# Elektronische Wahlen mit bedingungslosem Wahlgeheimnis

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Dr. Rolf Haenni, Prof. Dr. Philipp Locher
Experte: Dr. Federico Flueckiger (Eidg. Finanzdepartement)



**Das Bedürfnis nach elektronischen Wahlen besteht schon seit längerem. Oft werden elektronische Wahlen auch als Lösung für die Mobilisierung der jüngeren Wählerschaft genannt. Trotz den veränderten Bedürfnissen müssen demokratische Eckpfeiler wie das Wahlgeheimnis oder die Sicherstellung der Wahlberechtigung gewährleistet sein. An diesem Punkt setzt unsere Bachelor-Thesis an, welche einen Proof of Concept eines Wahlsystems mit bedingungslosem Wahlgeheimnis zum Ziel hat.**

## Ausgangslage

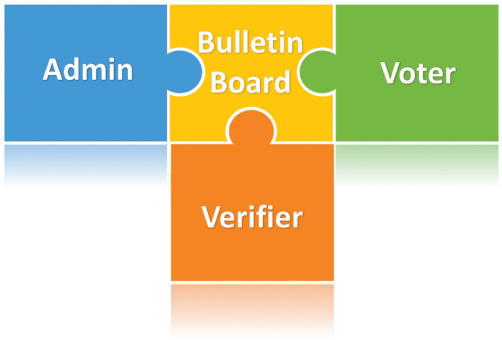
Bei den aktuellen Implementierungen von elektronischen Wahlsystemen werden vertrauenswürdige Drittparteien (trusted parties) benötigt. Diese verwalten beispielsweise die geheimen Schlüssel einer Wahl und haben somit Einsicht in die Wahldaten. Im Gegensatz zur heutigen Papierwahl werden die Stimmen nicht von unabhängigen Wahlhelfern ausgezählt, sondern von einer Software. Da der Programmcode und das Infrastruktur-Design nicht öffentlich einsehbar sind, muss den Entwicklern und Betreibern ein hohes Vertrauen entgegengebracht werden. Zusätzlich werden in den heutigen Wahlsystemen Verschlüsselungstechniken genutzt, welche auf heute nicht lösbaren Problemen beruhen. Es kann daher nicht sichergestellt werden, dass die Wahldaten auch in Zukunft sicher sind. Haenni und Locher haben in ihrer wissenschaftlichen Arbeit «Verifiable Internet Elections with Everlasting Privacy and Minimal Trust» beschrieben, wie die Vertrauensannahmen in die Drittparteien vermindert werden können und gleichzeitig ein bedingungsloses Wahlgeheimnis sichergestellt werden kann.

## Ziele

Im Rahmen unserer Arbeit haben wir einen Proof of Concept des Protokolls von Haenni und Locher implementiert. Neben der schwächeren Vertrauensannahme bietet das Protokoll ein Stimmgeheimnis, welches auch in Zukunft nicht gebrochen werden kann.
Das Ziel dieser Arbeit war die Entwicklung eines Grundsystems, welches die verschiedenen Komponenten zur Durchführung einer elektronischen Wahl umfasst.
Der Projektfokus lag von Anfang an bei der korrekten Implementierung des Protokolls sowie der kryptographischen Funktionen und weniger bei der Abdeckung der verschiedenen Wahltypen und der Gestaltung der Benutzeroberfläche.

## Umsetzung

Wir haben das Protokoll mit Hilfe der BFH-eigenen Unicrypt-Bibliothek realisiert und in vier Komponenten aufgeteilt. Als zentrale Komponente dient das Bulletin Board, eine Art digitales öffentliches Anschlagbrett, welches Informationen für alle beteiligten Parteien annimmt und zur Verfügung stellt. Die Wahladministration definiert mit Hilfe der Admin App die Wahlen und legt fest, wer stimmberechtigt ist. Des Weiteren gibt es eine Voter App, mit welcher der Wähler sich registrieren und an berechtigten Wahlen teilnehmen kann. Schliesslich haben wir eine Verifier App implementiert, welche das Stimmmaterial verifiziert und das Resultat publiziert.




Komponenten abcVote

Damit die Wahlerstellung, die Wählerregistrierung und die Publikation des Resultates gegen Manipulationen geschützt sind, werden die Nachrichten digital signiert und durch einen verschlüsselten Kanal gesendet. Zur erweiterten Sicherstellung der Wähleranonymität wurde die Möglichkeit implementiert, Stimmen über das Anonymisierungsnetzwerk Tor abzugeben.

## Fazit

Unser Proof of Concept erlaubt es Wahlen zu erstellen, durchzuführen und auszuzählen. Zusätzlich wird die Möglichkeit geboten Stimmen anonym via Tor-Netzwerk zu verschicken. Somit konnte gezeigt werden, dass der produktive Betrieb einer Infrastruktur mit bedingungslosem Wahlgeheimnis möglich ist.
Allerdings wurden aufgrund des zeitlichen Rahmens einige Aspekte weggelassen, welche für eine produktive Version adressiert werden müssen.

Timo Bürk

Sebastian Nellen
sebastian@nellen.it