Rational Secret Sharing AS Extensive Games

http://www.firstlight.cn 2010-04-05

Some punishments in rational secret sharing schemes turn out to be empty threats. In this paper, we first model 2-out-of-2 rational secret sharing in an extensive game with imperfect information, and then provide a strategy for achieving secret recovery in this game. Moreover, we prove that the strategy is a sequential equilibrium which means after any history of the game no player can benefit from deviations so long as the other players stick to the strategy. Therefor, by considering rational secret sharing as an extensive game, we design a scheme which eliminates empty threats. Except assuming the existence of a simultaneous broadcast channel, our scheme can have dealer off-line and extend to the t-out-of-n rational secret sharing, and also satisfies computational equilibria in some sense.

存档文本