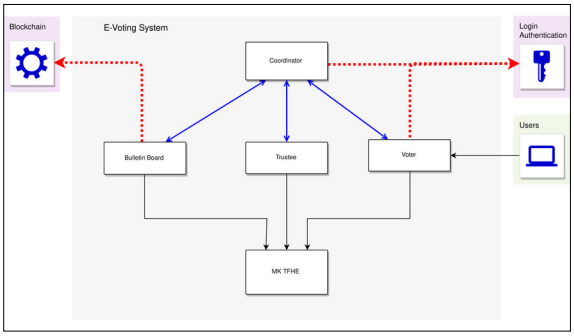

Rolf
Furrer


Romeo
Spinas

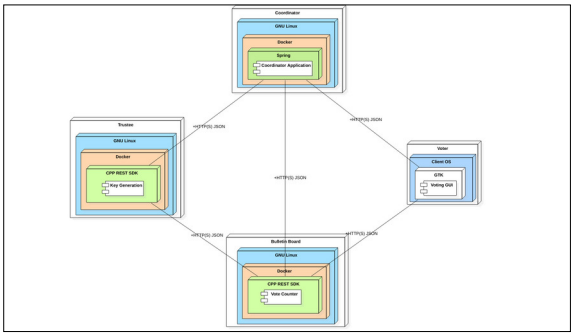

Lukas
Lätsch

Diplomanden	Rolf Furrer, Romeo Spinas, Lukas Lätsch
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich, ZH
Themengebiet	Sicherheit

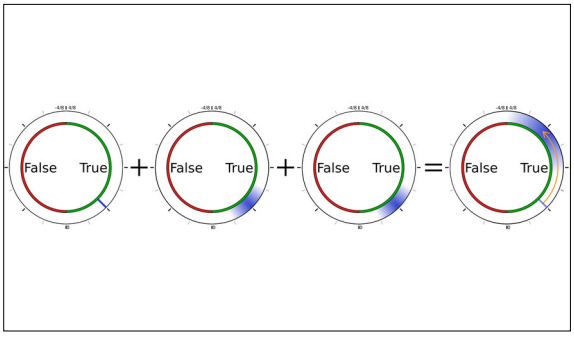
Post-Quantum E-Voting



Umsysteme
Eigene Darstellung



Architekturdiagramm
Eigene Darstellung



OR-Gate mit homomorpher Verschlüsselung
Eigene Darstellung

Ziel der Arbeit: Die meisten Länder wenden gegenwärtig ein papierbasiertes Wahlsystem an. Der Kostenaufwand solcher Systeme ist relativ gross. Es gibt immer mehr Länder, die an einem E-Voting-System arbeiten. Die Kernpunkte eines E-Voting-Systems sind die Verifiability, Privacy und Transparency bestmöglich zu gewährleisten. Es soll ein zukunftssicheres E-Voting-System erstellt werden. Die folgenden Punkte heben das E-Voting-System besonders heraus:

• Der Verschlüsselungsalgorithmus soll gegenüber Quantum-Computern resistent sein, somit wird der Algorithmus immer noch sicher sein, nachdem Quanten-Computer genügend leistungsfähig sind.
• Die Stimmen können verschlüsselt aufsummiert werden, dadurch kennt der Stimmenzähler das Ergebnis und die Identität des Wählers nicht.
• Eine einzelne Partei sollte die Daten nicht alleine entschlüsseln können.

Das entwickelte E-Voting-System soll für Abstimmungen eingesetzt werden, wie zum Beispiel an Generalversammlungen oder auch an nationalen Abstimmungen. Es gibt eine Library, die die oben genannten Punkte und Kernpunkte erfüllt, basierend auf diesen wird in dieser Bachelorarbeit ein E-Voting-System entwickelt. Bei der Arbeit wird zudem auf den architektonischen Aufbau der Software geachtet, welcher für die Sicherstellung des Vertrauens in das Wahlsystem entscheidend ist.

Ergebnis: Die Einarbeitung in die Verschlüsselungstheorie und den Aufbau der Library wurde in der Studienarbeit erarbeitet und darauf aufbauend ist in der Bachelorarbeit das Wissen vertieft worden. Aufbauend auf der Library ist erfolgreich ein E-Voting-System entwickelt worden, welches alle zentralen und die meisten optionalen Anforderungen abdeckt. Das E-Voting-System benötigt mindestens die drei eigenständigen Applikationen Coordinator, Bulletin Board und Trustee sowie einen Voter um abzustimmen. Die Komponenten sind mit mehreren JSON-Schnittstellen untereinander verbunden. Die Rechenoperationen auf dem Bulletin Board sind aufwendig, deswegen wurde von Beginn der Entwicklung an ein Augenmerk auf die Parallelisierung der Operationen gelegt.

Fazit: Der Grundaufbau des E-Voting-Systems ermöglicht es, eine Abstimmung durchzuführen, jedoch ist das System noch nicht in einer realen Abstimmung einsetzbar. Die verschiedenen Teilapplikationen können sich untereinander noch nicht eindeutig identifizieren. Die Wahlberechtigung der Wähler zu prüfen, wird durch das E-Voting-System noch nicht unterstützt. Die abstimmungsbezogenen Daten können in der Zukunft anstatt in einer Datenbank in einer Blockchain abgespeichert werden. Es sind schon einige Optimierungen zur Beschleunigung des E-Voting-Systems unternommen worden, es könnte aber zusätzlich die Verteilung des Bulletin Boards auf mehrere Rechner implementiert werden.