Bachelorthesis-Aufgabe

Elektronische Wahlen mit bedingungslosem Wahlgeheimnis

ID	IHNR1-1-17
Studierende	Timo Bürk Sebastian Nellen
Betreuer	Prof. Dr. Rolf Haenni Prof. Philipp Locher
Experten	Dr. Federico Flueckiger
Aufgabe	Bei elektronischen Wahlen ist das Garantieren des Stimmgeheimnisses ein wesentlich schwierigeres Problem als bei klassischen Wahlen mit Papierstimmen. Es ist mittels kryptographischen Methoden zwar möglich, das Mischen der Stimmzettel elektronisch nachzubilden, die Sicherheit dabei ist aber immer nur so stark wie die verwendeten kryptographischen Verfahren und Parameter. Obwohl diese heute als sicher gelten, kann man davon auszugehen, dass in Zukunft, zum Beispiel in 30, 50 oder 100 Jahren, diese nicht mehr genügen. Somit besteht ein Risiko, dass das Stimmgeheimnis nachträglich noch gebrochen werden kann. In der Literatur der kryptographischen Wahlprotokolle gibt es verschiedene Vorschläge für Systeme, in denen das Wahlgeheimnis bedingungslos geschützt werden kann, d.h. unabhängig des technischen Fortschritts und von neuen wissenschaftlichen Erkenntnissen. In diesem Projekt geht es darum, eines dieser Systeme zu analysieren und in Form eines Prototypen zu implementieren.