

# Mobile Hattrick

## Lab 06

Thibaut Britz

Andri Toggenburger

Roger Seidel

Michael Lorenzi

Betreuer: Michael Kuhn

Prof. Roger Wattenhofer

# Ziel / Aufgabe

- Multiplayer-Spiel für Mobiltelefone
  - P2P, ohne mobilen Internetzugang
  - Fokus auf:
    - Cheating erschweren
    - Ehrliche Spieler schützen

# Spiel (1)

- Spiel über Bluetooth
  - Aufstellung/Formation wählen
  - Auswechslungen zur Halbzeit
- Verbesserungen bei Erfolg
  - Stärkekpunkte auf Spieler verteilbar
- Rangliste
  - Lokal und Global



# Spiel (2)

- Simulation
  - Tore
  - Torschützen
  - Chancenverhältnis
  - Verletzungen
- Kein Geld, kein Transfermarkt

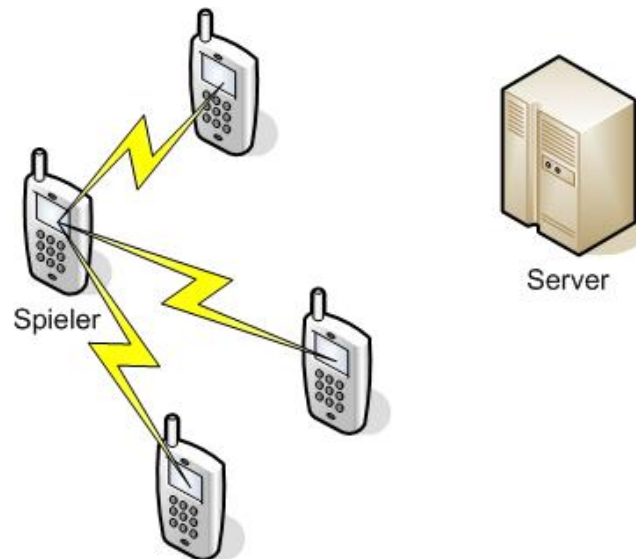


# Server

- Zentraler Server im Internet
- Warum?
  - Spiele nachberechnen
    - Cheating erkennen
  - Globale IDs, Globale Rangliste führen
  - Banliste
- Verbindung über GPRS oder via PC-Link
  - PC-Link: USB/Infrarot/BT, kostenlos

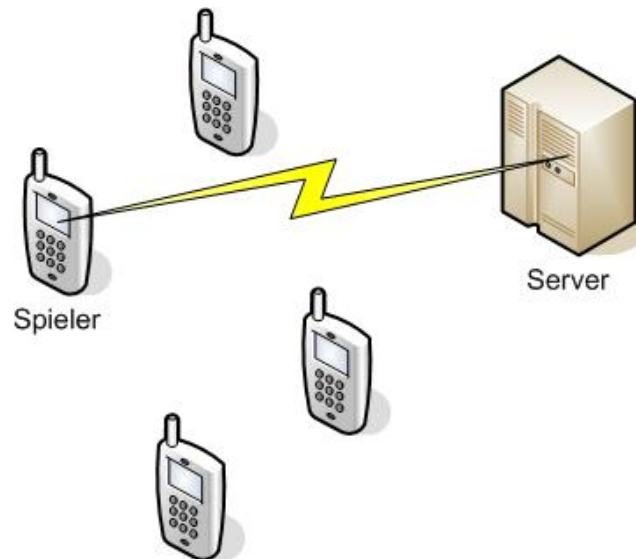
# Rollen Server / Natels

- Natels/Spieler berechnen das Spiel lokal und speichern es
  - Gemeinsames Berechnen



# Rollen Server / Natels

- Natels/Spieler berechnen das Spiel lokal und speichern es
  - Gemeinsames Berechnen
- Beide Spieler schicken das Spiel irgendwann dem Server
  - Verifikation, Rangliste
  - Banliste führen, falls ein Spieler sich nicht meldet oder versucht zu cheaten



# Kryptographie

- Commitments
  - Überprüfbare Verpflichtung auf einen Wert ohne ihn zu zeigen (analog ungeöffneter Briefumschlag)
  - Commitments für Zufallszahlen und Aufstellungen werden ausgetauscht
- Public-Key-Infrastruktur
  - Clients / Server haben (secret key / public key)
  - Verschlüsselung, Signaturen

# Spiel-Protokoll

## Phase 1:

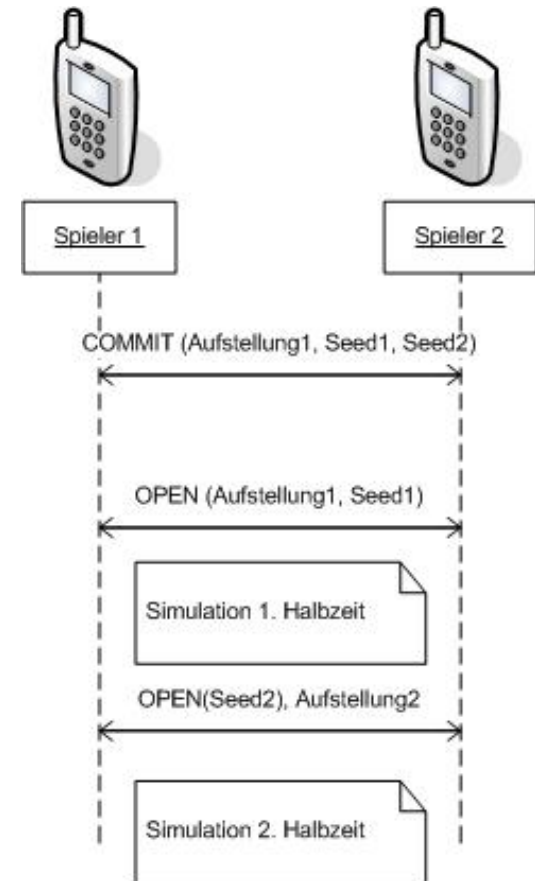
- Commitments der Seed-Werte (für beide Halbzeiten) und Aufstellungen austauschen, dasselbe verschlüsselt für den Server
  - Spiel gilt als gespielt, kann vom Server verifiziert werden
  - Spieler kennen den Ausgang des Spiels aber noch nicht

## Phase 2:

- Öffnen der Commitments für die 1. Halbzeit
  - Bitweises XOR der Seed-Werte der beiden Spieler
  - Seed für PRG bei beiden Clients gleich -> gleiche Simulation

## Phase 3:

- Simulieren der 1. Halbzeit, Austausch der neuen Aufstellungen, öffnen der Commitments für die 2. Halbzeit



# Angriffsmöglichkeiten

- Absichtlicher Verbindungsabbruch
  - Spieler kann verhindern dass Auswechslungen in der Pause gemacht werden können
- Koalitionen
  - Zufallszahlen austauschen bis das gewünschte Resultat herauskommt
  - Spiele selektiv zum Server schicken

# Demo

- Vielen Dank für eure Aufmerksamkeit
  
- Demo