Secure Voting

- Insecure Boting

Member

109550005	張可晴
109550025	謝翔丞
109550027	紀竺均
109550031	李旻融
109550118	孫宜君

Introduction

Purpose

- Convenience
- fast and accurate calculation of result
- reduce of manipulation

Implementation

Homomorphic Encryption

- private data protection
- A + B = C -> C(A)+C(B)=C(C)

Block Chain

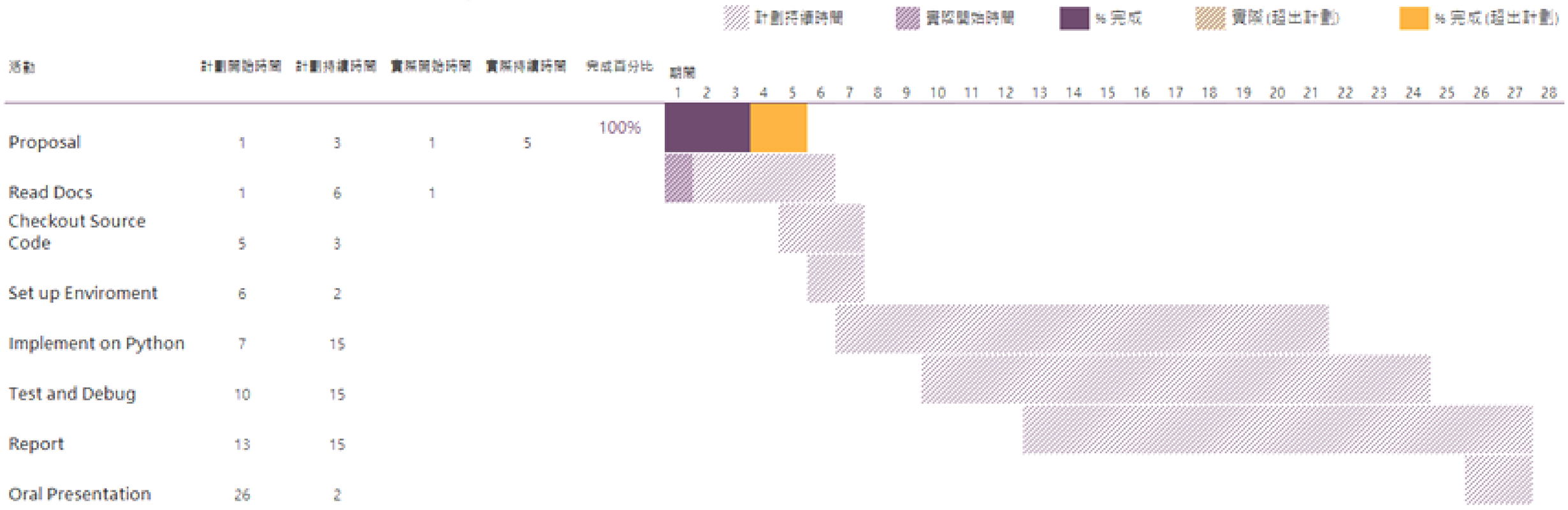
- public accessment
- can't be tampered

Election Guard

- open source software development kit
- homomorphic encryption
- end-to-end verification of elections

Work Plan

密碼工程 Final Proposal



Reference

https://github.com/microsoft/electionguard