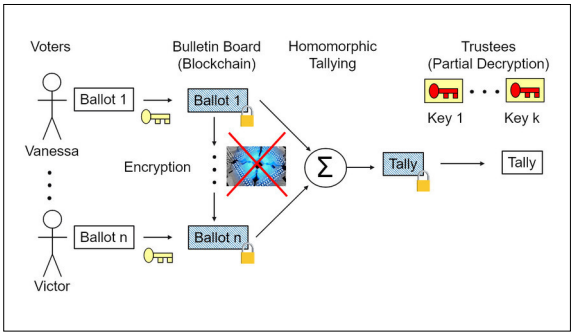

Rolf
Furrer


Romeo
Spinas

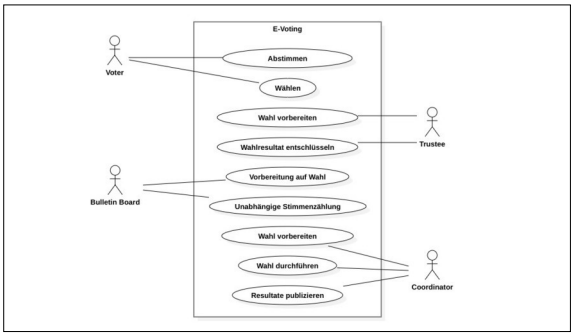

Lukas
Lätsch

Studenten	Rolf Furrer, Romeo Spinas, Lukas Lätsch
Examinator	Prof. Dr. Andreas Steffen
Themengebiet	Software

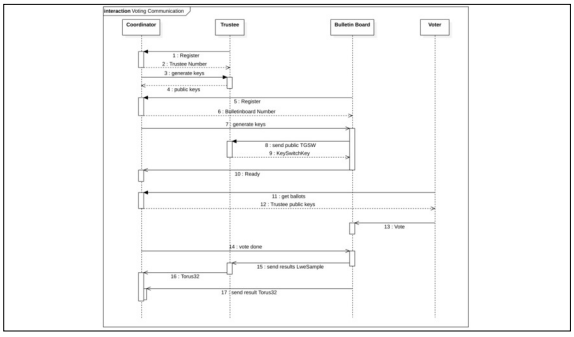
Post-Quantum E-Voting



Post-Quantum E-Voting
Aufgabenstellung, Prof. Dr. Andreas Steffen



Usecases
Eigene Darstellung



Abstimmungsverlauf
Eigene Darstellung

Einleitung: Die Studienarbeit basiert auf der Doktorarbeit von Ilaria Chillotti\cite{phdManuscript} zum Thema 'Fast Fully Homomorphic Encryption Library over the Torus'(TFHE). Dabei handelt es sich um eine Verschlüsselung, die es erlaubt, auf verschlüsselten Daten logische Operationen auszuführen. Der Nachteil ist jedoch, dass mehr Performance nötig ist um die Berechnungen durchzuführen. Die Arbeit von Ilaria Chillotti und ihrer Forschungskollegen haben die Geschwindigkeit der Verschlüsselung verbessert. Dadurch ist es möglich diese Verschlüsselungsart ohne immensen Zeitaufwand einzusetzen. Bei E-Voting Systemen mit konventionellen Verschlüsselungen werden die Stimmen vor dem Zusammenzählen entschlüsselt. Die homomorphe Verschlüsselung ermöglicht es die verschlüsselten Stimmen zu zählen und somit das Wahlgeheimnis zu bewahren.
Ein weiteres Schwäche einiger Verschlüsselung ist das Entwicklungsstand der Quantencomputer. Schätzungsweise wird intern 10 Jahren ein Grossteil der heutigen Verschlüsselungen unsicher, das ist bei TFHE nicht der Fall.

Vorgehen: Im Rahmen der Arbeit mussten wir auf der Basis der TFHE Library in C++ einen einfachen Prototypen einer Post-Quantum E-Voting Anwendung erstellen. Der Prototyp muss Ja/Nein Abstimmung und der Wahl eines Vertreters aus mehreren Kandidaten unterstützen. Zusätzlich muss auch eine Stimmenthaltung ermöglicht werden.Zur Verhinderung von Wahlbetrug mussten zudem die Schlüssel auf unabhängige Parteien verteilt werden können. Eine zusätzliche optionale Anforderung ist der Einsatz mehrerer Stimmenzähler, um eine weitere Betrugsmöglichkeit eliminieren zu können.
Im Arbeitsumfang ist die Verifikation der Wähler durch die Verwendung von Public Key Signaturen, sowie die Sicherstellung der Nachvollziehbarkeit durch den Einsatz einer Blockchain nicht enthalten.

Fazit: Das wichtigste Ergebnis unserer Arbeit ist die Implementation eines E-Voting Prototypen. Zu diesem Zweck haben wir in ersten Phase die bestehende Library überarbeitet. Dies beinhaltet den Einsatz von Objektorientierung sowie das anheben des Standards auf C++17. Zudem haben wir den Funktionsumfang der Library erweitert. Beispielsweise braucht es für das E-Voting eine Funktion zum Zusammenzählen der Stimmen. Des Weiteren haben wir bei der Überarbeitung sicherheitstechnische Aspekte beachtet.
In einer zweiten Phase haben wir einen Prototypen mit vier Teilapplikationen erstellt. Es handelt sich dabei um den Coordinator, Trustee, das Bulletin Board und den Voter. Eine Abstimmungsdurchführung kann vereinfacht mit einem Coordinator, Trustee, Bulletin Board und einem bis mehreren Voter durchgeführt werden.
Die Überarbeitung der Library und die Modularisierung des Prototypen hat dazu geführt, dass der neue erstellte Code deutlich lesbarer geworden ist, zusätzlich ist die Anwendung übersichtlicher und kürzer geworden.
Nach Performance Tests haben wir eine geringfügige Differenz der Ausführungszeit festgestellt. Das liegt vorwiegend an der Objektorientierung und der Löschung der sensiblen Daten.