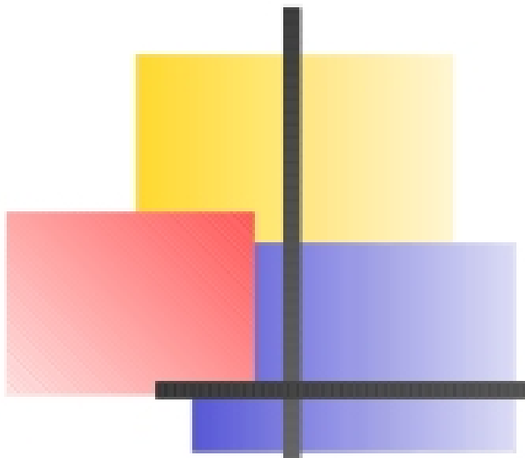

How to Play Any Mental Game

Paper by Oded Goldreich, Silvio Micali, and Avi Wigderson

Presentation by Paul Kuliniewicz

What Is a Mental Game?

- Another way to look at **secure multiparty computation**.
- Common input CI.
- Each player i has private input x_i.
- Each player should receive result $f(CI, x_1, \ldots, x_n)$ without learning about other players' private inputs.

Games as State Machines

- Set $S = \{\sigma_1, \sigma_2, \ldots\}$ of possible states.
- Each player i has a **knowledge function** $K_i(\sigma)$ that represents i's knowledge at state σ.
- Each action is a state transition.
- At the final state, each player i receives **payoff** $p_i(\sigma)$.