

"Risk" in an untrusted setting

Jude Southworth

February 8, 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.

Rationale

▶ **Federation**

- ▶ Federated platforms can have longer lifespans than centralised platforms.
- ▶ Federated platforms are more resistant to censorship and can help promote anonymity and privacy.

▶ **Security**

- ▶ Constantly looking for ways to secure against threats specific to federated and decentralised infrastructures.
- ▶ Security issues can be devastating even to decentralised infrastructures.

State of the art

- ▶ Private key encryption.
- ▶ Signatures.
- ▶ Additive homomorphic encryption.
- ▶ **Web platform.** Rapidly evolving.
- ▶ **Monero, Zcash.** Decentralised ledgers respectively using the *Bulletproof* and *ZK-SNARK* zero-knowledge proof systems.

Results

Emulated P2P environment using WebSockets.

Results

Produce shared random values without beacons using commitment schemes.

Results

Generating large primes using ECMAScript BigInt and Rabin-Miller.

Results

Implementation of the Paillier additive homomorphic cryptosystem.

Results

Implementation of Risk.