template

Fareed Sheriff

January 7, 2023

Introduction

This is a description for a game made for the 2023 IAP Modern Zero-Knowledge and Weblab classes. It is a simple multiplayer game where each player consists of a circular base and square bullets. Every player starts with a circle of radius r_i that shrinks as they fire bullets. The game ends when one person's `hp` shrinks to ≤ 0 (a win) or when both players' `hp` are below the threshold required to fire a bullet (typically 1 `hp` — a stalemate). Only bullets can harm players; players themselves cannot directly attack others. The game is played in a square field — bullets that hit the border reflect off and players cannot go past the border.

Mechanisms

Players have access to circles (their base) and bullets. The player base radius is inversely proportional to the speed at which players move — the smaller the base, the faster players move. The `hp` of both players is initially set to $k > 1$ to ensure that each person can fire off at least one bullet. The `hp` of a player decreases by 1 for each bullet fired and decreases by $k \geq 2$ for each opponent bullet they receive. The radius of the circle is $\sqrt{k_i}$ where k is the `hp` of player i and as k decreases, the radius decreases as well. Players can recover `hp` by recovering their bullets, which they can do by either moving over their bullets or by pressing `[CTRL]`, which pulls the bullets toward them. Players move their base with the arrow keys, aim bullets with the mouse, and fire bullets with `[SPACE]`.

Zero-Knowledge

Each player also does not know the location of opponent bullets outside a predetermined radius of their base but does know the location of opponent bases. This radius is fixed for the duration of the game, so when a player's base shrinks they have greater area in which to see opponent items. This is implemented through a zero-knowledge proof that an opponent item is within some fixed radius of a player's base using a zk range proof. We also ensure that the locations of all player items are always up-to-date by hashing the coordinates into a Merkle tree and checking that the Merkle root is always the same. Also, for every new move that gets played, a zkp is generated for the move to verify that it doesn't violate board constraints and that it doesn't change direction or speed without influence from the base. Furthermore, we ensure that players do not teleport using a technique similar to the one used in the 'fog-of-war' implemented in Dark Forest.