Advisor	Sophia Yakoubov
Students	Emil Mors & Mikkel Katholm
Languages	English
Text tools	LaTeX, Typst
Other tools	Git, Python, VS Code

Project Description

This project investigates privacy-preserving electronic voting with a focus on ranked-choice methods. The aim is to define and analyze a clear security framework for ranked-choice voting (RCV) by extending existing ideal functionalities from plurality voting to RCV. The project will review prior work on electronic voting and existing security definitions. Furthermore, we will propose an ideal functionality for privacy-preserving ranked-choice tallying and design a protocol that achieves this functionality using standard cryptographic primitives. We will implement and evaluate a prototype. If time permits, we will also explore how this work can be extended as a component within the UC framework. The deliverables include a formal specification of the functionality, a protocol with security arguments, a prototype implementation, and a final report.

Provisional Table of Contents

- Abstract (10–20 lines)
- Section 1: Introduction (1–2 pages)
- Section 2: Literature Review (4–6 pages)
  Existing work on electronic voting, ranked-choice tallying, and security definitions.
- Section 3: Security Framework (4–6 pages)
  Review of existing security notions and extension of ideal functionalities to ranked-choice voting.
- Section 4: Protocol Design (4–8 pages)
  Proposed protocol for privacy-preserving ranked-choice voting.
- Section 5: Prototype and Evaluation (4–6 pages)
  Implementation details, performance measurements, and analysis.
- Section 6: Discussion and Extensions (2–4 pages)
  Relation to prior work, potential UC integration, and future directions.
- Section 7: Conclusion (1–2 pages)
- Acknowledgements (3–5 lines)
- References ($\frac{1}{2}$–4 pages)
- Appendix with code, tables, and detailed proofs (5–20 pages)

Provisional Time Plan

First week of September (15 hours)
Planning activities, refining research questions, and scheduling.

Rest of September and first half of October (3×15 hours)
Literature review and drafting Sections 2–3.

Rest of October and first week of November ($2 \times 15 + 2 \times 30$ hours)
Completion of Sections 2–3 and draft of Section 4 (protocol design).

Rest of November (3×30 hours)
Refinement of Section 4 and draft of Section 5 (prototype and evaluation).

First three weeks of December (3×30 hours)
Completion of Sections 4–5 and draft of Section 6 (discussion and extensions).

Last week of December (30 hours)
Write missing parts, merge drafts, ensure consistency, and proofread.