"Risk" in an untrusted setting

Jude Southworth

January 28, 2023

Risk

- *Risk* is a popular strategy board game.
- It is played on a single board, depicting a world map, partitioned into regions.
- A player owns a region of the map by stationing troops within the region.
- Players fight for regions by gambling some of their troops against the troops in the other player's region.

Risk

- *Risk* has a variant called "fog of war".
- In this variant, players cannot see the number of troops stationed within regions they don't control, or don't neighbour.
- This variant is therefore only played online, in a **trusted setup**.

Proposition

- Play fog-of-war Risk in an untrusted setup.
- In the untrusted setup, the same guarantees should be made as the trusted setup, but on a peer-to-peer network.

Proposition

- Zero-knowledge proofs.
- Asymmetric encryption.
- Hashing.
  -