SMPC for Decentralized Distributed Systems

Frederic Klein – Proposal Talk

Institute of Medical Informatics
Uniklinik RWTH Aachen

UNIKLINIK RWTH AACHEN

mhealth

The Hygiene Games

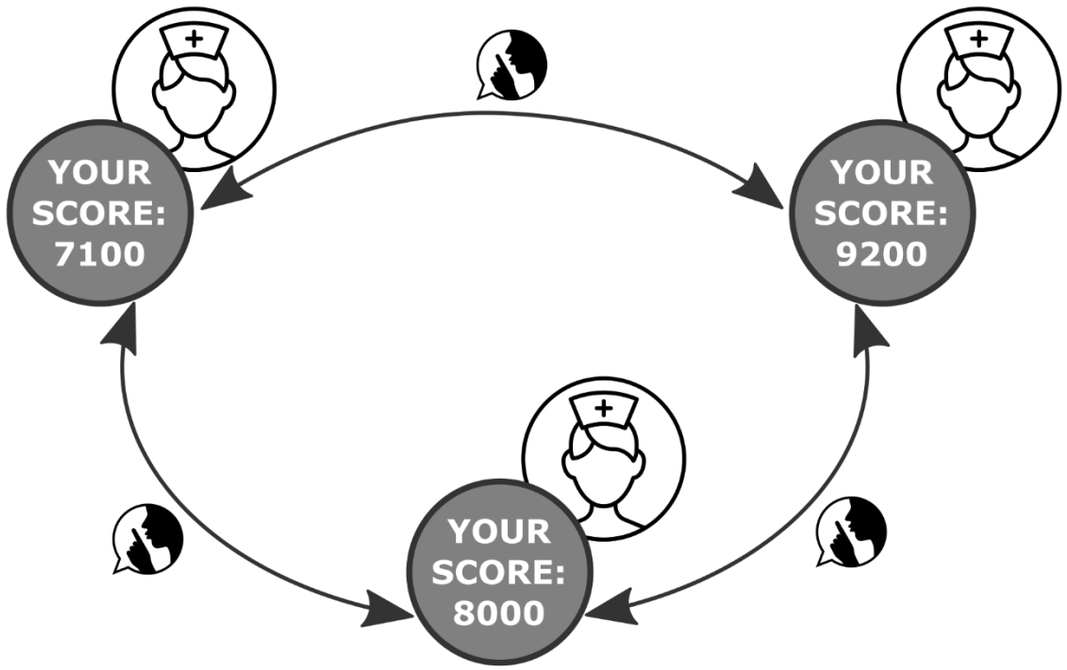
- Gamification for hand hygiene
- Requirements
  - Privacy protection
  - Computation of system statistics
  - Bluetooth mesh network

Privacy Protection

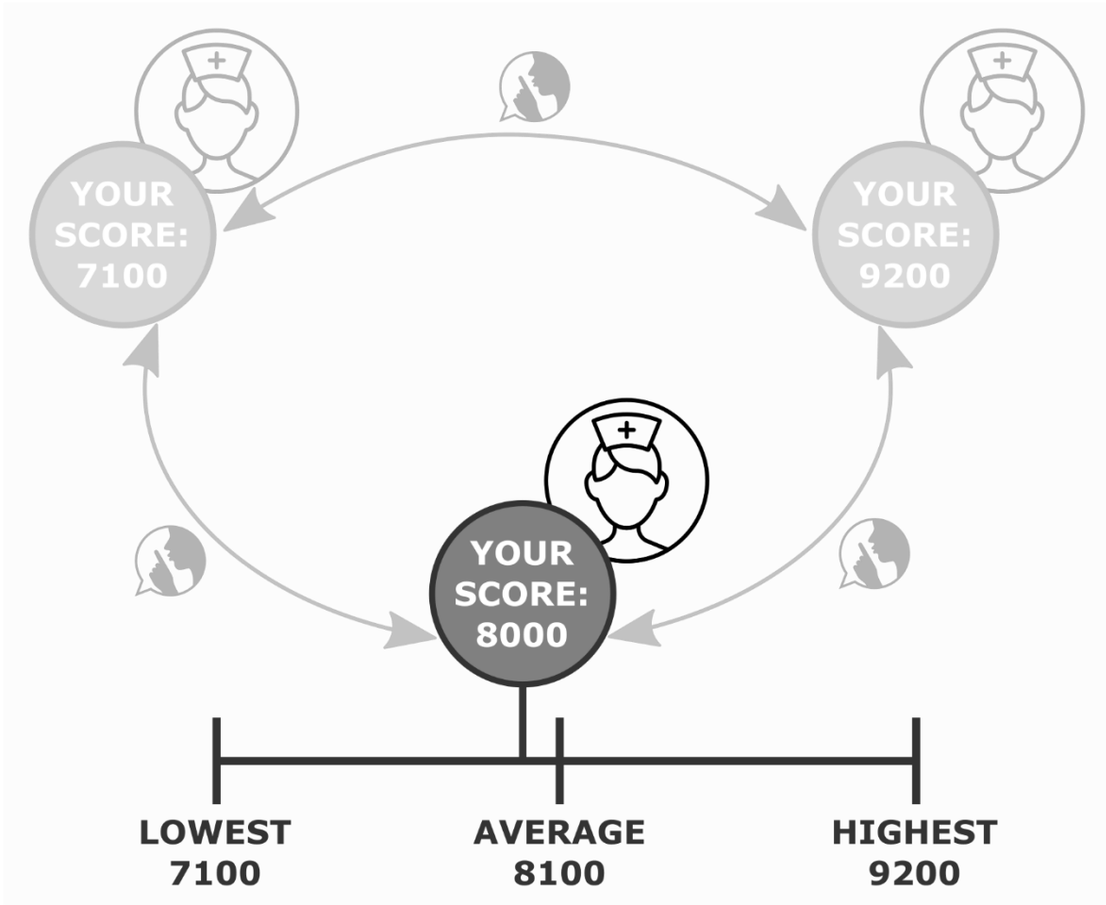
- Personal data on own device
- Modest value without comparison

Privacy Protection

- Exchange data for comparison



Privacy Protection



SMPC

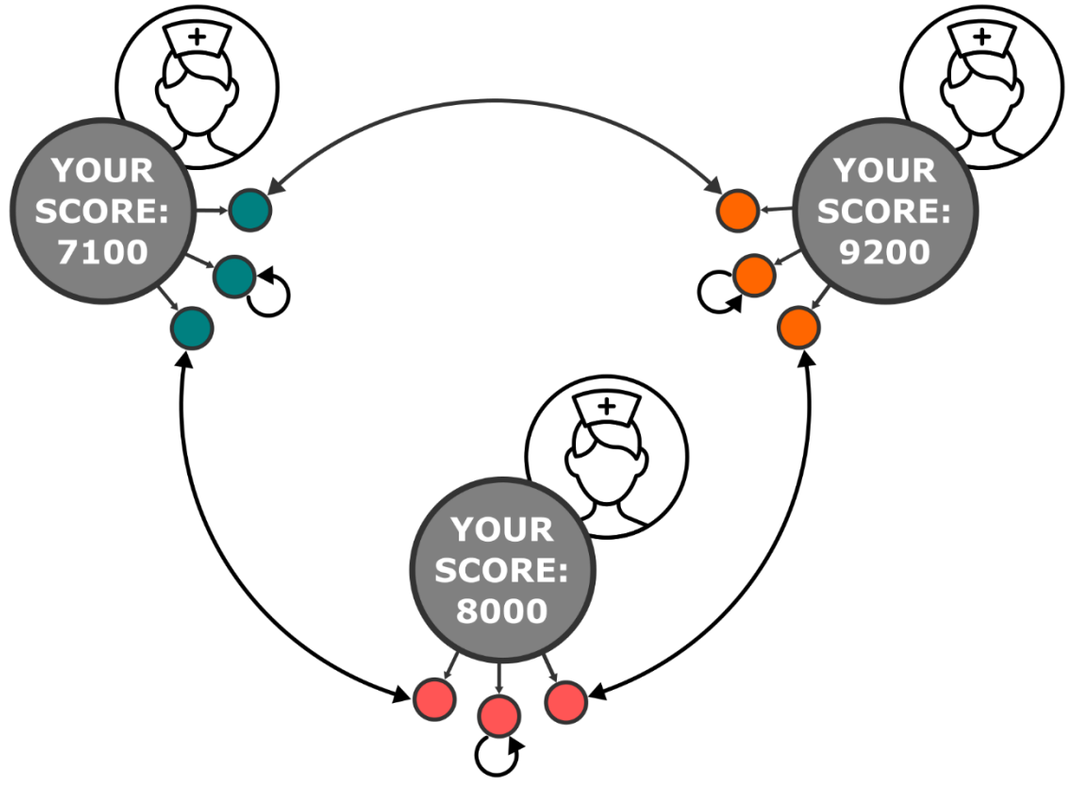
- Subfield of cryptography:
  - compute function over inputs of multiple parties
  - keep the inputs private

SMPC

- Three parties
- Score as input

SMPC

- Secret sharing: n shares for n parties

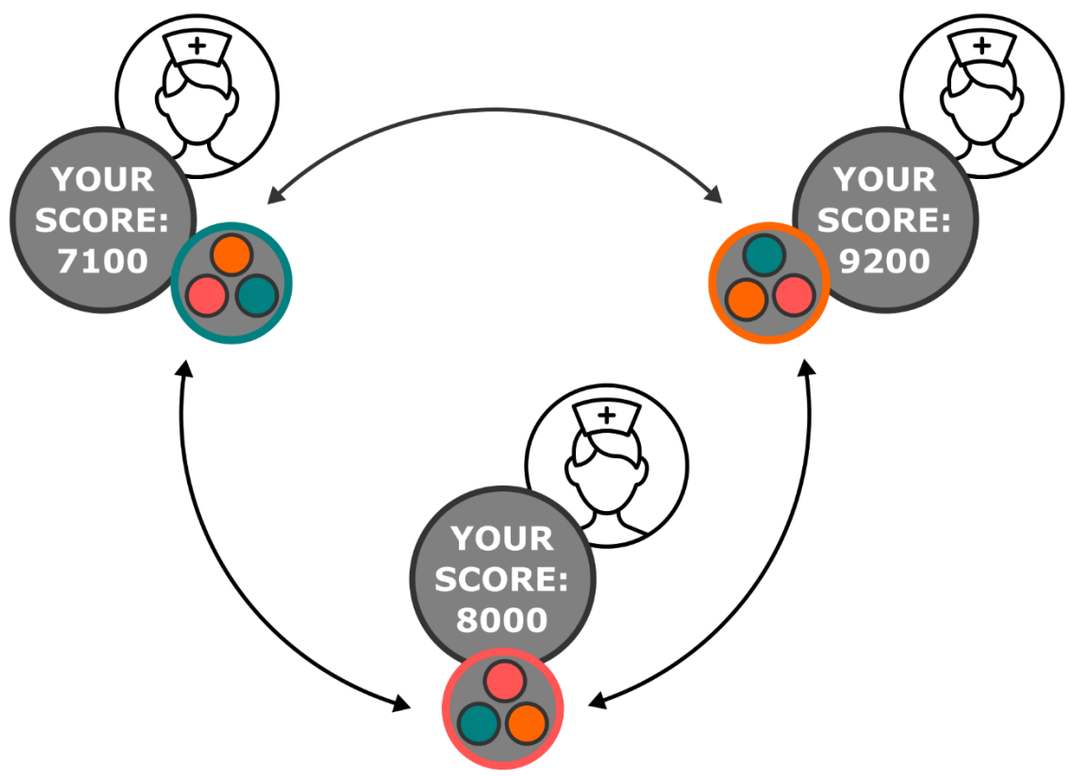


SMPC

- Each player: set of n shares

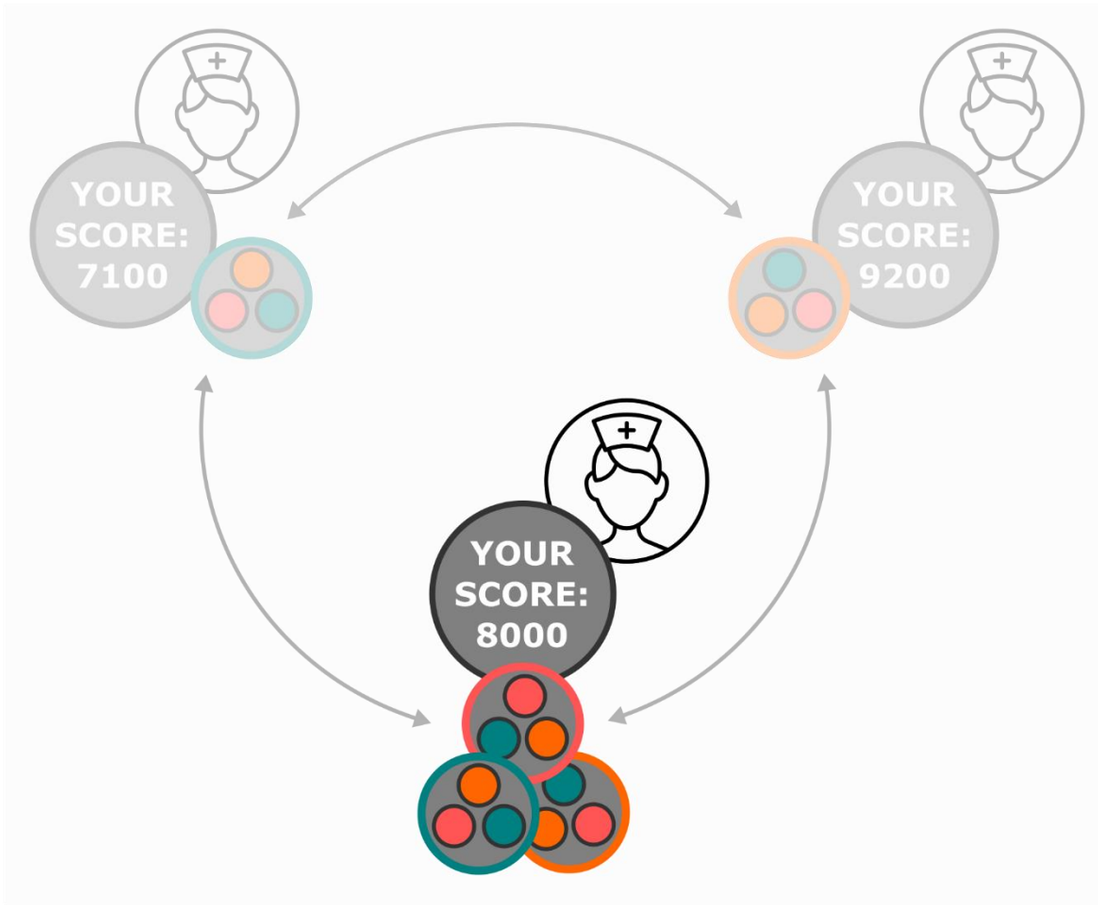
SMPC

- Computation on shares
- Broadcasting of result

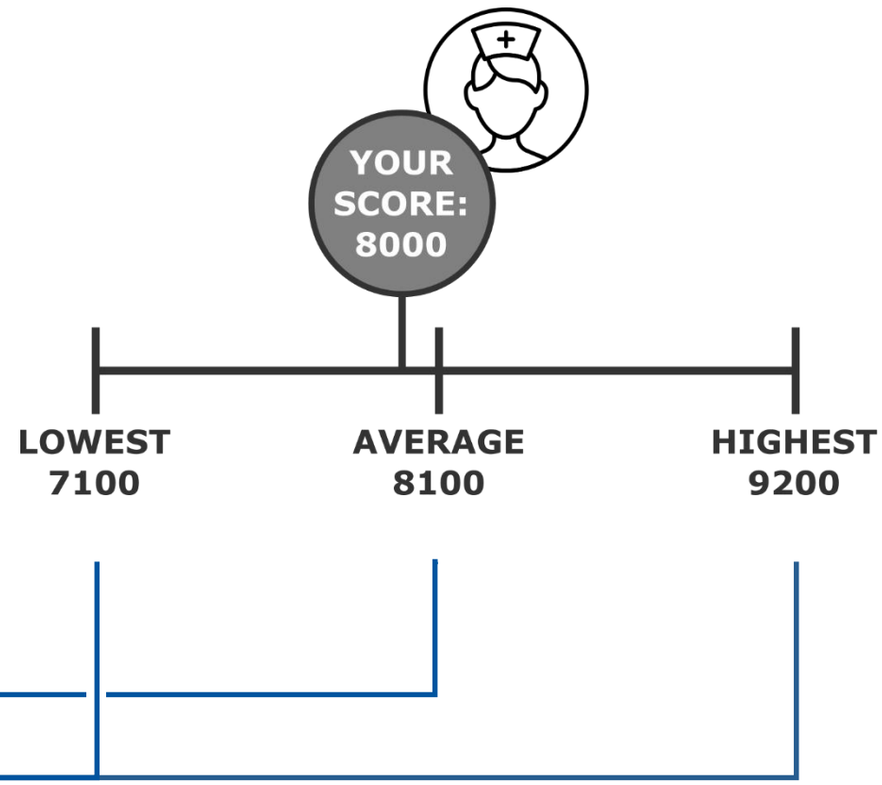


SMPC

- Each party:
  - Complete information for computation
  - Other inputs remain secret



SMPC



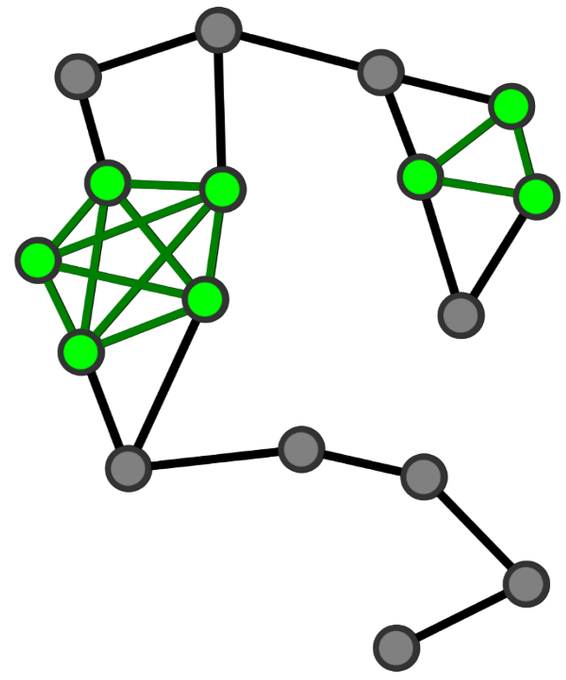
- Algorithms
  - Secure addition
  - Secure comparison

Decentralization

- Mesh network
- Computation partners not stationary
- Partitioning possible
- No central database server

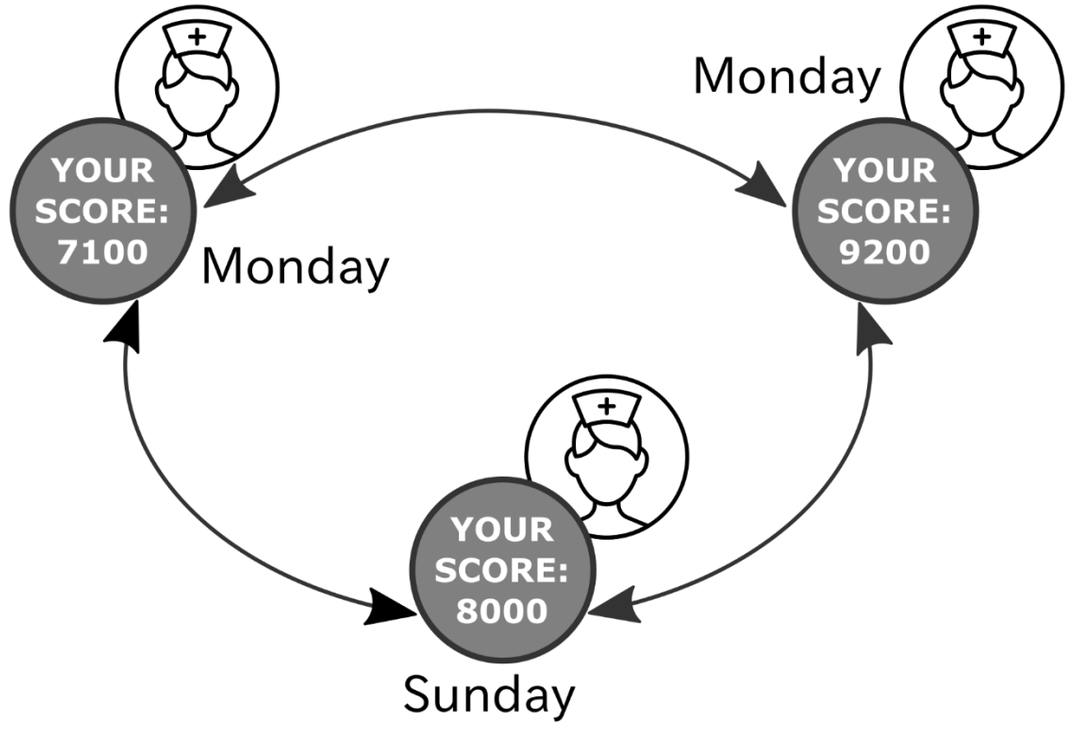
Decentralization

- Broadcast protocols
  - Detection of nodes
  - Distribute data
- Distributed Database
  - Blockchain



Distribution

- Synchronization of clocks (Berkeley)
- Coordinator election



Requirements

- C library; JNI for Java/Android usage
- Node coordination and synchronization
- SMPC
- Data distribution and preservation

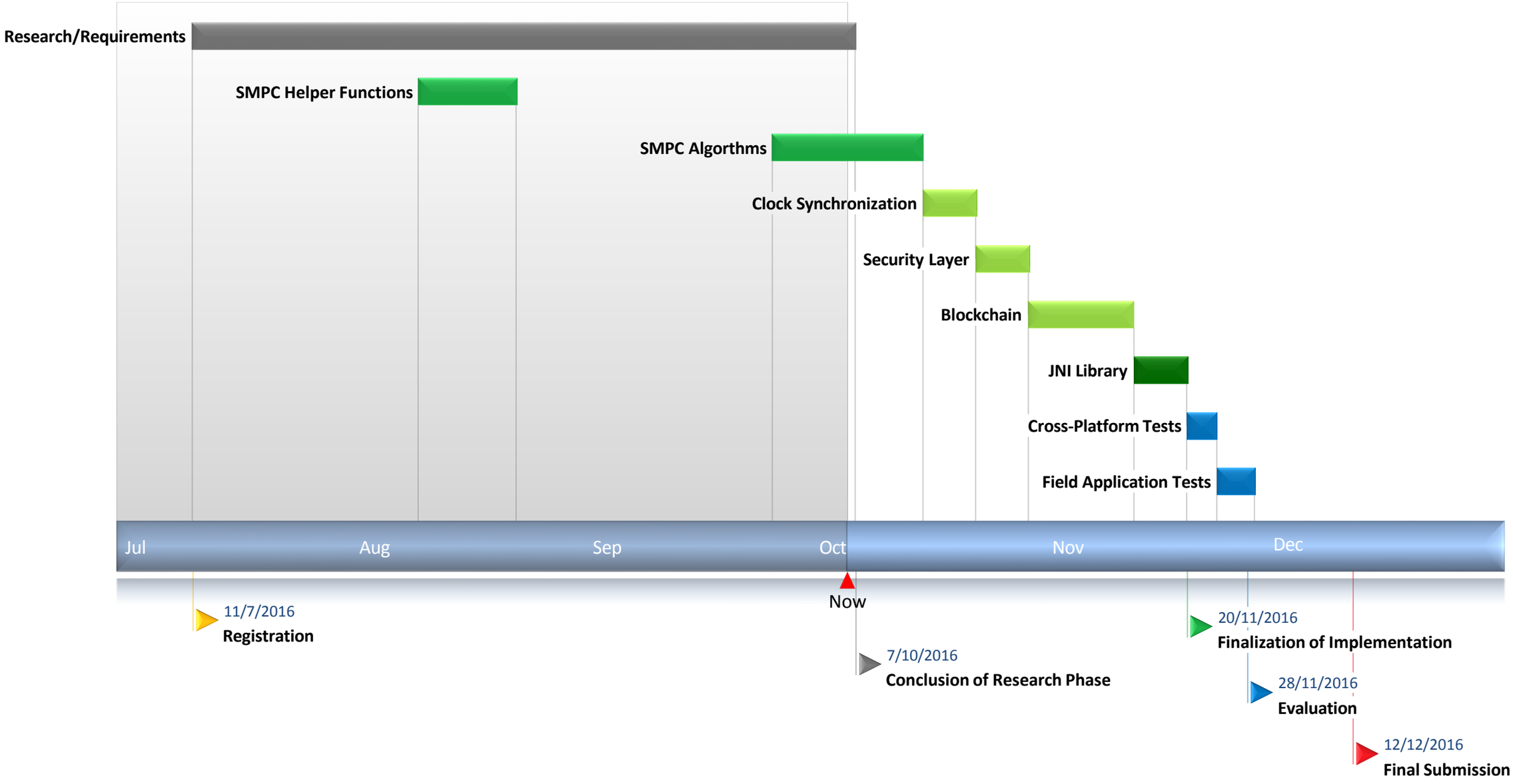
Tasks

- Secure addition protocol
- Secure comparison protocol
- Secure communication layer
- Detection/notification of participants
- Coordinator election
- Clock synchronization
- Distributed Database/blockchain
- Flooding

Evaluation

- Test framework with devices of diverse computation power
  - RasPi 3, various Android devices, Xadow GSM+BLE, TI CC2650STK
- Field application tests
- Attack scenarios
- Security evaluation in different environments

Schedule


Research/Requirements
SMPC Helper Functions
SMPC Algorthms
Clock Synchronization
Security Layer
Blockchain
JNI Library
Cross-Platform Tests
Field Application Tests
Jul
Aug
Sep
Oct
Nov
Dec
Now
11/7/2016
Registration
7/10/2016
Conclusion of Research Phase
20/11/2016
Finalization of Implementation
28/11/2016
Evaluation
12/12/2016
Final Submission

Summary

- SMPC for Decentralized Distributed Systems
  - privacy protecting computations
  - Mesh network