81%
	nein		26	9%
	weiss nicht		32	11%
Sollen Internet-Wahlen in der Schweiz flächendeckend eingeführt werden?	ja		180	59%
	nein		81	27%
	weiss nicht		42	14%





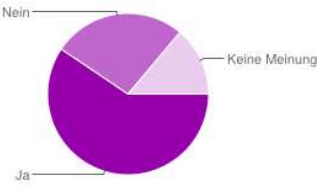


Tabelle 4: Resultate der Wählerbefragung: Allgemeine Fragen zu Internet-Wahlen.