Battleship with ZK-SNARKS

March 22, 2024

1 Definitions

A **shot** represents a player's attempt at shooting at a ship. A **hit** represents a shot that has reached a ship. A **kill** represents a successful sinking of a ship.

2 Setup

We use two different proofs. The first one P_g proves that the grid provided by the opponent is valid and has the hash value h and the second one P_s proves that the given list of shots S_i for grid of hash h produce the correct number of hits H_i and kills K_i for turn i.

3 Encoding

A **grid** is represented as an ordered list $\{b_1, b_2, ..., b_{100}\}$ where $b_i \in \{0, 1\}$ representing the squares of the board from left to right and top to bottom:

$$\begin{aligned} \text{grid} = \{&\text{A1, B1, ..., J1,} \\ &\text{A2, B2, ..., J2,} \\ &\vdots \\ &\text{A10, B10, ..., J10}\} \end{aligned}$$

$$= \{b_1, b_2, \ldots, b_{100}\} \text{ with } b_i \in \{0, 1\}$$

We encode the position of each ship as a unique number in $\mathbb{Z}_2^{100}$